Surveillance and the Critical Digital Humanities

Christina Boyles and Andrew Boyles Peterson
Welcome to DHSI 2023!

Thank you for joining the DHSI community!

In this coursepack, you will find essential workshop materials prefaced by some useful general information about DHSI 2023.

Given our community’s focus on things computational, it will be a surprise to no one that we might expect additional information and materials online for some of the workshops—which will be made available to you where applicable—or that the most current version of all DHSI-related information may be found on our website at dhsi.org. Do check in there first if you need any information that's not in this coursepack.

Please also note that materials in DHSI’s online workshop folders could be updated at any point. We recommend checking back on any DHSI online workshop folder(s) that have been shared with you in case additional materials are added as DHSI approaches and takes place.

And please don't hesitate to be in touch with us at institut@uvic.ca or via Twitter at @AlyssaA_DHSI or @DHInstitute if we can be of any help.

We hope you enjoy your time with us!
Statement of Ethics & Inclusion

Please review the DHSI Statement of Ethics & Inclusion available here: https://dhsi.org/statement-of-ethics-inclusion/

DHSI is dedicated to offering a safe, respectful, friendly, and collegial environment for the benefit of everyone who attends and for the advancement of the interests that bring us together. There is no place at DHSI for harassment or intimidation of any kind.

By registering for DHSI, you have agreed to comply with these commitments.

Virtual Sessions

Your registration in DHSI 2023 also includes access to the virtual institute lecture sessions. Access details for these talks will be shared as DHSI approaches.

Due to the high volume of attendees, please ensure your DHSI registration name or DHSI preferred name and your Zoom name match so that we know to let you into the virtual sessions.

DHSI Materials

DHSI materials (ex. videos, documents, etc.) are intended for registrant use only. By registering, you have agreed that you will not circulate any DHSI content. If someone asks you for the materials, please invite them to complete the registration form to request access or contact us at institut@uvic.ca.
Auditor and participant registration

If you registered to audit any workshops, note that auditor involvement is intended to be fully self-directed without active participation in the workshop. The auditor option offers more flexibility regarding pace and time with the workshop content. Your registration as an auditor will include access to some asynchronous workshop materials only and does not include access to live workshop sessions and/or individual/group instruction or consultation. Please direct any questions about DHSI workshop auditing to institut@uvic.ca.

If you registered as a participant in any workshops, your registration includes access to asynchronous content + active participation in live workshop session(s). The workshop instructor(s) will contact you about the date(s), time(s), and platform(s) of the live workshop session(s).

If you are unsure whether you registered as an auditor or participant, please check your registration confirmation email. Further questions can be directed to institut@uvic.ca.

Schedule

The at-a-glance schedule of DHSI 2023 courses, workshops, institute lectures and aligned conferences & events can be found here: https://dhsi.org/timetable/

All times are listed in North American Pacific Time Zone.

For those who registered as participants in any workshops, live sessions for online workshops are not currently listed on the above-referenced schedule. Instructors will be in touch with registered participants directly about the exact date(s) and time(s) of their live workshop session(s).
Acknowledgements

We would like to thank our partners and sponsors (including the Social Sciences and Humanities Research Council), workshop instructors, aligned conference & event organizers, institute lecturers, local facilitators, and beyond for making this possible.

Further information

General DHSI 2023 information: https://dhsi.org/program/

Full course listings (in-person): https://dhsi.org/on-campus-courses/

Full workshop listings (online): https://dhsi.org/online-workshops/


Aligned conferences & events (online): https://dhsi.org/online-aligned-conferences-events/

Institute lectures: https://dhsi.org/institute-lectures/

Frequently asked questions: https://dhsi.org/faq/

Any questions not addressed in the above pages? Please email us at institut@uvic.ca!
Hello,

Welcome to Surveillance and the Digital Humanities! Enclosed are the schedule and readings for the week. We are looking forward to some terrific discussions, so please come to class with each day’s readings complete. Our course will be sticking closely to the schedule, with a variety of tech and group activities slated in addition to our discussions.

Thank you all, and we look forward to seeing you in June!

All the best,

Christina Boyles
cboyles@msu.edu

Andy Boyles Petersen
andyjp@msu.edu
Surveillance and the Digital Humanities

Monday, June 6
10:15-12:00  **Introductions**
Foucault, *Discipline and Punish*, Panopticism

13:30-16:00  **Historical Surveillance**
Browne, *Dark Matters*, “Through the Door of No Return,” pp. 31-62

Tuesday, June 7
09:00-12:00  **Mass Surveillance**
Nesbit, *Quartz*, “Google’s true origin partly lies in CIA and NSA research grants for mass surveillance”

13:30-16:00  **Social Media**
Gillmor, ACLU, “Facebook Is Tracking Me Even Though I’m Not on Facebook”

Wednesday, June 8
09:00-12:00  **Biometrics**

13:30-16:00  **Algorithms**
Noble, excerpt from *Algorithms of Oppression*, “A Society, Searching,” pp. 35-63
Gallagher, *Computers & Composition*, “Writing for Algorithmic Audiences”

Thursday, June 9
09:00-12:00  **Sousveillance**

13:30-16:00  **Strategies for Activism**
Our Data Bodies, “Reclaiming Our Data Interim Report”

Friday, June 10
09:00-12:00  Prepping our Course Exhibit
Day 1: Introductions and Historical Surveillance
Michel Foucault. Discipline & Punish (1975), Panopticism

III. DISCIPLINE

3. Panopticism


The following, according to an order published at the end of the seventeenth century, were the measures to be taken when the plague appeared in a town.

First, a strict spatial partitioning: the closing of the town and its outlying districts, a prohibition to leave the town on pain of death, the killing of all stray animals; the division of the town into distinct quarters, each governed by an intendant. Each street is placed under the authority of a syndic, who keeps it under surveillance; if he leaves the street, he will be condemned to death. On the appointed day, everyone is ordered to stay indoors: it is forbidden to leave on pain of death. The syndic himself comes to lock the door of each house from the outside; he takes the key with him and hands it over to the intendant of the quarter; the intendant keeps it until the end of the quarantine. Each family will have made its own provisions; but, for bread and wine, small wooden canals are set up between the street and the interior of the houses, thus allowing each person to receive his ration without communicating with the suppliers and other residents; meat, fish and herbs will be hoisted up into the houses with pulleys and baskets. If it is absolutely necessary to leave the house, it will be done in turn, avoiding any meeting. Only the intendants, syndics and guards will move about the streets and also, between the infected houses, from one corpse to another, the ‘crows’, who can be left to die: these are ‘people of little substance who carry the sick, bury the dead, clean and do many vile and abject offices’. It is a segmented, immobile, frozen space. Each individual is fixed in his place. And, if he moves, he does so at the risk of his life, contagion or punishment.

Inspection functions ceaselessly. The gaze is alert everywhere: ‘A considerable body of militia, commanded by good officers and men of substance’, guards at the gates, at the town hall and in every quarter to ensure the prompt obedience of the people and the most absolute authority of the magistrates, ‘as also to observe all disorder, theft and extortion’. At each of the town gates there will be an observation post; at the end of each street sentinels. Every day, the intendant visits the quarter in charge, inquires whether the syndics have carried out their tasks, whether the inhabitants have anything to complain of; they ‘observe their actions’. Every day, too, the syndic goes into the street for which he is responsible; stops before each house: gets all the inhabitants to appear at the windows (those who live overlooking the courtyard will be allocated a window looking onto the street at which no one but they may show themselves); he calls each of them by name; informs himself as to the state of each and every one of them - ‘in which respect the inhabitants will be compelled to speak the truth under pain of death’; if someone does not appear at the window, the syndic must ask why: ‘In this way he will find out easily enough whether dead or sick are being concealed.’ Everyone locked up in his cage, everyone at his window, answering to his name and showing himself when asked - it is the great review of the living and the dead.

This surveillance is based on a system of permanent registration: reports from the syndics to the intendants, from the intendants to the magistrates or mayor At the beginning of the ‘lock up’, the role of each of the inhabitants present in the town is laid down, one by one; this document bears ‘the name, age, sex of everyone, notwithstanding his condition’: a copy is sent to the intendant of the quarter, another to the office of the town hall, another to enable the syndic to make his daily roll call. Everything that may be observed during the course of the visits - deaths, illnesses, complaints, irregularities is noted down and transmitted to the intendants and magistrates. The magistrates have complete control over medical treatment; they have appointed a physician in charge; no other practitioner may treat, no apothecary prepare medicine, no confessor visit a sick person without having received from him a written note ‘to prevent anyone from concealing and dealing with those sick of the contagion, unknown to the magistrates’. The registration of the pathological must be constantly centralized. The relation of each individual to his disease and to his death passes through the representatives of power, the registration they make of it, the decisions they take on it.

Five or six days after the beginning of the quarantine, the process of purifying the houses one by one is begun. All the inhabitants are made to leave; in each room ‘the furniture and goods’ are raised from the ground or suspended from the air; perfume is poured around the room; after carefully sealing the windows, doors and even the keyholes with wax, the
perfume is set alight. Finally, the entire house is closed while the perfume is consumed; those who have carried out the work are searched, as they were on entry, 'in the presence of the residents of the house, to see that they did not have something on their persons as they left that they did not have on entering'. Four hours later, the residents are allowed to re-enter their homes.

This enclosed, segmented space, observed at every point, in which the individuals are inserted in a fixed place, in which the slightest movements are supervised, in which all events are recorded, in which an uninterrupted work of writing links the centre and periphery, in which power is exercised without division, according to a continuous hierarchical figure, in each which individual is constantly located, examined and distributed among the living beings, the sick and the dead - all this constitutes a compact model of the disciplinary mechanism. The plague is met by order; its function is to sort out every possible confusion: that of the disease, which is transmitted when bodies are mixed together; that of the evil, which is increased when fear and death overcome prohibitions. It lays down for each individual his place, his body, his disease and his death, his well-being, by means of an omnipresent and omniscient power that subdivides itself in a regular, uninterrupted way even to the ultimate determination of the individual, of what characterizes him, of what belongs to him, of what happens to him. Against the plague, which is a mixture, discipline brings into play its power, which is one of analysis. A whole literary fiction of the festival grew up around the plague: suspended laws, lifted prohibitions, the frenzy of passing time, bodies mingling together without respect, individuals unmasked, abandoning their statutory identity and the figure under which they had been recognized, allowing a quite different truth to appear. But there was also a political dream of the plague, which was exactly its reverse: not the collective festival, "but strict divisions; not laws transgressed, but the penetration of regulation into even the smallest details of everyday life through the mediation of the complete hierarchy that assured the capillary functioning of power; not masks that were put on and taken off, but the assignment to each individual of his 'true' name, his 'true' place, his 'true' body, his 'true' disease. The plague as a form, at once real and imaginary, of disorder had as its medical and political correlative discipline. Behind the disciplinary mechanisms can be read the haunting memory of 'contagions', of the plague, of rebellions, crimes, vagabondage, desertions, people who appear and disappear, live and die in disorder.

If it is true that the leper gave rise to rituals of exclusion, which to a certain extent provided the model for and general form of the great Confinement, then the plague gave rise to disciplinary projects. Rather than the massive, binary division between one set of people and another, it called for multiple separations, individualizing distributions, an organization in depth of surveillance and control, an intensification and a ramification of power. The leper was caught up in a practice of rejection, of exile-enclosure; he was left to his doom in a mass among which it was useless to differentiate; those sick of the plague were caught up in a meticulous tactical partitioning in which individual differentiations were the constricting effects of a power that multiplied, articulated and subdivided itself; the great confinement on the one hand; the correct training on the other. The leper and his separation; the plague and its segmentations. The first is marked; the second analysed and distributed. The exile of the leper and the arrest of the plague do not bring with them the same political dream. The first is that of a pure community, the second that of a disciplined society. Two ways of exercising power over men, of controlling their relations, of separating out their dangerous mixtures. The plague-stricken town, traversed throughout with hierarchy, surveillance, observation, writing; the town immobilized by the functioning of an extensive power that bears in a distinct way over all individual bodies - this is the utopia of the perfectly governed city. The plague (envisaged as a possibility at least) is the trial in the course of which one may define ideally the exercise of disciplinary power. In order to make rights and laws function according to pure theory, the jurists place themselves in imagination in the state of nature; in order to see perfect disciplines functioning, rulers dreamt of the state of plague. Underlying disciplinary projects the image of the plague stands for all forms of confusion and disorder; just as the image of the leper, cut off from all human contact, underlies projects of exclusion.

They are different projects, then, but not incompatible ones. We see them coming slowly together, and it is the peculiarity of the nineteenth century that it applied to the space of exclusion of which the leper was the symbolic inhabitant (beggars, vagabonds, madmen and the disorderly formed the real population) the technique of power proper to disciplinary partitioning. Treat 'lepers' as 'plague victims', project the subtle segmentations of discipline onto the confused space of internment, combine it with the methods of analytical distribution proper to power, individualize the excluded, but use procedures of individualization to mark exclusion - this is what was operated regularly by disciplinary power from the beginning of the nineteenth century in the psychiatric asylum, the penitentiary, the reformatory, the approved school and, to some extent, the hospital. Generally speaking, all the authorities exercising individual control function according to a double mode; that of binary division and branding (mad/sane; dangerous/harmless; normal/abnormal); and that of coercive assignment of differential distribution (who he is; where he must be; how he is to be characterized; how he is to be recognized; how a constant surveillance is to be exercised over him in an individual way, etc.). On the one hand, the lepers are treated as plague victims; the tactics of individualizing disciplines are imposed on the excluded; and, on the other hand, the universality of disciplinary controls makes it possible to brand the 'leper' and to bring into play against him the dualistic mechanisms of exclusion. The constant division between the normal and the abnormal, to which every individual is subjected, brings us back to our own time, by applying the binary
branding and exile of the leper to quite different objects; the existence of a whole set of techniques and institutions for measuring, supervising and correcting the abnormal brings into play the disciplinary mechanisms to which the fear of the plague gave rise. All the mechanisms of power which, even today, are disposed around the abnormal individual, to brand him and to alter him, are composed of those two forms from which they distantly derive.

Bentham’s Panopticon is the architectural figure of this composition. We know the principle on which it was based: at the periphery, an annular building; at the centre, a tower; this tower is pierced with wide windows that open onto the inner side of the ring; the peripheric building is divided into cells, each of which extends the whole width of the building; they have two windows, one on the inside, corresponding to the windows of the tower; the other, on the outside, allows the light to cross the cell from one end to the other. All that is needed, then, is to place a supervisor in a central tower and to shut up in each cell a madman, a patient, a condemned man, a worker or a schoolboy. By the effect of backlighting, one can observe from the tower, standing out precisely against the light, the small captive shadows in the cells of the periphery. They are like so many cages, so many small theatres, in which each actor is alone, perfectly individualized and constantly visible. The panoptic mechanism arranges spatial unities that make it possible to see constantly and to recognize immediately. In short, it reverses the principle of the dungeon; or rather of its three functions - to enclose, to deprive of light and to hide - it preserves only the first and eliminates the other two. Full lighting and the eye of a supervisor capture better than darkness, which ultimately protected. Visibility is a trap.

To begin with, this made it possible - as a negative effect - to avoid those compact, swarming, howling masses that were to be found in places of confinement, those painted by Goya or described by Howard. Each individual, in his place, is securely confined to a cell from which he is seen from the front by the supervisor; but the side walls prevent him from coming into contact with his companions. He is seen, but he does not see; he is the object of information, never a subject in communication. The arrangement of his room, opposite the central tower, imposes on him an axial visibility; but the divisions of the ring, those separated cells, imply a lateral invisibility. And this invisibility is a guarantee of order. If the inmates are convicts, there is no danger of a plot, an attempt at collective escape, the planning of new crimes for the future, bad reciprocal influences; if they are patients, there is no danger of contagion; if they are madmen there is no risk of their committing violence upon one another; if they are schoolchildren, there is no copying, no noise, no chatter; no waste of time; if they are workers, there are no disorders, no theft, no coalitions, none of those distractions that slow down the rate of work, make it less perfect or cause accidents. The crowd, a compact mass, a locus of multiple exchanges, individualities merging together, a collective effect, is abolished and replaced by a collection of separated individualities. From the point of view of the guardian, it is replaced by a multiplicity that can be numbered and supervised; from the point of view of the inmates, by a sequestered and observed solitude (Bentham, 60-64).

Hence the major effect of the Panopticon: to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power. So to arrange things that the surveillance is permanent in its effects, even if it is discontinuous in its action; that the perfection of power should tend to render its actual exercise unnecessary; that this architectural apparatus should be a machine for creating and sustaining a power relation independent of the person who exercises it; in short, that the inmates should be caught up in a power situation of which they are themselves the bearers. To achieve this, it is at once too much and too little that the prisoner should be constantly observed by an inspector: too little, for what matters is that he knows himself to be observed; too much, because he has no need in fact
of being so. In view of this, Bentham laid down the principle that power should be visible and unverifiable. Visible: the inmate will constantly have before his eyes the tall outline of the central tower from which he is spied upon. Unverifiable: the inmate must never know whether he is being looked at at any one moment; but he must be sure that he may always be so. In order to make the presence or absence of the inspector unverifiable, so that the prisoners, in their cells, cannot even see a shadow, Bentham envisaged not only venetian blinds on the windows of the central observation hall, but, on the inside, partitions that intersected the hall at right angles and, in order to pass from one quarter to the other, not doors but zig-zag openings; for the slightest noise, a gleam of light, a brightness in a half-opened door would betray the presence of the guardian. The Panopticon is a machine for dissociating the see/being seen dyad: in the peripheric ring, one is totally seen, without ever seeing; in the central tower, one sees everything without ever being seen.

It is an important mechanism, for it automatizes and disindividualizes power. Power has its principle not so much in a person as in a certain concerted distribution of bodies, surfaces, lights, gazes; in an arrangement whose internal mechanisms produce the relation in which individuals are caught up. The ceremonies, the rituals, the marks by which the sovereign’s surplus power was manifested are useless. There is a machinery that assures dissymmetry, disequilibrium, difference. Consequently, it does not matter who exercises power. Any individual, taken almost at random, can operate the machine: in the absence of the director, his family, his friends, his visitors, even his servants (Bentham, 45). Similarly, it does not matter what motive animates him: the curiosity of the indiscreet, the malice of a child, the thirst for knowledge of a philosopher who wishes to visit this museum of human nature, or the perversity of those who take pleasure in spying and punishing. The more numerous those anonymous and temporary observers are, the greater the risk for the inmate of being surprised and the greater his anxious awareness of being observed. The Panopticon is a marvellous machine which, whatever use one may wish to put it to, produces homogeneous effects of power.

A real subjection is born mechanically from a fictitious relation. So it is not necessary to use force to constrain the convict to good behaviour, the madman to calm, the worker to work, the schoolboy to application, the patient to the observation of the regulations. Bentham was surprised that panoptic institutions could be so light: there were no more bars, no more chains, no more heavy locks; all that was needed was that the separations should be clear and the openings well arranged. The heaviness of the old ‘houses of security’, with their fortress-like architecture, could be replaced by the simple, economic geometry of a ‘house of certainty’. The efficiency of power, its constraining force have, in a sense, passed over to the other side - to the side of its surface of application. He who is subjected to a field of visibility, and who knows it, assumes responsibility for the constraints of power; he makes them play spontaneously upon himself; he inscribes in himself the power relation in which he simultaneously plays both roles; he becomes the principle of his own subjection. By this very fact, the external power may throw off its physical weight; it tends to the non-corporeal; and, the more it approaches this limit, the more constant, profound and permanent are its effects: it is a perpetual victory that avoids any physical confrontation and which is always decided in advance.

Bentham does not say whether he was inspired, in his project, by Le Vaux’s menagerie at Versailles: the first menagerie in which the different elements are not, as they traditionally were, distributed in a park (Loisel, 104-7). At the centre was an octagonal pavilion which, on the first floor, consisted of only a single room, the king’s salon; on every side large windows looked out onto seven cages (the eighth side was reserved for the entrance), containing different species of animals. By Bentham’s time, this menagerie had disappeared. But one finds in the programme of the Panopticon a similar concern with individualizing observation, with characterization and classification, with the analytical arrangement of space. The Panopticon is a royal menagerie; the animal is replaced by man, individual distribution by specific
It is polyvalent in its applications; it serves to reform prisoners, to instruct schoolchildren, to confine the insane, to supervise workers, to put beggars and idlers to work. It is a type of location of bodies in space, of distribution of individuals in relation to one another, of hierarchical organization, of disposition of centres and channels of power, of definition of the instruments and modes of intervention of power, which can be implemented in hospitals, workshops, schools, prisons. Whenever one is dealing with a multiplicity of individuals on whom a task or a particular form of behaviour must be imposed, the panoptic schema may be used. It is - necessary modifications apart - applicable to all establishments whatsoever, in which, within a space not too large to be covered or commanded by buildings, a number of persons are meant to be kept under inspection' (Bentham, 40; although Bentham takes the penitentiary in mind, it is because it has many different functions to fulfil - safe custody, confinement, solitude, forced labour and instruction).

So much for the question of observation. But the Panopticon was also a laboratory; it could be used as a machine to carry out experiments, to alter behaviour, to train or correct individuals. To experiment with medicines and monitor their effects. To try out different punishments on prisoners, according to their crimes and character, and to seek the most effective ones. To teach different techniques simultaneously to the workers, to decide which is the best. To try out pedagogical experiments - and in particular to take up once again the well-debated problem of secluded education, by using orphans. One would see what would happen when, in their sixteenth or eighteenth year, they were presented with other boys or girls; one could verify whether, as Helvetius thought, anyone could learn anything; one would follow 'the genealogy of every observable idea'; one could bring up different children according to different systems of thought, making certain children believe that two and two do not make four or that the moon is a cheese, then put them together when they are twenty or twenty-five years old; one would then have discussions that would be worth a great deal more than the sermons or lectures on which so much money is spent; one would have at least an opportunity of making discoveries in the domain of metaphysics. The Panopticon is a privileged place for experiments on men, and for analysing with complete certainty the transformations that may be obtained from them. The Panopticon may even provide an apparatus for supervising its own mechanisms. In this central tower, the director may spy on all the employees that he has under his orders: nurses, doctors, foremen, teachers, warders; he will be able to judge them continuously, alter their behaviour, impose upon them the methods he thinks best; and it will even be possible to observe the director himself. An inspector arriving unexpectedly at the centre of the Panopticon will be able to judge at a glance, without anything being concealed from him, how the entire establishment is functioning. And, in any case, enclosed as he is in the middle of this architectural mechanism, is not the - 5 director's own fate entirely bound up with it ? The incompetent physician who has allowed contagion to spread, the incompetent prison governor or workshop manager will be the first victims of an epidemic or a revolt. "By every tie I could devise", said the master of the Panopticon, "my own fate had been bound up by me with theirs" (Bentham, 177). The Panopticon functions as a kind of laboratory of power. Thanks to its mechanisms of observation, it gains in efficiency and in the ability to penetrate into men's behaviour; knowledge follows the advances of power, discovering new objects of knowledge over all the surfaces on which power is exercised.

The plague-stricken town, the panoptic establishment - the differences are important. They mark, at a distance of a century and a half, the transformations of the disciplinary programme. In the first case, there is an exceptional situation: against an extraordinary evil, power is mobilized; it makes itself everywhere present and visible; it invents new mechanisms; it separates, it immobilizes, it partitions constructs for a time what is both a counter-city and the perfect society; it imposes an ideal functioning, but one that is reduced, in the final analysis, like the evil that it combats, to a simple dualism of life and death: that which moves brings death, and one kills that which moves. The Panopticon, on the other hand, must be understood as a generalizable model of functioning; a way of defining power relations in terms of the everyday life of men. No doubt Bentham presents it as a particular institution, closed in upon itself. Utopias, perfectly closed in upon themselves, are common enough. As opposed to the ruined prisons, littered with mechanisms of torture, to be seen in Piranesi's engravings, the Panopticon presents a cruel, ingenious cage. The fact that it should have given rise, even in our own time, to so many variations, projected or realized, is evidence of the imaginary intensity that it has possessed for almost two hundred years. But the Panopticon must not be understood as a dream building: it is the diagram of a mechanism of power reduced to its ideal form; its functioning, abstracted from any obstacle, resistance or friction, must be represented as a pure architectural and optical system: it is in fact a figure of political technology that may and must be detached from any specific use.
In each of its applications, it makes it possible to perfect the exercise of power. It does this in several ways: because it can reduce the number of those who exercise it, while increasing the number of those on whom it is exercised. Because it is possible to intervene at any moment and because the constant pressure acts even before the offences, mistakes or crimes have been committed. Because, in these conditions, its strength is that it never intervenes, it is exercised spontaneously and without noise, it constitutes a mechanism whose effects follow from one another. Because, without any physical instrument other than architecture and geometry, it acts directly on individuals; it gives ‘power of mind over mind’. The panoptic schema makes any apparatus of power more intense: it assures its economy (in material, in personnel, in time); it assures its efficacy by its preventative character, its continuous functioning and its automatic mechanisms. It is a way of obtaining from power ‘in hitherto unexampled quantity’, ‘a great and new instrument of government . . . ; its great excellence consists in the great strength it is capable of giving to any institution it may be thought proper to apply it to’ (Bentham, 66).

It’s a case of ‘it’s easy once you’ve thought of it’ in the political sphere. It can in fact be integrated into any function (education, medical treatment, production, punishment); it can increase the effect of this function, by being linked closely with it; it can constitute a mixed mechanism in which relations of power (and of knowledge) may be precisely adjusted, in the smallest detail, to the processes that are to be supervised; it can establish a direct proportion between ‘surplus power’ and ‘surplus production’. In short, it arranges things in such a way that the exercise of power is not added on from the outside, like a rigid, heavy constraint, to the functions it invests, but is so subtly present in them as to increase their efficiency by itself increasing its own points of contact. The panoptic mechanism is not simply a hinge, a point of exchange between a mechanism of power and a function; it is a way of making power relations function in a function, and of making a function function through these power relations. Bentham’s Preface to Panopticon opens with a list of the benefits to be obtained from his ‘inspection-house’: ‘Morals reformed - health preserved - industry invigorated - instruction diffused - public burdens lightened - Economy seated, as it were, upon a rock - the gordian knot of the Poor-Laws not cut, but untied - all by a simple idea in architecture!’ (Bentham, 39)

Furthermore, the arrangement of this machine is such that its enclosed nature does not preclude a permanent presence from the outside: we have seen that anyone may come and exercise in the central tower the functions of surveillance, and that, this being the case, he can gain a clear idea of the way in which the surveillance is practised. In fact, any panoptic institution, even if it is as rigorously closed as a penitentiary, may without difficulty be subjected to such irregular and constant inspections: and not only by the appointed inspectors, but also by the public; any member of society will have the right to come and see with his own eyes how the schools, hospitals, factories, prisons function. There is no risk, therefore, that the increase of power created by the panoptic machine may degenerate into tyranny; he disciplinary mechanism will be democratically controlled, since it will be constantly accessible ‘to the great tribunal committee of the world’. This Panopticon, subtly arranged so that an observer may observe, at a glance, so many different individuals, also enables everyone to come and observe any of the observers. The seeing machine was once a sort of dark room into which individuals spied; it has become a transparent building in which the exercise of power may be supervised by society as a whole.

The panoptic schema, without disappearing as such or losing any of its properties, was destined to spread throughout the
A whole disciplinary generalization - the Benthamite physics of power represents an acknowledgement of this - had operated throughout the classical age. The spread of disciplinary institutions, whose network was beginning to cover an ever larger surface and occupying above all a less and less marginal position, testifies to this: what was an islet, a privileged place, a circumstantial measure, or a singular model, became a general formula; the regulations characteristic of the Protestant and pious armies of William of Orange or of Gustavus Adolphus were transformed into regulations for all the armies of Europe; the model colleges of the Jesuits, or the schools of Batencour or Demia, following the example set by Sturm, provided the outlines for the general forms of educational discipline; the ordering of the naval and military hospitals provided the model for the entire reorganization of hospitals in the eighteenth century.

But this extension of the disciplinary institutions was no doubt only the most visible aspect of various, more profound processes.

1. The functional inversion of the disciplines. At first, they were expected to neutralize dangers, to fix useless or disturbed populations, to avoid the inconveniences of over-large assemblies; now they were being asked to play a positive role, for they were becoming able to do so, to increase the possible utility of individuals. Military discipline is no longer a mere means of preventing looting, desertion or failure to obey orders among the troops; it has become a basic technique to enable the army to exist, not as an assembled crowd, but as a unity that derives from this very unity an increase in its forces; discipline increases the skill of each individual, coordinates these skills, accelerates movements,
increases fire power, broadens the fronts of attack without reducing their vigour, increases the capacity for resistance, etc. The discipline of the workshop, while remaining a way of enforcing respect for the regulations and authorities, of preventing thefts or losses, tends to increase aptitudes, speeds, output and therefore profits; it still exerts a moral influence over behaviour, but more and more it treats actions in terms of their results, introduces bodies into a machinery, forces into an economy. When, in the seventeenth century, the provincial schools or the Christian elementary schools were founded, the justifications given for them were above all negative: those poor who were unable to bring up their children left them 'in ignorance of their obligations: given the difficulties they have in earning a living, and themselves having been badly brought up, they are unable to communicate a sound upbringing that they themselves never had'; this involves three major inconveniences: ignorance of God, idleness (with its consequent drunkenness, impurity, larceny, brigandage); and the formation of those gangs of beggars, always ready to stir up public disorder and 'virtually to exhaust the funds of the Hotel-Dieu' (Demia, 60-61). Now, at the beginning of the Revolution, the end laid down for primary education was to be, among other things, to 'fortify', to 'develop the body', to prepare the child 'for a future in some mechanical work', to give him 'an observant eye, a sure hand and prompt habits' (Talleyrand's Report to the Constituent Assembly, lo September 1791, quoted by Leon, 106). The disciplines function increasingly as techniques for making useful individuals. Hence their emergence from a marginal position on the confines of society, and detachment from the forms of exclusion or expropriation, confinement or retreat. Hence the slow loosening of their kinship with religious regularities and enclosures. Hence also their rooting in the most important, most central and most productive sectors of society. They become attached to some of the great essential functions: factory production, the transmission of knowledge, the diffusion of aptitudes and skills, the war-machine. Hence, too, the double tendency one sees developing throughout the eighteenth century to increase the number of disciplinary institutions and to discipline the existing apparatuses.

2. The swarming of disciplinary mechanisms. While, on the one hand, the disciplinary establishments increase, their mechanisms have a certain tendency to become 'de-institutionalized', to emerge from the closed fortresses in which they once functioned and to circulate in a 'free' state; the massive, compact disciplines are broken down into flexible methods of control, which may be transferred and adapted. Sometimes the closed apparatuses add to their internal and specific function a role of external surveillance, developing around themselves a whole margin of lateral controls. Thus the Christian School must not simply train docile children; it must also make it possible to supervise the parents, to gain information as to their way of life, their resources, their piety, their morals. The school tends to constitute minute social observatories that penetrate even to the adults and exercise regular supervision over them: the bad behaviour of the child, or his absence, is a legitimate pretext, according to Demia, for one to go and question the neighbours, especially if there is any reason to believe that the family will not tell the truth; one can then go and question the parents themselves, to find out whether they know their catechism and the prayers, whether they are determined to root out the vices of their children, how many beds there are in the house and what the sleeping arrangements are; the visit may end with the giving of alms, the present of a religious picture, or the provision of additional beds (Demia, 39-40). Similarly, the hospital is increasingly conceived of as a base for the medical observation of the population outside; after the burning down of the Hotel-Dieu in 1772, there were several demands that the large buildings, so heavy and so disordered, should be replaced by a series of smaller hospitals; their function would be to take in the sick of the quarter, but also to gather information, to be alert to any endemic or epidemic phenomena, to open dispensaries, to give advice to the inhabitants and to keep the authorities informed of the sanitary state of the region.

One also sees the spread of disciplinary procedures, not in the form of enclosed institutions, but as centres of observation disseminated throughout society. Religious groups and charity organizations had long played this role of 'disciplining' the population. From the Counter-Reformation to the philanthropy of the July monarchy, initiatives of this type continued to increase; their aims were religious (conversion and moralization), economic (aid and encouragement to work) or political (the struggle against discontent or agitation). One has only to cite by way of example the regulations for the charity associations in the Paris parishes. The territory to be covered was divided into quarters and cantons and the members of the associations divided themselves up along the same lines. These members had to visit their respective areas regularly. They will strive to eradicate places of ill-repute, tobacco shops, life-classes, gaming house, public scandals, blasphemy, impiety, and any other disorders that may come to their knowledge. They will also have to make individual visits to the poor; and the information to be obtained is laid down in regulations: the stability of the lodging, knowledge of prayers, attendance at the sacraments, knowledge of a trade, morality (and 'whether they have not fallen into poverty through their own fault'); lastly, 'one must learn by skilful questioning in what way they behave at home. Whether there is peace between them and their neighbours, whether they are careful to bring up their children in the fear of God . . . whether they do not have their older children of different sexes sleeping together and with them, whether they do not allow licentiousness and cajolery in their families, especially in their older daughters. If one has any doubts as to whether they are married, one must ask to see their marriage certificate'.

3. The state-control of the mechanisms of discipline. In England, it was private religious groups that carried out, for a long time, the functions of social discipline (cf. Radzinovitz, 203-14); in France, although a part of this role remained in the hands of parish guilds or charity associations, another - and no doubt the most important part - was very soon taken
The organization of a centralized police had long been regarded, even by contemporaries, as the most direct expression of absolutism; the sovereign had wished to have 'his own magistrate to whom he might directly entrust his orders, his commissions, intentions, and who was entrusted with the execution of orders and orders under the King's private seal' (a note by Duval, first secretary at the police magistrature, quoted in Funck-Brentano, 1). In effect, in taking over a number of pre-existing functions - the search for criminals, urban surveillance, economic and political supervision the police magistratures and the magistrature-general that presided over them in Paris transposed them into a single, strict, administrative machine: 'All the radiations of force and information that spread from the circumference culminate in the magistrate-general. . . . It is he who operates all the wheels that together produce order and harmony. The effects of his administration cannot be better compared than to the movement of the celestial bodies' (Des Essarts, 344 and 528).

But, although the police as an institution were certainly organized in the form of a state apparatus, and although this was certainly linked directly to the centre of political sovereignty, the type of power that it exercises, the mechanisms it operates and the elements to which it applies are specific. It is an apparatus that must be coextensive with the entire social body and not only by the extreme limits that it embraces, but by the minuteness of the details it is concerned with. Police power must bear 'over everything': it is not however the totality of the state nor of the kingdom as visible and invisible body of the monarch; it is the dust of events, actions, behaviour, opinions - 'everything that happens'; the police are concerned with 'those things of every moment', those 'unimportant things', of which Catherine II spoke in her Great Instruction (Supplement to the Instruction for the drawing up of a new code, 1769, article 535). With the police, one is in the indefinite world of a supervision that seeks ideally to reach the most elementary particle, the most passing phenomenon of the social body: 'The ministry of the magistrates and police officers is of the greatest importance; the objects that it embraces are in a sense definite, one may perceive them only by a sufficiently detailed examination' (Delamare, unnumbered Preface): the infinitely small of political power.

And, in order to be exercised, this power had to be given the instrument of permanent, exhaustive, omnipresent surveillance, capable of making all visible, as long as it could itself remain invisible. It had to be like a faceless gaze that transformed the whole social body into a field of perception: thousands of eyes posted everywhere, mobile attentions ever on the alert, a long, hierarchized network which, according to Le Maire, comprised for Paris the forty-eight commissaires, the twenty inspecteurs, then the 'observers', who were paid regularly, the 'basses mouches', or secret agents, who were paid by the day, then the informers, paid according to the job done, and finally the prostitutes. And this unceasing observation had to be accumulated in a series of reports and registers; throughout the eighteenth century, an immense police text increasingly covered society by means of a complex documentary organization (on the police registers in the eighteenth century, cf. Chassaingne). And, unlike the methods of judicial or administrative writing, what was registered in this way were forms of behaviour, attitudes, possibilities, suspicions - a permanent account of individuals' behaviour.

Now, it should be noted that, although this police supervision was entirely 'in the hands of the king', it did not function in a single direction. It was in fact a double-entry system: it had to correspond, by manipulating the machinery of justice, to the immediate wishes of the king, but it was also capable of responding to solicitations from below; the celebrated lettres de cachet, or orders under the king's private seal, which were long the symbol of arbitrary royal rule and which brought detention into disrepute on political grounds, were in fact demanded by families, masters, local notables, neighbours, parish priests; and their function was to punish by confinement a whole infra-penality, that of disorder, agitation, disobedience, bad conduct; those things that Ledoux wanted to exclude from his architecturally perfect city and which he called 'offences of non-surveillance'. In short, the eighteenth-century police added a disciplinary function to its role as the auxiliary of justice in the pursuit of criminals and as an instrument for the political supervision of plots, opposition movements or revolts. It was a complex function since it linked the absolute power of the monarch to the lowest levels of power disseminated in society; since, between these different, enclosed institutions of discipline (workshops, armies, schools), it extended an intermediary network, acting where they could not intervene, disciplining the non-disciplinary spaces; but it filled in the gaps, linked them together, guaranteed with its armed force an interstitial discipline and a meta-discipline. 'By means of a wise police, the sovereign accustoms the people to order and obedience' (Vattel, 162).

The organization of the police apparatus in the eighteenth century sanctioned a generalization of the disciplines that became co-extensive with the state itself. Although it was linked in the most explicit way with everything in the royal power that exceeded the exercise of regular justice, it is understandable why the police offered such slight resistance to the rearrangement of the judicial power; and why it has not ceased to impose its prerogatives upon it, with everincreasing weight, right up to the present day; this is no doubt because it is the secular arm of the judiciary; but it is also because to a far greater degree than the judicial institution, it is identified, by reason of its extent and mechanisms, with a society of the disciplinary type. Yet it would be wrong to believe that the disciplinary functions were confiscated and absorbed once and for all by a state apparatus.
'Discipline' may be identified neither with an institution nor with an apparatus; it is a type of power, a modality for its exercise, comprising a whole set of instruments, techniques, procedures, levels of application, targets; it is a 'physics' or an 'anatomy' of power, a technology. And it may be taken over by either 'specialized' institutions (the penitentiaries or 'houses of correction' of the nineteenth century), or by institutions that use it as an essential instrument for a particular end (schools, hospitals), or by pre-existing authorities that find in it a means of reinforcing or reorganizing their internal mechanisms of power (one day we should show how intra-familial relations, essentially in the parents-children cell, have become 'disciplined', absorbing since the classical age external schemata, first educational and military, then medical, psychiatric, psychological, which have made the family the privileged locus of emergence for the disciplinary question of the normal and the abnormal); or by apparatuses that have made discipline their principle of internal functioning (the disciplinarization of the administrative apparatus from the Napoleonic period), or finally by state apparatuses whose major, if not exclusive, function is to assure that discipline reigns over society as a whole (the police).

On the whole, therefore, one can speak of the formation of a disciplinary society in this movement that stretches from the enclosed disciplines, a sort of social 'quarantine', to an indefinitely generalizable mechanism of 'panopticism'. Not because the disciplinary modality of power has replaced all the others; but because it has infiltrated the others, sometimes undermining them, but serving as an intermediary between them, linking them together, extending them and above all making it possible to bring the effects of power to the most minute and distant elements. It assures an infinitesimal distribution of the power relations.

A few years after Bentham, Julius gave this society its birth certificate (Julius, 384-6). Speaking of the panoptic principle, he said that there was much more there than architectural ingenuity: it was an event in the 'history of the human mind'. In appearance, it is merely the solution of a technical problem; but, through it, a whole type of society emerges. Antiquity had been a civilization of spectacle. 'To render accessible to a multitude of men the inspection of a small number of objects': this was the problem to which the architecture of temples, theatres and circuses responded. With spectacle, there was a predominance of public life, the intensity of festivities, sensual proximity. In these rituals in which blood flowed, society found new vigour and formed for a moment a single great body. The modern age poses the opposite problem: 'To procure for a small number, or even for a single individual, the instantaneous view of a great multitude.' In a society in which the principal elements are no longer the community and public life, but, on the one hand, private individuals and, on the other, the state, relations can be regulated only in a form that is the exact reverse of the spectacle: 'It was to the modern age, to the ever-growing influence of the state, to its ever more profound intervention in all the details and all the relations of social life, that was reserved the task of increasing and perfecting its guarantees, by using and directing towards that great aim the building and distribution of buildings intended to observe a great multitude of men at the same time.'

Julius saw as a fulfilled historical process that which Bentham had described as a technical programme. Our society is one not of spectacle, but of surveillance; under the surface of images, one invests bodies in depth; behind the great abstraction of exchange, there continues the meticulous, concrete training of useful forces; the circuits of communication are the supports of an accumulation and a centralization of knowledge; the play of signs defines the anchorages of power; it is not that the beautiful totality of the individual is amputated, repressed, altered by our social order, it is rather that the individual is carefully fabricated in it, according to a whole technique of forces and bodies. We are much less Greeks than we believe. We are neither in the amphitheatre, nor on the stage, but in the panoptic machine, invested by its effects of power which we bring to ourselves since we are part of its mechanism. The importance, in historical mythology, of the Napoleonic character probably derives from the fact that it is at the point of junction of the monarchical, ritual exercise of sovereignty and the hierarchical, permanent exercise of indefinite discipline. He is the individual who looms over everything with a single gaze which no detail, however minute, can escape: 'You may consider that no part of the Empire is without surveillance, no crime, no offence, no contravention that remains unpunished, and that the eye of the genius who can enlighten all embraces the whole of this vast machine, without, however, the slightest detail escaping his attention' (Treilhard, 14). At the moment of its full blossoming, the disciplinary society still assumes with the Emperor the old aspect of the power of spectacle. As a monarch who is at one and the same time a usurper of the ancient throne and the organizer of the new state, he combined into a single symbol, ultimate figure the whole of the long process by which the pomp of sovereignty, the necessarily spectacular manifestations of power, were extinguished one by one in the daily exercise of surveillance, in a panopticism in which the vigilance of intersecting gazes was soon to render useless both the eagle and the sun.

The formation of the disciplinary society is connected with a number of broad historical processes - economic, juridico-political and, lastly, scientific - of which it forms part.

1. Generally speaking, it might be said that the disciplines are techniques for assuring the ordering of human multiplicities. It is true that there is nothing exceptional or even characteristic in this; every system of power is presented with the same problem. But the peculiarity of the disciplines is that they try to define in relation to the multiplicities a tactics of power that fulfils three criteria: firstly, to obtain the exercise of power at the lowest possible cost
Perhaps be said that the methods for administering the accumulation of men 220 Panopticism made possible a political
If the economic take-off of the West began with the techniques that made possible the accumulation of capital, it might
army or a school, reaches the threshold of a discipline when the relation of the one to the other becomes favourable.
the power which, in order to make them useful, must control them. A multiplicity, whether in a workshop or a nation, an
rather than to deploy the ostentatious signs of sovereignty. In a word, the disciplines are the ensemble of minute
power that insidiously objectifies those on whom it is applied; to form a body of knowledge about these individuals,
classification. In short, to substitute for a power that is manifested through the brilliance of those who exercise it, a
multiplicity that they regiment, such as hierarchical surveillance, continuous registration, perpetual assessment and
increase both the docility and the utility of all the elements of the system. This triple objective of the disciplines
 corresponds to a well-known historical conjuncture. One aspect of this conjuncture was the large demographic thrust of
the eighteenth century; an increase in the floating population (one of the primary objects of discipline is to fix; it is an
anti-nomadic technique); a change of quantitative scale in the groups to be supervised or manipulated (from the
beginning of the seventeenth century to the eve of the French Revolution, the school population had been increasing
rapidly, as had no doubt the hospital population; by the end of the eighteenth century, the peace-time army exceeded
200,000 men). The other aspect of the conjuncture was the growth in the apparatus of production, which was becoming
more and more extended and complex, it was also becoming more costly and its profitability had to be increased. The
development of the disciplinary methods corresponded to these two processes, or rather, no doubt, to the new need to
adjust their correlation. Neither the residual forms of feudal power nor the structures of the administrative monarchy, nor
the local mechanisms of supervision, nor the unstable, tangled mass they all formed together could carry out this role:
they were hindered from doing so by the irregular and inadequate extension of their network, by their often conflicting
functioning, but above all by the ‘costly’ nature of the power that was exercised in them. It was costly in several senses:
because directly it cost a great deal to the Treasury; because the system of corrupt offices and farmed-out taxes weighed
indirectly, but very heavily, on the population; because the resistance it encountered forced it into a cycle of perpetual
reinforcement; because it proceeded essentially by levying (levying on money or products by royal, seigniorial,
ecclesiastical taxation; levying on men or time by corvées of press-ganging, by locking up or banishing vagabonds). The
development of the disciplines marks the appearance of elementary techniques belonging to a quite different economy:
mechanisms of power which, instead of proceeding by deduction, are integrated into the productive efficiency of the
apparatuses from within, into the growth of this efficiency and into the use of what it produces. For the old principle of
‘levying-violence’, which governed the economy of power, the disciplines substitute the principle of ‘mildness-production-
profit’. These are the techniques that make it possible to adjust the multiplicity of men and the multiplication of the
apparatuses of production (and this means not only ‘production’ in the strict sense, but also the production of knowledge
and skills in the school, the production of health in the hospitals, the production of destructive force in the army).

In this task of adjustment, discipline had to solve a number of problems for which the old economy of power was not
sufficiently equipped. It could reduce the inefficiency of mass phenomena: reduce what, in a multiplicity, makes it much
less manageable than a unity; reduce what is opposed to the use of each of its elements and of their sum; reduce
everything that may counter the advantages of number. That is why discipline fixes; it arrests or regulates movements; it
clears up confusion; it dissipates compact groupings of individuals wandering about the country in unpredictable ways; it
establishes calculated distributions. It must also master all the forces that are formed from the very constitution of an
organized multiplicity; it must neutralize the effects of counter-power that spring from them and which form a resistance
to the power that wishes to dominate it: agitations, revolts, spontaneous organizations, coalitions - anything that may
establish horizontal conjunctions. Hence the fact that the disciplines use procedures of partitioning and verticality, that
they introduce, between the different elements at the same level, as solid separations as possible, that they define
compact hierarchical networks, in short, that they oppose to the intrinsic, adverse force of multiplicity the technique of
the continuous, individualizing pyramid. They must also increase the particular utility of each element of the multiplicity,
but by means that are the most rapid and the least costly, that is to say, by using the multiplicity itself as an instrument
of this growth. Hence, in order to extract from bodies the maximum time and force, the use of those overall methods
known as time-tables, collective training, exercises, total and detailed surveillance. Furthermore, the disciplines must
increase the effect of utility proper to the multiplicities, so that each is made more useful than the simple sum of its
elements: it is in order to increase the utilizable effects of the multiple that the disciplines define tactics of distribution,
reciprocal adjustment of bodies, gestures and rhythms, differentiation of capacities, reciprocal coordination in relation to
apparatuses or tasks. Lastly, the disciplines have to bring into play the power relations, not above but inside the very
texture of the multiplicity, as discreetly as possible, as well articulated on the other functions of these multiplicities and
also in the least expensive way possible: to this correspond anonymous instruments of power, coextensive with the
multiplicity that they regiment, such as hierarchical surveillance, continuous registration, perpetual assessment and
classification. In short, to substitute for a power that is manifested through the brilliance of those who exercise it, a
power that insidiously objectifies those on whom it is applied; to form a body of knowledge about these individuals,
rather than to deploy the ostentatious signs of sovereignty. In a word, the disciplines are the ensemble of minute
technical inventions that made it possible to increase the useful size of multiplicities by decreasing the inconveniences of
the power which, in order to make them useful, must control them. A multiplicity, whether in a workshop or a nation, an
army or a school, reaches the threshold of a discipline when the relation of the one to the other becomes favourable.

If the economic take-off of the West began with the techniques that made possible the accumulation of capital, it might
perhaps be said that the methods for administering the accumulation of men 220 Panopticism made possible a political
take-off in relation to the traditional, ritual, costly, violent forms of power, which soon fell into disuse and were superseded by a subtle, calculated technology of subjection. In fact, the two processes - the accumulation of men and the accumulation of capital - cannot be separated; it would not have been possible to solve the problem of the accumulation of men without the growth of an apparatus of production capable of both sustaining them and using them; conversely, the techniques that made the cumulative 'multiplicity of men useful accelerated the accumulation of capital. At a less general level, the technological mutations of the apparatus of production, the division of labour and the elaboration of the disciplinary techniques sustained an ensemble of very close relations (cf. Marx, Capital, vol. 1, chapter XIII and the very interesting analysis in Guerry and Deleuze). Each makes the other possible and necessary; each provides a model for the other. The disciplinary pyramid constituted the small cell of power within which the separation, coordination and supervision of tasks was imposed and made efficient; and analytical partitioning of time, gestures and bodily forces constituted an operational schema that could easily be transferred from the groups to be subjected to the mechanisms of production; the massive projection of military methods onto industrial organization was an example of this modelling of the division of labour following the model laid down by the schemata of power. But, on the other hand, the technical analysis of the process of production, its 'mechanical' breaking-down, were projected onto the labour force whose task it was to implement it: the constitution of those disciplinary machines in which the individual forces that they bring together are composed into a whole and therefore increased is the effect of this projection. Let us say that discipline is the unitary technique by which the body is reduced as a 'political' force at the least cost and maximized as a useful force. The growth of a capitalist economy gave rise to the specific modality of disciplinary power whose general formulas, techniques of submitting forces and bodies, in short, 'political anatomy', could be operated in the most diverse political regimes, apparatuses or institutions.

2. The panoptic modality of power - at the elementary, technical, merely physical level at which it is situated - is not under the immediate dependence or a direct extension of the great juridico-political structures of a society; it is nonetheless not absolutely independent. Historically, the process by which the bourgeoisie became in the course of the eighteenth century the politically dominant class was masked by the establishment of an explicit, coded and formally egalitarian juridical framework, made possible by the organization of a parliamentary, representative regime. But the development and generalization of disciplinary mechanisms constituted the other, dark side of these processes. The general juridical form that guaranteed a system of rights that were egalitarian in principle was supported by these tiny, everyday, physical mechanisms, by all those systems of micro-power that are essentially non-egalitarian and asymmetrical that we call the disciplines. And although, in a formal way, the representative regime makes it possible, directly or indirectly, with or without relays, for the will of all to form the fundamental authority of sovereignty, the disciplines provide, at the base, a guarantee of the submission of forces and bodies. The real, corporal disciplines constituted the foundation of the formal, juridical liberties. The contract may have been regarded as the ideal foundation of law and political power; panopticism constituted the technique, universally widespread, of coercion. It continued to work in depth on the juridical structures of society, in order to make the effective mechanisms of power function in opposition to the formal framework that it had acquired. The 'Enlightenment', which discovered the liberties, also invented the disciplines.

In appearance, the disciplines constitute nothing more than an infra-law. They seem to extend the general forms defined by law to the infinities of individual lives; or they appear as methods of training that enable individuals to become integrated into these general demands. They seem to constitute the same type of law on a different scale, thereby making it more meticulous and more indulgent. The disciplines should be regarded as a sort of counter-law They have the precise role of introducing insuperable asymmetries and excluding reciprocities. First, because discipline creates between individuals a 'private' link, which is a relation of constraints entirely different from contractual obligation; the acceptance of a discipline may be underwritten by contract; the way in which it is imposed, the mechanisms it brings into play, the non-reversible subordination of one group of people by another, the 'surplus' power that is always fixed on the same side, the inequality of position of the different 'partners' in relation to the common regulation, all these distinguish the disciplinary link from the contractual link, and make it possible to distort the contractual link systematically from the moment it has as its content a mechanism of discipline. We know, for example, how many real procedures undermine the legal fiction of the work contract: workshop discipline is not the least important. Moreover, whereas the juridical systems define juridical subjects according to universal norms, the disciplines characterize, classify, specialize; they distribute along a scale, around a norm, hierarchize individuals in relation to one another and, if necessary, disqualify and invalidate. In any case, in the space and during the time in which they exercise their control and bring into play the asymmetries of their power, they effect a suspension of the law that is never total, but is never annulled either. Regular and institutional as it may be, the discipline, in its mechanism, is a 'counter-law'. And, although the universal juridicism of modern society seems to fix limits on the exercise of power, its universally widespread panopticism enables it to operate, on the underside of the law, a machinery that is both immense and minute, which supports, reinforces, multiplies the asymmetry of power and undermines the limits that are traced around the law. The minute disciplines, the panopticisms of every day may well be below the level of emergence of the great apparatuses and the great political struggles. But, in the genealogy of modern society, they have been, with the class domination that traverses it, the
political counterpart of the juridical norms according to which power was redistributed. Hence, no doubt, the importance that has been given for so long to the small techniques of discipline, to those apparently insignificant tricks that it has invented, and even to those 'sciences' that give it a respectable face; hence the fear of abandoning them if one cannot find any substitute; hence the affirmation that they are at the very foundation of society, and an element in its equilibrium, whereas they are a series of mechanisms for unbalancing power relations definitively and everywhere; hence the persistence in regarding them as the humble, but concrete form of every morality, whereas they are a set of physico-political techniques.

To return to the problem of legal punishments, the prison with all the corrective technology at its disposal is to be resituated at the point where the codified power to punish turns into a disciplinary power to observe; at the point where the universal punishments of the law are applied selectively to certain individuals and always the same ones; at the point where the redefinition of the juridical subject by the penalty becomes a useful training of the criminal; at the point where the law is inverted and passes outside itself, and where the counter-law becomes the effective and institutionalized content of the juridical forms. What generalizes the power to punish, then, is not the universal consciousness of the law in each juridical subject; it is the regular extension, the infinitely minute web of panoptic techniques.

3. Taken one by one, most of these techniques have a long history behind them. But what was new, in the eighteenth century, was that, by being combined and generalized, they attained a level at which the formation of knowledge and the increase of power regularly reinforce one another in a circular process. At this point, the disciplines crossed the 'technological' threshold. First the hospital, then the school, then, later, the workshop were not simply 'reordered' by the disciplines; they became, thanks to them, apparatuses such that any mechanism of objectification could be used in them as an instrument of subjection, and any growth of power could give rise in them to possible branches of knowledge; it was this link, proper to the technological systems, that made possible within the disciplinary element the formation of clinical medicine, psychiatry, child psychology, educational psychology, the rationalization of labour. It is a double process, then: an epistemological 'thaw' through a refinement of power relations; a multiplication of the effects of power through the formation and accumulation of new forms of knowledge.

The extension of the disciplinary methods is inscribed in a broad historical process: the development at about the same time of many other technologies - agronomical, industrial, economic. But it must be recognized that, compared with the mining industries, the emerging chemical industries or methods of national accountancy, compared with the blast furnaces or the steam engine, panopticism has received little attention. It is regarded as not much more than a bizarre little utopia, a perverse dream - rather as though Bentham had been the Fourier of a police society, and the Phalanstery had taken on the form of the Panopticon. And yet this represented the abstract formula of a very real technology, that of individuals. There were many reasons why it received little praise; the most obvious is that the discourses to which it gave rise rarely acquired, except in the academic classifications, the status of sciences; but the real reason is no doubt that the power that it operates and which it augments is a direct, physical power that men exercise upon one another. An inglorious culmination had an origin that could be only grudgingly acknowledged. But it would be unjust to compare the disciplinary techniques with such inventions as the steam engine or Amici's microscope. They are much less; and yet, in a way, they are much more. If a historical equivalent or at least a point of comparison had to be found for them, it would be rather in the inquisitorial technique.

The eighteenth century invented the techniques of discipline and the examination, rather as the Middle Ages invented the judicial investigation. But it did so by quite different means. The investigation procedure, an old fiscal and administrative technique, had developed above all with the reorganization of the Church and the increase of the princely states in the twelfth and thirteenth centuries. At this time it permeated to a very large degree the jurisprudence first of the ecclesiastical courts, then of the lay courts. The investigation as an authoritarian search for a truth observed or attested time of many other technologies - agronomical, industrial, economic. But it must be recognized that, compared with the mining industries, the emerging chemical industries or methods of national accountancy, compared with the blast furnaces or the steam engine, panopticism has received little attention. It is regarded as not much more than a bizarre little utopia, a perverse dream - rather as though Bentham had been the Fourier of a police society, and the Phalanstery had taken on the form of the Panopticon. And yet this represented the abstract formula of a very real technology, that of individuals. There were many reasons why it received little praise; the most obvious is that the discourses to which it gave rise rarely acquired, except in the academic classifications, the status of sciences; but the real reason is no doubt that the power that it operates and which it augments is a direct, physical power that men exercise upon one another. An inglorious culmination had an origin that could be only grudgingly acknowledged. But it would be unjust to compare the disciplinary techniques with such inventions as the steam engine or Amici's microscope. They are much less; and yet, in a way, they are much more. If a historical equivalent or at least a point of comparison had to be found for them, it would be rather in the inquisitorial technique.

The extension of the disciplinary methods is inscribed in a broad historical process: the development at about the same time of many other technologies - agronomical, industrial, economic. But it must be recognized that, compared with the mining industries, the emerging chemical industries or methods of national accountancy, compared with the blast furnaces or the steam engine, panopticism has received little attention. It is regarded as not much more than a bizarre little utopia, a perverse dream - rather as though Bentham had been the Fourier of a police society, and the Phalanstery had taken on the form of the Panopticon. And yet this represented the abstract formula of a very real technology, that of individuals. There were many reasons why it received little praise; the most obvious is that the discourses to which it gave rise rarely acquired, except in the academic classifications, the status of sciences; but the real reason is no doubt that the power that it operates and which it augments is a direct, physical power that men exercise upon one another. An inglorious culmination had an origin that could be only grudgingly acknowledged. But it would be unjust to compare the disciplinary techniques with such inventions as the steam engine or Amici's microscope. They are much less; and yet, in a way, they are much more. If a historical equivalent or at least a point of comparison had to be found for them, it would be rather in the inquisitorial technique.

The eighteenth century invented the techniques of discipline and the examination, rather as the Middle Ages invented the judicial investigation. But it did so by quite different means. The investigation procedure, an old fiscal and administrative technique, had developed above all with the reorganization of the Church and the increase of the princely states in the twelfth and thirteenth centuries. At this time it permeated to a very large degree the jurisprudence first of the ecclesiastical courts, then of the lay courts. The investigation as an authoritarian search for a truth observed or attested time of many other technologies - agronomical, industrial, economic. But it must be recognized that, compared with the mining industries, the emerging chemical industries or methods of national accountancy, compared with the blast furnaces or the steam engine, panopticism has received little attention. It is regarded as not much more than a bizarre little utopia, a perverse dream - rather as though Bentham had been the Fourier of a police society, and the Phalanstery had taken on the form of the Panopticon. And yet this represented the abstract formula of a very real technology, that of individuals. There were many reasons why it received little praise; the most obvious is that the discourses to which it gave rise rarely acquired, except in the academic classifications, the status of sciences; but the real reason is no doubt that the power that it operates and which it augments is a direct, physical power that men exercise upon one another. An inglorious culmination had an origin that could be only grudgingly acknowledged. But it would be unjust to compare the disciplinary techniques with such inventions as the steam engine or Amici's microscope. They are much less; and yet, in a way, they are much more. If a historical equivalent or at least a point of comparison had to be found for them, it would be rather in the inquisitorial technique.

The extension of the disciplinary methods is inscribed in a broad historical process: the development at about the same time of many other technologies - agronomical, industrial, economic. But it must be recognized that, compared with the mining industries, the emerging chemical industries or methods of national accountancy, compared with the blast furnaces or the steam engine, panopticism has received little attention. It is regarded as not much more than a bizarre little utopia, a perverse dream - rather as though Bentham had been the Fourier of a police society, and the Phalanstery had taken on the form of the Panopticon. And yet this represented the abstract formula of a very real technology, that of individuals. There were many reasons why it received little praise; the most obvious is that the discourses to which it gave rise rarely acquired, except in the academic classifications, the status of sciences; but the real reason is no doubt that the power that it operates and which it augments is a direct, physical power that men exercise upon one another. An inglorious culmination had an origin that could be only grudgingly acknowledged. But it would be unjust to compare the disciplinary techniques with such inventions as the steam engine or Amici's microscope. They are much less; and yet, in a way, they are much more. If a historical equivalent or at least a point of comparison had to be found for them, it would be rather in the inquisitorial technique.
century, have their technical matrix in the petty, malicious minutiae of the disciplines and their investigations. These investigations are perhaps to psychology, psychiatry, pedagogy, criminology, and so many other strange sciences, what the terrible power of investigation was to the calm knowledge of the animals, the plants or the earth. Another power, another knowledge. On the threshold of the classical age, Bacon, lawyer and statesman, tried to develop a methodology of investigation for the empirical sciences. What Great Observer will produce the methodology of examination for the human sciences? Unless, of course, such a thing is not possible. For, although it is true that, in becoming a technique for the empirical sciences, the investigation has detached itself from the inquisitorial procedure, in which it was historically rooted, the examination has remained extremely close to the disciplinary power that shaped it. It has always been and still is an intrinsic element of the disciplines. Of course it seems to have undergone a speculative purification by integrating itself with such sciences as psychology and psychiatry. And, in effect, its appearance in the form of tests, interviews, interrogations and consultations is apparently in order to rectify the mechanisms of discipline: educational psychology is supposed to correct the rigours of the school, just as the medical or psychiatric interview is supposed to rectify the effects of the discipline of work. But we must not be misled; these techniques merely refer individuals from one disciplinary authority to another, and they reproduce, in a concentrated or formalized form, the schema of power-knowledge proper to each discipline (on this subject, cf. Tort). The great investigation that gave rise to the sciences of nature has become detached from its politico-juridical model; the examination, on the other hand, is still caught up in disciplinary technology.

In the Middle Ages, the procedure of investigation gradually superseded the old accusatory justice, by a process initiated from above; the disciplinary technique, on the other hand, insidiously and as if from below, has invaded a penal justice that is still, in principle, inquisitorial. All the great movements of extension that characterize modern penalty - the problematization of the criminal behind his crime, the concern with a punishment that is a correction, a therapy, a normalization, the division of the act of judgement between various authorities that are supposed to measure, assess, diagnose, cure, transform individuals - all this betrays the penetration of the disciplinary examination into the judicial inquisition.

What is now imposed on penal justice as its point of application, its 'useful' object, will no longer be the body of the guilty man set up against the body of the king; nor will it be the juridical subject of an ideal contract; it will be the disciplinary individual. The extreme point of penal justice under the Ancien Regime was the infinite segmentation of the body of the regicide: a manifestation of the strongest power over the body of the greatest criminal, whose total destruction made the crime explode into its truth. The ideal point of penalty today would be an indefinite discipline: an interrogation without end, an investigation that would be extended without limit to a meticulous and ever more analytical observation, a judgement that would at the same time be the constitution of a file that was never closed, the calculated leniency of a penalty that would be interlaced with the ruthless curiosity of an examination, a procedure that would be at the same time the permanent measure of a gap in relation to an inaccessible norm and the asymptotic movement that strives to meet in infinity. The public execution was the logical culmination of a procedure governed by the Inquisition. The practice of placing individuals under 'observation' is a natural extension of a justice imbued with disciplinary methods and examination procedures. Is it surprising that the cellular prison, with its regular chronologies, forced labour, its authorities of surveillance and registration, its experts in normality, who continue and multiply the functions of the judge, should have become the modern instrument of penalty? Is it surprising that prisons resemble factories, schools, barracks, hospitals, which all resemble prisons?
Additional pictures from the original French edition: http://monarch.gsu.edu/jcrampton/foucault/foucault_dp.html
He [Father Olbés] sent for the husband and he asked him why his wife hadn't borne children. The Indian pointed to the sky . . . to signify that only God knew the cause . . . asked through the interpreter if he slept with his wife, to which the Indian said yes. Then the father had them placed in a room together so that they would perform coitus in his presence. The Indian refused, but they forced him to show him his penis in order to affirm that he had it in good order. The father next brought the wife and had . . . her enter another room in order to examine her reproductive parts.

—David E. Stannard, American Holocaust

The focus of surveillance studies has generally been on the modern, bureaucratic state. And yet, as David Stannard's (1992) account of the sexual surveillance of indigenous peoples within the Spanish mission system in the Americas demonstrates, the history of patriarchal and colonialist surveillance in this continent is much longer. The traditional account of surveillance studies tends to occlude the manner in which the settler state is foundationally built on surveillance. Because surveillance studies focuses on the modern, bureaucratic state, it has failed to account for the gendered colonial history of surveillance. Consequently, the strategies for addressing surveillance do not question the state itself, but rather seek to modify the extent to which and the manner in which the state
surveils. As Mark Rifkin (2011) and Scott Morgensen (2011) additionally demonstrate, the sexual surveillance of native peoples was a key strategy by which native peoples were rendered manageable populations within the colonial state. One would think that an anticolonial feminist analysis would be central to the field of surveillance studies. Yet, ironically, it is this focus on the modern state that often obfuscates the settler colonialist underpinning of technologies of surveillance. I explore how a feminist surveillance-studies focus on gendered colonial violence reshapes the field by bringing into view that which cannot be seen: the surveillance strategies that have effected indigenous disappearance in order to establish the settler state itself. In particular, a focus on gendered settler colonialism foregrounds how surveillance is not simply about “seeing” but about “not-seeing” the settler state.

**Surveillance and the Biopolitical Modern State**

David Lyon (2007) defines surveillance as follows.

> For the sake of argument, we may start by saying that it is the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction. Surveillance directs its attention in the end to individuals (even though aggregate data, such as those available in the public domain, may be used to build up a background picture). It is focused. By systematic, I mean that this attention to personal details is not random, occasional or spontaneous; it is deliberate and depends on certain protocols and techniques. Beyond this, surveillance is routine; it occurs as a “normal” part of everyday life in all societies. (14)

The field of surveillance studies is important, Lyon argues, because of the “rapidly increasing influence of surveillance in our daily lives and in the operation of very large-scale operations” (ibid., 9). The growth in surveillance is often tied to Foucauldian notions of the rise of the disciplinary society and the ascendancy of biopolitics in which peoples become populations to be counted, measured, and regulated in order to promote the life of the normalizing state. Because certain populations are deemed threats to the normalizing state, they must be constantly monitored, and thus are subject to what Ruth Wilson Gilmore (2007) defines as “premature death” in order to preserve the body of the whole. And yet Foucault notes that, ironically, these biopolitical moves were first prac-
ticed on the bourgeoisie themselves. Through the disciplining of the bourgeois body, the "normal" body is defined as the measure by which all other bodies are marked as "deviant" (Foucault 1980, 123). Logics of normalization must have some pretense to universality even as these normalizing strategies are not evenly applied. Thus, it is no surprise that these disciplinary techniques come to be used broadly, not just on those populations deemed to be threats.

The Temporality of Settler Colonial Biopolitics

As noted by many critical-race- and ethnic-studies scholars, the manner in which Foucauldian analyses of the state tend to temporally situate biopower during the era of the modern state disappears the biopolitics of settler colonialism and transatlantic slavery. Alexander Weheliye (2014) points out that Foucault's conception of a complicated biopower is juxtaposed against a simpler "ordinary racism" (Foucault 1997, 128). As Foucault asserts, "I am certainly not saying that racism was invented at this time. It had already been in existence for a very long time. But I think it functioned elsewhere" (ibid., 254). Relegated to both a theoretical and geotemporal "elsewhere," Foucault then provides no elaboration on the nature of this "other" racism." As Weheliye (2014) argues, when biopower is rendered as the real racism, whose apex can be found in Nazi Germany, indigenous genocide, slavery, and colonialism disappear into given forms of simple racism that require no account of their logics. Similarly, Achille Mbembe argues that the mechanics of Nazi Germany are not fundamentally different from the "necropolitics" of the colony or the plantation in which "'peace' is more likely to take on the face of a 'war without end'" (2003, 23). Denise Ferreira da Silva's germinal text, Toward a Global Idea of Race (2007), also demonstrates that these forms of racism precede the modern state as Western epistemology is itself fundamentally a racial project. A focus on biopolitical racism as it is tied to the modern state thus often occludes analysis of the racial logics of settler colonialism and plantation slavery.

Surveillance studies's focus on the modern state similarly hides an analysis of the settler colonialist and white supremacist logics of surveillance that precede the ascendancy of the modern state. Furthermore, attention to these colonial and white supremacist logics of surveillance require a feminist analysis, since colonialism and white supremacy are structured by heteropatriarchy. For instance, Mark Rifkin's When Did Indi-
ans Become Straight? and Scott Morgensen’s Spaces Between Us call attention to the heteropatriarchal nature of colonial bio/necropolitics. That is, the shift from categorizing native peoples within the U.S. polity according to their membership in distinct nations to lumping them together under the racial category of “Indian” is often understood as a colonial tactic. But what Rifkin and Morgensen demonstrate is that this categorization is dependent on heteronormativity. Since they pose a threat to the colonial order, native nations are broken up into heteronormative individual family units in order to facilitate their absorption into the colonial state. This absorption occurs through a colonialist surveillance strategy by which the sexual and gender identities of native peoples must be constantly marked and policed. Through this surveillance, native peoples become racialized “Indians” who are managed through the politics of biopower (Rifkin 2011). Of course, as racialized subjects, native nations still constitute a threat to the well-being of the colonial state and hence are never properly heteronormative. The United States continues to be obsessed with solving the “Indian problem,” whether through boarding schools or land allotments. But Indianization, as it were, allows colonialism to become a population problem rather than a political problem (ibid.). Native nations are seen as sufficiently domesticated to be administered through government policy, rather than seen as a continuing political threat requiring ongoing military intervention.

In addition, as Driskill, Finley, Gilley, and Morgensen (2011) argue, native peoples are fundamentally “queered” under settler colonialism such that conquest is justified by their sexual perversity. Deemed “sodomites,” native peoples’ presumed sexual perversity justifies their genocide. Indigenous colonization is then achieved through sexual regulation, such as sexual acts of terror (the mass rapes of native peoples in massacres), as well as policies of normalization in which heteropatriarchy is instilled in native communities through allotment, boarding schools, and criminalization, among other contemporary forms of the surveillance and regulation of native peoples. As I have argued elsewhere, sexual violence was a primary colonial strategy by which native peoples were rendered inherently rapeable, and by extension their lands inherently invadeable, and their resources inherently extractable (A. Smith 2005a). Thus, contrary to Lyon’s assertion that “the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction” preceded the rise of the bureaucratic state, these strategies
were foundational to the settler state that required the gendered reclassification of the people from various indigenous nations into “Indians.”

As Patrick Wolfe (1999) notes, settler colonialism is a structure, not an event; that is, settler colonialism requires the continual disappearance of the indigenous peoples on whose land the settler state is situated (2). Consequently, these colonial heteropatriarchal logics continue. As Jacqui Alexander’s critique of the heteropatriarchal postcolonial state demonstrates, on one hand, the postcolonial state (or states that strive to be postcolonial) is imagined to be incapable of self-governance through its previously described presumed sexual perversity. It thus seeks to prove its ability to self-govern by continuing the colonial policing of supposed sexually perverse “nonprocreative noncitizens” within its borders to legitimate its claims to govern. In policing the gender and sexual boundaries of the nation-state by purifying it of imagined racialized and gendered contaminants, Alexander (2005) argues, the postcolonial state succeeds in obfuscating the permeability of its boundaries to multinational capital. This policing, structured under the logics of what Maria Josefina Saldaña-Portillo (2003) terms “aggrieved masculinity,” then serves to allay the anxiety of the postcolonial state and postcolonial aspirants in the wake of the postcolonial state’s feminization within the heteropatriarchal logics of global capital. While Lyon’s analysis points us to the surveillance strategies of the state, an anticolonial feminist analysis demonstrates that the problem is instead the state itself as surveillance strategy. Consequently, it is no surprise that states that have “decolonized” perpetuate the same surveillance strategies, because surveillance is structured into the logic of the state itself. That is, if we relocate the focus of surveillance studies from the bureaucratic state to the settler colonial, white supremacist, and heteropatriarchal state, we may then reformulate our analysis of surveillance.

In particular, I would like to foreground the focus of the field of surveillance studies on “seeing.” According to Lyon, “Surveillance studies is about seeing things and, more particularly, about seeing people” (2007, 1). The “watchful gaze,” as Lyon labels it, is what gives surveillance its “quintessential characteristic” (2007, 1). A focus on gendered settler colonialism would instead foreground how surveillance is about a simultaneous seeing and not-seeing. That is, the purposeful gaze of the state on some things and peoples serves the purpose of simultaneously making some hypervisible through surveillance while making others invisible. The colo-
nial gaze that surveils native communities to monitor, measure, and ac-
count for their “dysfunctional” behaviors conceals from view the settler
colonial state that creates these conditions in the first place. A feminist
surveillance studies focus on gendered colonial violence highlights that
which cannot be seen—indigenous disappearance.

The Settler Surveillance Strategies of Not-Seeing

Settler colonialism fundamentally relies on a logic of not-seeing. In par-
ticular, on a not-seeing of the indigenous people’s lands in order to allow
their colonial takeover. Terra nullius, the legal justification used for the
expropriation of indigenous land in Australia and elsewhere—or to use
the Zionist justification for Palestinian expulsion, “a land without a
people for a people without a land”—is premised on the not-seeing of
peoples already there. Within the United States, this expropriation relied
on the “doctrine of discovery.” As outlined in the case Johnson v. McIntosh
(1823), “Discovery is the foundation of title, in European nations, and
this overlooks all proprietary rights in the natives.” “Discovery” neces-
sarily rests on the absence of native peoples, who would otherwise be
the actual “discoverers” of their lands. And, as Robert Williams (2005)
notes, U.S. jurisprudence has never renounced the doctrine of discovery
on which Indian case law is based. Consequently, the colonial project is a
somewhat precarious project of disappearing the peoples that it cannot
see—a genocide that must disavow itself. As Sarita See argues, “If the
history of the American empire is defined by forgetting, its aesthetic is
structured by double disavowal. According to the New World aesthetic,
it seems possible to erase the erasure of the past” (2009, 66). Thus, the
strategies of surveillance are always simultaneously not just about what
can be seen, but about disappearing from view that which delegitimizes
the state itself. What must not be seen is not only the peoples themselves,
but the forms of governance and ways of life that they represent.

Gender violence is a central strategy of settler colonialism and white
supremacy. Colonizers did not just kill off indigenous peoples in this land:
native massacres were always accompanied by sexual mutilation and rape.
The goal of colonialism is not just to kill colonized peoples, but to destroy
their sense of being people (A. Smith 2005a). The generally nonpatriar-
chal and nonhierarchical nature of many native communities posed a
threat to European patriarchal societies. Consequently, when colonists
first came to this land, they saw the necessity of instilling patriarchy in

26  Andrea Smith
native communities, for they realized that indigenous peoples would not accept colonial domination if their own indigenous societies were not structured on the basis of social hierarchies. Patriarchy rests on a gender-binary system; hence, it is no coincidence that colonizers also targeted indigenous peoples who did not fit within this binary model. Gender violence thus inscribed patriarchy onto the bodies of native peoples, naturalizing social hierarchies and colonial domination.

The imposition of heteropatriarchy serves not only to secure colonial domination for indigenous peoples, but also to secure patriarchy within the colonizing society against the threats of the alternative governance structures that indigenous societies represent. It is noteworthy that the high status of women and the relatively peaceful nature of many native societies did not escape the notice of white peoples, in particular of white women (A. Smith 2005b). A society based on domination, hierarchy, and violence works only when it seems natural or inevitable. Given an alternative, peoples will generally choose not to live under violent conditions. The demonization of native societies, as well as their resulting destruction, was necessary to securing the “inevitability” of patriarchy within colonial societies. Again, the colonialist surveillance of native bodies served the simultaneous purposes of making them visible to the state while at the same time making invisible the threat to the settler state posed by indigenous governance.

To further remove the threats that indigenous governance systems posed to settler societies, the problem resulting from this colonial disease was relocated from a patriarchal and violent settler state to the “Indian” problem. As Wolfe (1999) notes, the more gender-equalitarian nature of some indigenous societies became anthropologically marked as the sign of their unevolved, premodern status. By adopting patriarchy, colonialists speculated, native peoples might evolve toward “humanity” and “civilization.” Native peoples were to be bureaucratically managed through allotment processes, church- and government-run boarding schools, and government-run health programs, among other strategies to facilitate their ascension to humanity. While courts often held that native peoples were potential citizens with the right to vote—unlike African Americans in the antebellum period—such potential could be realized, from the colonialist perspective, only when those peoples mature out of their status as native. In addition, native peoples were generally assigned the legal status of children, deemed legally incompetent to handle their own affairs and thus legally marked as “nonworkers.” Native
peoples’ pathway to citizenship thus depended on their maturation into adult (i.e., white) workers. Thus, native peoples’ acquisition of citizenship and voting rights was framed as a reward for proving their ability to work.

In 1887 the Dawes Allotment Act divided native lands into individual allotments of 80–160 acres. The federal government then expropriated the remaining surplus lands. Native peoples were given fees in trust for twenty-five years, until deemed “competent” by the secretary of the interior. They could then obtain fee patents enabling them to sell their lands. The rationale for this policy was that the practice of communal land ownership among native peoples was discouraging them from working the land. In the 1887 Indian commissioner’s report, J. D. C. Atkins explains the need for allotment:

Take the most prosperous and energetic community in the most enterprising section of our country—New England; give them their lands in common, furnish them annuities of food and clothing, send them teachers to teach their children, preachers to preach the gospel, farmers to till their lands, and physicians to heal their sick, and I predict that in a few years, a generation or two at most, their manhood would be smothered. . . .

This pauperizing policy above outlined was, however, to some extent necessary at the beginning of our efforts to civilize the savage Indian. He was taken a hostile barbarian, his tomahawk red with the blood of the pioneer; he was too wild to know any of the arts of civilization. . . . Hence some such policy had to resort to settle the nomadic Indian and place him under control. This policy was a tentative one. . . . Now, as fast as any tribe becomes sufficiently civilized and can be turned loose and put upon its own footing, it should be done. Agriculture and education will gradually do this work and finally enable the Government to leave the Indian to stand alone. (Report of the Secretary of the Interior 1887, n.p.)

The report warns that allotment will not work overnight: “Idleness, improvidence, ignorance, and superstition cannot by law be transformed into industry, thrift, intelligence, and Christianity speedily” (ibid., 4). Consequently, surveillance practices were essential, in order to instill normalizing discipline as a means to forcibly absorb native peoples into the colonial state. This pathway toward civilization required native peoples to adapt to a capitalist work model. The commissioner’s report further explained how work could save native peoples from barbarism.
It must be apparent . . . that the system of gathering the Indians in bands or tribes on reservations[,] . . . thus relieving them of the necessity of labor, never will and never can civilize them. Labor is an essential element in producing civilization. . . . The greatest kindness the government can bestow upon the Indian is to teach him to labor for his own support, thus developing his true manhood, and, as a consequence, making him self-relying and self-supporting. (ibid., 6–7)

Thus, through the careful policing and monitoring of native social structures, it would be possible to save native peoples from themselves, as well as to absorb them into colonial whiteness.

Despite these colonial strategies, native peoples never seemed to attain humanity. Homi Bhabha (1997) and Edward Said (1994) argue that the colonization process involves partially assimilating the colonized in order to establish colonial rule. If the colonized group were to remain completely different from the colonists, it would implicitly challenge the supremacy of colonial rule, by introducing questions around whether the way colonizers live is the only way to live. Hence, in order to preserve the cultural ideals of the colonizers, the colonized had to resemble the colonists—but only partially, for if the colonized were to be completely assimilated, they would be equal to the colonists, and there would be no reason to continue to colonize them. In this way, the promised assimilation was never total or complete, which created a permanent colonial anxiety with respect to the indigenous peoples who were to be absorbed. As Kevin Bruyneel contends, advocacy for bestowing full citizenship on native peoples soon gave way to notions of a more qualified citizenship, as native peoples were deemed to be civilizing too slowly. Because of native peoples’ imposed ontological status as children, they were never considered mature enough to earn full independence from their colonial fathers (Bruyneel 2004, 3).

**Surveillance and Gender Violence**

The surveillance strategies employed to normalize native peoples—from the monitoring of sexual behavior in Indian boarding schools to the surveillance of land ownership through the Dawes Allotment Act—have never come to an end, even though colonial policymakers continually promise they will. The civilizing policies directed against native peoples have never seemed to succeed enough to justify dismantling them. Of
course, one indicator used to determine that native peoples are continuing to be a "problem" and are not sufficiently "civilized" is the high rate of gender violence within native communities. As Dian Million (2014) brilliantly notes, the U.S. government's funding of healing programs goes hand-in-hand with the imposition of neoliberal economic regimes on Indian communities. According to this logic, native communities do not deserve the right of self-determination because they are violent. Instead, under the guise of colonial paternalism, the state deems it necessary to carefully monitor and surveil the violence within native communities in order to once again save native peoples from themselves. Of course, in this constant "seeing" of violence within native communities, the state hides from view the fact that most such violence is a direct result of state policy. What must not get seen is the inherent violence of the state itself.

In one example of this dynamic, the Australian government declared a national emergency in the Northern Territory as a result of the publication of the Little Children Are Sacred report, which detailed the "problem" of child abuse in aboriginal communities in a manner similar to the way gender violence in native communities is framed in the United States (Povinelli 2011, 59). The government seized control of indigenous lands through military police action, instituted compulsory medical exams for children, and took control of the finances for all indigenous programs. Through this intense surveillance, native peoples could be monitored in terms of school attendance, purchasing choices, and medical practices. While the report itself made an effort not to blame child abuse on aboriginal "culture," it was used by the Australian government to identify aboriginal culture as the problem and thus to justify its surveillance practices. Through these surveillance strategies, the Australian government could "see" and hence surveil the problem of indigenous child abuse, yet it did not see that these abuses were themselves the result of gendered colonial policies, such as the government kidnapping of aboriginal children from their communities in order to place them in violent government schools (Manne 2004)—one example in which state abuse created child abuse as an epidemic problem in native communities. The only solution the state can "see" to ending gender and child abuse is the settler state. What cannot be seen is the fact that such violence is the result of state violence.

Similarly, many native activists who organize around sexual violence in native communities frame their activist work from a decolonization perspective, yet the solutions that emerge from that work usually result
in increased federal intervention in native communities, such as the recent Tribal Law and Order Act that was passed in the wake of Amnesty International’s report on sexual assault in Indian country, Maze of Injustice (K. Robertson 2012). Of course, native activists who engage in such policy work are not ignorant of the risks of advocating for changes in federal policies (Smith 2005b). They are aware of the contradiction of trying to further the long-term project of decolonization while attempting to secure some measure of safety for survivors of violence in the short term. They constantly struggle with the question of whether relying on state surveillance even as a short-term solution to violence diminishes the possibilities of developing alternative strategies which refuse settler colonial logics in the long term.

It is important to note that the apparatus of settler colonial surveillance does not impact only native peoples. The “normalizing” society must necessarily inflict the logics of normalization on all peoples, not just on those who are “oppressed.” If it were only the oppressed who were subjected to normalizing logics, the logics would not seem “normal.” This is why the intent of genocide is not just to destroy native peoples, but to eliminate alternatives to the settler state for nonnative peoples. If alternatives to the white supremacist, capitalist, heteropatriarchal settler state were to persist, the settler state’s status as the prototype for normal would be at risk. Settler logics inform both how violence against native women is addressed, as well as how gender violence in general is addressed. Furthermore, the mainstream antiviolence movement relies on a settler framework for combating violence in ways that make it complicit in the state’s surveillance strategies. These strategies then inform how the mainstream movement manages and “sees” gender violence, while simultaneously preventing it from seeing other approaches to ending violence. For example, at an antiviolence conference I attended, the participants supported the war in Afghanistan because they believed it would liberate women from the violence of the Taliban; their reliance on state-driven surveillance strategies for addressing violence through the military and criminal-justice systems prevented them from seeing that militarism itself perpetuates violence against women.

One of the reasons for the antiviolence movement’s investment in the state derives from its concerns with the private sphere. As Lyon notes, much of the focus of surveillance studies is on “privacy” — how the state monitors the individual lives of peoples. Of course, as feminist scholars argue, the assumption that the protection of privacy is an unmediated
good is problematic, since the private sphere is where women are gener-
ally subjected to violence. And, as feminists of color in particular have
noted, not all women are equally entitled to privacy. Saidiya Hartman
points out that, on the one hand, the abuse and enslavement of African
Americans was often marked as taking place in the private sphere and
hence beyond the reach of the state to correct. And yet, paradoxically, the
private space of black families was seen as an extension of the workplace
and hence subject to police power (Hartman 1997, 160, 173). Anannya
Bhattacharjee similarly recounts an incident in which a domestic worker
complained to her social-justice organization that she was being abused
by her white employer. When Bhattacharjee on behalf of the organization
contacted the police to report the incident, she was told that “if her orga-
nization tried to intervene by rescuing this person, that would be trespas-
sing: In this case, the privacy of these wealthy employers’ home was
held to be inviolate, while the plight of an immigrant worker being held
in a condition of involuntary servitude was not serious enough to merit
police action. . . . The supposed privacy and sanctity of the home is a rela-
tive concept, whose application is heavily conditioned by racial and eco-
nomic status” (Bhattacharjee 2000, 29). As Patricia Allard notes, women
of color who receive public assistance are not generally deemed worthy of
privacy—they are subjected to the constant surveillance of the state. Of
course, all women seeking public services can be surveilled, but welfare is
generally racialized in the public imaginary through the figure of the “wel-
fare queen.” Andrea Ritchie (2006), Anannya Bhattacharjee (2001), and
other scholars document how women of color, particularly those who are
non-gender conforming, who seek police intervention in cases of domes-
tic violence often find themselves subject to sexual assault, murder, and
other forms of police-inflicted brutality.

If the private sphere is not a place of safety and refuge, what then
becomes the source of protection from violence in the home? The anti-
vio1ence movement has generally relied on the state. As a result, there
is often a disconnect between racial-justice and gender-justice groups.
Racial-justice groups focus on the state as an agent of violence from
which they need protection. Largely white antiviolence groups, and for
that matter, many women-of-color groups, have seen the state as the
solution to addressing intercommunal gender violence (Ritchie 1996).
As Bhattacharjee (2000) notes, this has put antiviolence groups in the
problematic position of marching against police brutality while simulta-
neously calling on the police to solve the problem of sexual/domestic vio-
lence as if it were two different institutions. As one example, I attended a meeting of tribally based antiviolence advocates who were discussing the need to address gender violence from the perspective of tribal sovereignty, and when the time came to develop actual strategies for addressing violence, the response was to call for more FBI agents on the reservation. Gender violence thus stands as the exception to the rule of opposing state surveillance. In this setup, the state becomes the solution to violence, so antiviolence programs must adopt the surveillance strategies of the state when they provide services. For instance, many domestic-violence shelters screen out women who are not documented, who have criminal histories, who are sex workers, or who have substance-abuse issues. One advocate told me that her program did background searches on potential clients and had them arrested if they had any outstanding warrants! This, despite the fact that these women have warrants out for their abusers and are trying to escape abusers who have forced them into criminal activity. Moreover, shelters are often run like prisons. As Emi Koyama brilliantly notes, women in shelters are constantly surveilled to make sure they conform to the behavior deemed fitting by the shelter staff. Koyama describes her experience in a shelter.

I am a survivor of domestic violence. I am someone who has stayed in a shelter, back in 1994. My experience there was horrendous; I constantly felt the policing gaze of shelter workers across the half-open door, and feared “warnings” and punishments that seemed to be issued arbitrarily. No, to describe the practice as “arbitrary” would be inaccurate; it was clearly selective in terms of who gets them most frequently: the poor Black and Latina women with children, especially if they are in “recovery” from alcohol or drug “abuse.” Snitching on other residents was actively encouraged: residents were rewarded for reporting rule violations of other residents and their children, even when the allegations were not exactly accurate. I did not know whom to trust. Eventually, the feeling of constant siege by shelter staff and all the “crazymaking” interactions pushed me over the edge, and I cut myself with a knife. Not surprisingly, they put me in a mental hospital, effectively ending my stay at the shelter before I could find a permanent, safer space to live.

Eventually, Koyama became involved in the antiviolence movement, where she worked for a shelter and found herself, against her politics, sometimes engaging in the same policing activities. When a woman who
spoke Arabic called the shelter asking for services, Koyama’s supervisor told her to tell the survivor that she needed to find another shelter. Koyama complied.

This episode marked my last day working at the domestic violence shelter, which is more than two years ago now, but I continue to ache from this experience. Of course, this was not the first time that I questioned how shelters were being run. I questioned everything: its “clean and sober” policy regarding substance use, its policy against allowing women to monitor their own medications, its use of threats and intimidations to control survivors, its labeling of ordinary disagreements or legitimate complaints as “disrespectful communication,” its patronizing “life skills” and “parenting” classes, its seemingly random enforcement of rules that somehow always push women of color out of the shelter first. I hated just about everything that went on in a shelter, and I refused to participate in most of these. I never issued formal “warnings” against any of the residents, preferring instead to have dialogs about any problems as casually as possible. I pretended that I did not smell the alcohol in the women’s breaths so long as their behaviors did not cause any problems for other residents. I never ever walked a woman to the bathroom and watched her as she peed into a little cup for drug tests, as the shelter policy expected of me to do. I did everything I could to sabotage the system I viewed as abusive: I was disloyal. But in many other situations, I failed. To this day, I ask myself why I did not simply ignore my supervisor’s order on that day, let the woman come to the shelter and deal with the consequences later. (Koyama 2006, 215)

Essentially, shelter staff take on the role of abusers or prison guards in the lives of survivors.

Women-of-color advocates are in the difficult position of trying to dismantle the structures of settler colonialism and white supremacy in the long term, while securing safety for survivors of violence in the short term. Under these conditions of immediate threat, women of color will often become preoccupied with addressing immediate short-term crises. In addition, these state-driven surveillance strategies for addressing violence force us to see violence in specific ways that foreclose the possibility of seeing violence in other ways. In particular, these strategies frame survivors of violence as themselves the problem: survivors are “sick” and require healing from a professional who will monitor their behavior to
ensure that they are healing properly. Those who do not “heal” are no longer deemed worthy of this “antiviolence” project. Thus, by seeing gender violence through the lens of the state, we can only see survivors as clients who need services, rather than as potential organizers who might dismantle social structures of violence.

Indigenous feminism reshapes the manner in which we engage surveillance studies, demonstrating that focus on the surveillance strategies of the state obscure the fact that the state is itself a surveillance strategy. There is not a pure or benign state beyond its strategies of surveillance. Yet, the state, rather than being recognized for its complicity in gender violence, has become the institution promising to protect women from domestic and sexual violence by providing a provisional “sanctuary” of sorts from the now criminally defined “other” that is the perpetrator of gender violence (Richie 2000). As I have argued elsewhere (A. Smith 2005a), the state is largely responsible for introducing gender violence into indigenous communities as part of a colonial strategy that follows a logic of sexual violence. Gender violence becomes the mechanism by which U.S. colonialism is effectively and pervasively exerted on native nations (A. Smith 2005a). The complicity of the state in perpetrating gender violence in other communities of color, through slavery, prisons, and border patrol, is also well documented (Bhattacharjee 2001; Davis 2003, 1981; A. Smith 2005b).

The state actually has no interest in gender or racial justice, since state laws are often, in practice, used against the people they supposedly protect. For instance, the New York Times recently reported that the effects of the strengthened anti-domestic violence legislation is that battered women kill their abusive partners less frequently; however, batterers do not kill their partners less frequently, and this is more true in black than in white communities (Butterfield 2000). With mandatory arrest laws, police officers frequently arrest those being battered rather than batterers. Thus, laws passed to protect battered women are actually protecting their batterers! Many scholars have analyzed the ineffectiveness of the criminal-justice system in addressing gender violence, particularly against poor women, women of color, sex workers, and queer communities (Richie 1996; A. Smith 2005b; Sokoloff 2005). The mainstream antiviolence movement’s reliance on policies embedded in state violence to solve the problem of gender violence depends on what David Kazanjian (2003) refers to as the “colonizing trick”: the liberal myth that the United States was founded on democratic principles that have eroded through
post-9/11 policies, which obfuscates how the state was built on the pillars of capitalism, colonialism, and white supremacy.

Reliance on state surveillance prevents us from seeing other possibilities for ending violence, such as through communal organization that might be able to address violence more effectively. This is apparent in the mandate of much surveillance studies, which tends to focus on curtailing state surveillance without questioning the state itself. Consequently, this work does not explore possibilities for different forms of governance, ones not based on the logics of patriarchal and colonial surveillance. The work of indigenous activists to develop indigenous nations that are not based on the principles of domination, violence, and control cannot be seen—even by antiviolence activists (A. Smith 2008). An evocative example is an experience I had working with the group Incite! Women of Color Against Violence. I was conducting a workshop on community accountability. We were discussing the following question: if there was violence in your community, is there anything you could do that would not involve primarily working with the police? During this discussion, one woman stated that she lived in an apartment complex in which a man was battering his partner. She did not know what to do, because she did not trust the police, but she also did not want the abuse to continue. Her comment made me realize how much our reliance on the state has impacted not only survivors of violence but also people who might think to intervene. It did not occur to this woman—nor might it necessarily occur to many of us in a similar situation—to organize in the apartment complex to do something. The only potential interveners in this situation seems to be ourselves as individuals or the state. It seems like our only response is either a privatized response to violence or a communal one that is state-driven. The result is that not only do we not “see” other solutions to the problem of violence, but we also become absolved from having to see the violence in the first place. Essentially, the apparatus of state surveillance, which allows the state to see violence, absolves us from the responsibility of having to see it.

A feminist approach to surveillance studies highlights not only the strategies of the state, but how people have internalized these same strategies, and it asks us to rethink our investment in the state. Without this intervention, the state is presumed to be our protector; we should only modify the manner in which the state protects. For example, during a survey I conducted for the Department of Justice on tribal communities’ response to sexual assault, I found that most communities had
not developed a response, because they assumed the federal government was taking care of the problem. In fact, as Amnesty International later documented, the federal government very rarely prosecuted sexual assault crimes in Indian country (Amnesty International 2007). Because of an investment in the state, tribal governments had not invested in their own possibilities for addressing violence.

When one asks the question “What can I do?,” the answer is likely to call the police or to do nothing. But when one asks the question “What can we do?,” a whole range of other possibilities arises. In fact, groups around the country have asked that question and have developed a variety of community-accountability models that do not rely primarily on police involvement (Chen et al. 2011). Similarly, many native activists, such as Sarah Deer (2009), are active in organizing tribal communities to develop their own responses to sexual violence. Of course, all of these models have their own challenges. For example, will community-accountability models simply adopt the same strategies used by the state to address violence? How might these models develop without a romanticized notion of “community” that is not sexist, homophobic, or otherwise problematic—or the potentially problematic assumption that a “community” even exists in the first place? How might they address the immediate needs of survivors who may still require state intervention, even as they seek to eventually replace the state? These questions and others continue to inform the development of the community-accountability movement (Chen et al. 2011).

After 9/11, even radical scholars framed George Bush’s policies as an attack on the U.S. Constitution. According to Judith Butler, Bush’s policies were acts against “existing legal frameworks, civil, military, and international” (2004, 57). Amy Kaplan similarly describes Bush’s policies as rendering increasingly more peoples under U.S. jurisdiction as “less deserving of . . . constitutional rights” (2005, 853). Thus, Bush’s strategies were deemed a suspension of law. Progressive activists and scholars accused him of eroding U.S. democracy and civil liberties. Under this framework, progressives are called in to uphold the law, defend U.S. democracy, and protect civil liberties against “unconstitutional” actions. Surveillance studies often carries similar presumptions. That is, this field is concerned with the “rapidly increasing influence of surveillance in our daily lives and in the operation of very large-scale operations” (Lyon 2007, 9). It is concerned with what is presumed to be the increasing erosion of civil liberties and the loss of privacy that this surveillance entails. It takes the
state for granted, but is concerned that the state not overstep its proper boundaries. And yet, from the perspective of indigenous peoples, the eye of the state has always been genocidal, because the problem is not primarily the surveillance strategies of the state, but the state itself.

If we were to employ a settler colonial analytic, we would see the growth in surveillance strategies less as a threat to the democratic ideals of the United States than as a fulfillment of them. As these surveillance strategies grow, they impact everyone, not just native peoples, because the logic of settler colonialism structures the world for everyone. In particular, surveillance strategies not only allow the state to see certain things, but prevent us from seeing the state as the settler colonial, white supremacist, and heteropatriarchal formation that it is.

Notes

3. Lyon does note, “But privacy is both contested, and confined in its scope. Culturally and historically relative, privacy has limited relevance in some contexts” (2007, 19).
4. See, for example, Bhattacharjee 2001b; D. Roberts 1991.
5. Out of respect for person involved and in keeping with organizational confidentiality policies, Bhattacharjee does not give extended details of the incident.
6. Personal conversation, 12 February 2002. The advocate with whom I spoke does not wish to have her program identified.
7. Community-accountability models do not presume that we can expect to engage in “pure” strategies untainted by the current system. The goal is not to tell survivors that they can never call the police or engage the criminal-justice system. The question is not whether a survivor should call the police. The question is why we have given survivors no option but to call the police.
FEMINIST SURVEILLANCE STUDIES

RACHEL E. DUBROFSKY AND SHOSHANA AMIELLE MAGNET, EDITORS
NOTES ON SURVEILLANCE STUDIES
THROUGH THE DOOR OF NO RETURN

The door is a place, real, imaginary and imagined. As islands and dark continents are. It is a place which exists or existed. The door out of which Africans were captured, loaded onto ships heading for the New World. It was the door of a million exits multiplied. It is a door many of us wish never existed.

—DIONNE BRAND, A Map to the Door of No Return: Notes to Belonging

In early August 1785, English social reformer Jeremy Bentham set out from Brighton, England, destined for Krichëv, Russia. It was in Russia where Bentham would first conceive of the Panopticon in a series of letters “from Crecheff in White Russia, to a friend in England.” At one point during his journey, in an attempt to reach Constantinople, he embarked from Smyrna on a cramped Turkish caïque with “24 passengers on the deck, all Turks; besides 18 young Negresses (slaves) under the hatches.” Much of Bentham’s writings that addressed slavery were written before this voyage. In those texts he touches on such topics as sugar production, punishment, and abolition. Writing during the 1770s on “afflictive capital punishment,” that being when the degree of pain imposed upon the body surpasses that necessary to produce death, Bentham details the severe methods of torture and punishment reserved for “negro slaves” of the European colonies in the West Indies for the crime of rebellion, a crime so named, he writes,
"because they are the weakest, but which, if they were the strongest would be called an act of self-defense." While acknowledging Europe's desire for "sugar and coffee" and other crops produced through enslaved labor in the colonies, he suggests that when these goods are obtained by keeping people enslaved "in a state in which they cannot be kept but by the terror of such execution: are there any considerations of luxury or enjoyment that can counterbalance such evils?" On the terror of the codes that governed slave life in the West Indies, Bentham has this to say: "let the colonist reflect upon this: if such a code be necessary the colonies are a disgrace and an outrage on humanity; if not necessary, these laws are a disgrace to the colonists themselves." Bentham arrived in Krichëv in February 1786. One can only wonder if he thought of the terror of "capital punishment" and of the slave's "self-defense" when he came across those eighteen "young Negresses" held captive in the hatches of that cramped Turkish caique.

That somewhere along a journey that ends in The Panopticon; or, The Inspection House Jeremy Bentham traveled with "18 young Negresses (slaves)" guides me to question the ways that the captive black female body asks us to conceptualize the links between race, gender, slavery, and surveillance. In other words, how must we grapple with the Panopticon, with the knowledge that somewhere within the history of its formation are eighteen "young Negresses" held "under the hatches"? If Bentham's Panopticon depended on an exercise of power where the inspector sees everything while remaining unseen, how might the view from "under the hatches" be another site from which to conceptualize the operation of power? This chapter asks that we rethink the Panopticon (1786) through the plan of the slave ship Brooks (1789), as a way to link surveillance studies to black feminist scholarship.

The first section of this chapter offers an overview of the Panopticon, disciplinary power, and sovereign power. In the second section I discuss some of the ways that the Panopticon and panopticism have been put to use in theorizing surveillance, and in particular three analytical concepts derived from this model of social control: synopticon, banopticon, and postpanopticism. In the third section I discuss the plan of the slave ship. Following this, I examine surveillance technologies of slavery, such as advertisements for runaway slaves and the census, as well as a set of rules from the 1800s for the management of slaves on an East Texas plantation. I do this in order to understand how racializing surveillance functioned through these technologies. I end this chapter by looking to black feminist theorizing of sur-
veillance, including bell hooks on "talking back" (1989) and "black looks" (1992) and Patricia Hill Collins's concept of "controlling images" (2000) as a way to situate surveillance as both a discursive and a material practice. I also look to artist Robin Rhode's *Pan's Opticon* (2008) and artist Adrian Piper's video installation *What It's Like, What It Is #3* (1991), as these creative texts offer ways to understand black looks and talking back as oppositional practices that challenge the stereotyped representations of controlling images and their material effects. My use of Rhode's *Pan's Opticon* and Piper's *What It's Like, What It Is #3* is a way of drawing on black creative practices in order to articulate a critique of the surveillance of blackness. In this fashion, these works open up a way to think creatively about what happens if we center the conditions of blackness when we theorize surveillance.

Seeing without Being Seen: The Plan of the Panopticon

The Panopticon was conceived by Jeremy Bentham in 1786 and then amended and produced diagrammatically in 1791 with the assistance of English architect Willey Reveley. Bentham first came upon the idea through his brother Samuel, an engineer and naval architect who had envisioned the Panopticon as a model for workforce supervision. Pan, in Greek mythology, is the god of shepherds and flocks, the name derived from *painen*, meaning "pasture" and hinting at the root word of "pastoral," and in this way the prefix *pan-* gestures to pastoral power. Pastoral power is a power that is individualizing, beneficent, and "essentially exercised over a multiplicity in movement." Bentham imagined the Panopticon to be, as the name suggests, all-seeing and also polyvalent, meaning it could be put to use in any establishment where persons were to be kept under watch: prisons, schools, poorhouses, factories, hospitals, lazarettos, or quarantine stations. Or, as he wrote, "No matter how different, or even opposite the purpose: whether it be that of *punishing the incorrigible, guarding the insane, reforming the vicious, confining the suspected, employing the idle, maintaining the helpless, curing the sick, instructing the willing in any branch of industry, or training the rising race in the path of education.*" Of course, "the willing," "the idle," and the so-called rising race might be more able to leave this enclosure at will or by choice than "the suspected" or "the incorrigible." With this "seeing machine," the unverified few could watch the many and "the more constantly the persons to be inspected are under the eyes of the persons who should
inspect them, the more perfectly will the purpose of the establishment have
been attained.” This is control by design, where population management
and the transmission of knowledge about the subject could, as Bentham
explains, be achieved, “all by a simple idea of Architecture!”

The Panopticon's floor plan is this: a circular building where the prison­
ers would occupy cells situated along its circumference (figure 1.1). With the
inspector's lodge, or tower, at the center, his field of view is unobstructed:
at the back of each cell, a window, and in its front a type of iron grating
thin enough that it would enable the inspector to observe the goings-on
in the prisoner cells. The cells in the Panopticon make use of “protracted
partitions”—where the partitions extend beyond the iron grating that cov­
ers the front of the cell—so that communication between inmates is mini­
mized, and making for “lateral invisibility.” In this enclosed institution the
watched are separated from the watchers; the inspector's presence is un­
verifiable; and there is said to be no privacy for those that are subject to
this architecture of control. Security in the Panopticon, as Bentham asserts,
is achieved by way of small lamps, lit after dark and located outside each
window of the inspection tower, that worked to “extend to the night the
security of the day” through the use of reflectors. By employing mirrors in
this fashion, a blinding light was used as a means of preventing the prisoner
from knowing whether or not the inspection tower was occupied. Power,
in the Panopticon, is exercised by a “play of light,” as Michel Foucault put it;
and by “glance from center to periphery.” The inspection tower is
divided into quarters, by partitions formed by two diameters to the
circle, crossing each other at right angles. For these partitions the
thinnest materials might serve; and they might be made removable
at pleasure; the height, sufficient to prevent the prisoners seeing over
them from cells. Doors to these partitions, if left open at any time,
might produce the thorough light, to prevent this, divide each parti­
tion into two, at any part required, setting down the one-half at such
distance from the other as shall be equal to the aperture of a door.

With Bentham's plan for prison architecture, we can see how light, shad­
ows, mirrors, and walls are all employed in ways that are meant to engen­
der in many a prisoner a certain self-discipline under the threat of external
observation, as was its intended function. The Panopticon would allow for
a disciplinary exercise of power. Such exercises of power are not ones of
pomp and pageantry, like a queen's coronation, a state funeral, or a royal
wedding, or of the overt kind of spectacular violence that often accompanies sovereign power. Instead, in this instance, power is covert and achieved by a play of light.

If an act that is deemed criminal is an assault on the sovereign's power, an exercise of sovereign power is that which seeks to make the sovereign's surplus power plainly understood by all. It is spectacular and episodic, and functions “to make everyone aware,” often through ceremonial terror, “of the unrestrained presence of the sovereign.” This is a power exercised through excessive means and force, like the public execution of Damiens the regicide, the gruesome scene that opens Foucault's *Discipline and Punish: The Birth of the Prison* (1975). In 1757, Robert-Françoise Damiens was made to make the *amende honorable*, a symbolic apology for his crime.

---

against the sovereign. He was carted through the streets of Paris, France, holding a burning torch in one hand and his weapon of choice, a knife, in the other. Boiling resin, sulfur, wax, and oil were combined and poured into his open wounds, and he was drawn by horses, quartered, and eventually hacked apart for his attempt on the life of Louis XV, king of France. With onlookers surrounding, Damiens's body was burned and his ashes were "thrown to the winds."

Another, but less well-known, public execution took place twenty-three years before that of Damiens the regicide in Paris. This time it was in the French colony of Nouvelle-France, and it was a black woman who was subjected to this gruesome exercise of sovereign power. Marie-Joseph Angélique, a Portuguese-born enslaved black woman, was tried and convicted of setting a fire that left much of the town of Montréal in ruins in 1734, the arson itself ruled to be an affront to that same sovereign that Damiens the regicide attempted to assassinate, King Louis XV. Angélique arrived in Montréal from New England after being sold to François Poulin de Francheville in 1725. After Francheville's death in 1733, his wife, Thérèse de Couagne, became Angélique's sole mistress, but through escape, insolence, unruliness, and talking back, Angélique was never quite fully under Madame Francheville's complete control. Madame Francheville would later make arrangements to sell Angélique for six hundred pounds of gunpowder. That sale was never fulfilled as, on the evening of April 10, 1734, a fire broke out on the roof of the Francheville home and Angélique was named the arsonist and arrested the morning after. Claude Thibault, a white indentured servant from France who was under contract to Madame Francheville, was named as Angélique's accomplice. Thibault was Angélique's lover. Angélique and Thibault had escaped from Montréal that previous winter, but were captured and returned. Days after the fire, Thibault disappeared and was never arrested. Angélique's trial lasted two months. Under interrogation she reportedly stated, "No one told me to set the fire. No one helped me, because I did not do it." Later, under repeated torture, she recanted that assertion of her innocence—"C'est moi. It's me and no one else. I want to die. C'est moi." Condemned to death, she was carted through the streets of Montréal, made to make the amende honorable with a burning torch held in her hand at the door of the town's parish, and hanged. Angélique's body hung in the street for all to observe for hours after her execution, was later burned and her ashes thrown to the winds, as was the ceremony prescribed for the capital punishment of an arsonist according to French law.
The ceremony of Angélique’s execution, according to Katherine McKitterick, achieved at least two things: “spectacular punishment of someone and something that is said not to exist,” that something being blackness in and of Canada as absented presence; and “the destroying of bodily evidence.” The trial and hanging of Angélique points to the criminalization of black women’s resistance to captivity. The will of the sovereign was violently inscribed in Angélique’s excruciating and spectacular death (both a public spectacle and spectacularly elaborate in its excessive violence) and made known for all who observed it—both free and enslaved—the expendability of slave life.

Foucault chose to begin “The Body of the Condemned,” the first chapter of Discipline and Punish, with the brutal public execution of Robert-Françoise Damiens in order to set up, in stark contrast, his discussion of the discrete and also distributed way that exercises of disciplinary power operate in the form of rules “for the House of young prisoners in Paris,” where regulation of the subject happened through observation and also through routines, repetition, self-discipline, and by following instructions and timetables. For example, the delinquent’s day would be structured like this: “Art. 18 Rising. At the first drum roll, the prisoners must rise and dress in silence, as the supervisor opens the cell doors”; “Art. 20. Work... They form into work teams and go off to work, which must begin at six in the summer and seven in the winter”; and “Art. 22. School. At twenty minutes to eleven, at the drum-roll, the prisoners form into ranks, and proceed in divisions to the school. The class lasts two hours and consists alternately of reading, writing, drawing and arithmetic.”

The rules for the management of delinquents came eighty years after the execution of Damiens. Foucault cites both the execution and the rules to say that “they each define a certain penal style” and mark the decline of punishment as a public spectacle. Disciplinary power did not do away with or supplant the majestic and often gruesome instantiations of sovereign power, however. Instead, at times, both formulations of power—sovereign and disciplinary—worked together. In reading punishment as public spectacle in the Old France and the New, I chose to recount the hanging of Marie-Joseph Angélique here because her torture and killing evidences blackness and slavery in Canada pre-Book of Negroes (1783), pre-Underground Railroad escape of black people from the United States to Canada (early nineteenth century), and pre-Confederation (1867). Putting the life of Marie-Joseph Angélique in conversation with the death of the regicide Robert-Françoise Damiens is
my way of interrupting Foucault's reading of discipline and the birth of the prison, as doing so points to an alternative archive from which to understand the hold of both disciplinary and sovereign power on black life under slavery. While Foucault argued that the decline of the spectacle of public torture as punishment might have marked "a slackening of the hold on the body," this chapter contends that when that body is black, the grip hardly loosened during slavery and continued post-Emancipation with, for example, the mob violence of lynching and other acts of racial terrorism.22

Panopticon, Panoptical, Panopticism:
A Critical Reinterpretation

Various surveillance studies theorists have employed the Panopticon as an analytical tool in order to question how social control operates on certain bodies and in certain spaces, as well as a way to conceptualize disciplinary power and the ways that it comes to be internalized by some. Some theorists of surveillance have used the metaphor of the Panopticon to generate other ways of conceptualizing surveillance. For example, Thomas Mathiesen's synopticon (1997) is a reversal of the panoptic schema where the many watch the few in a mass-mediated fashion (think here of the reality television show Big Brother, where a television audience, as well as an Internet-based one, observe "houseguests" as they compete for prizes by way of twenty-four-hour continuous camera feeds), or Didier Bigo's banopticon, where those whom the state abandons are often banned based on a racialization of risk. Bigo takes the view that the practice of profiling and categorizing some into risk categories and then "projecting them by generalization upon the potential behaviour of each individual pertaining to the risk category" is the disposition of U.S.-led security measures and practices, and increasingly so post-9/11.23 With the banopticon, certain groups and individuals are labeled as potentially dangerous. This labeling as dangerous is then massively applied to certain nations and their citizens and to those outside the bounds of citizenship, where anxieties and the anticipation of risk stemming from those deemed "dangerous minorities" then shape security measures at borders, on city streets, and other spaces that come to be associated with risk, or with being at risk of becoming risky. According to Bigo, the banopticon is "characterized by the exceptionalism of power (rules of emergency and their tendency to become permanent), by the
way it excludes certain groups in the name of their future potential behaviour (profiling) and by the way it normalizes the non-excluded through its production of normative imperatives, the most important of which is free movement."24 The banopticon might look like trusted traveler programs that speed up border crossings for preapproved travelers who provide some form of biometric-based verification, or free trade zones where goods can be manufactured, transported, imported, and exported without duties or other barriers to trade. The banopticon could also take the form of stop-and-frisk policing practices where categories of suspicion could include “furtive movements,” or “fits a relative description,” or “change direction at the sight of an officer,” or “inappropriate attire for season.”25

Some scholars have pointed to what they see as an apparent overreliance on the Panopticon in the field of surveillance studies that leaves the role of visibility overstated. Others have suggested that the Panopticon is no longer useful, or that at least as a way of theorizing disciplinary power in the contemporary moment it cannot offer a complete account of, for example, surveillance and exercises of power within social media and cell phone usage, or by way of digital information databases and data aggregators. On this point, Roy Boyne offers a critique of panopticism in which he contends that “post-Panoptical subjects reliably watch over themselves” without need of the physical structure of the Panopticon.26 He suggests that panopticism has been “transcended by the emergent practice of pre-visualization” where simulation, profiling, and prevention occur, rather than merely observation.27 Also, Boyne names the “reversal of the Panoptical polarity,” where the many watch the few, as operating in conjunction with the Panopticon, where the few watch the activities of the many, in this way echoing Thomas Mathiesen on the synopticon.28 John Gilliom and Torin Monahan, in their analysis of social media sites such as Facebook, argue that “rather than being a prisonlike panopticon where trapped people follow the rules because they’re afraid someone is watching, with Facebook and similar sites people are probably more afraid that no one is watching, that no one cares what they’re up to.”29 With this apparent fear of not being noticed, Gilliom and Monahan say that social media users “discipline themselves in a different way by divulging as much as possible about their lives and thoughts.”30 Other theories, like the “social sorting” of people and populations into categories of risk, are offered as a means of qualifying and understanding forms of surveillance that are sometimes overlooked. On the overrepresentation of the panopticon and accounts that take power as

Notes on Surveillance Studies 39
unilaterally exercised, Lyon writes that “not only does this kind of account distract attention from the subtle interplay between surveillance power and the attitudes and activities of those subject to surveillance, it also places all the emphasis on forms of rational control.” Likewise, Kevin Haggerty names the Panopticon as “oppressive,” not only because of an overreliance placed upon it as an explanatory metaphor in works that analyze surveillance, but also for the way “the panoptic model has become reified, directing scholarly attention to a select subset of attributes of surveillance,” which has resulted in the panoptic schema being applied in areas where it is, as he argues, “ill-suited, and important attributes of surveillance that cannot be neatly subsumed under the ‘panoptic’ rubric have been neglected.” One area of contention that Haggerty points to is the claim that in the panoptic schema, who, or what, does the watching is irrespective, or, as Foucault wrote, “Stones can make people docile and knowable.” For Haggerty, it is a mistake not to take into account the “attitudes, predispositions, biases, prejudices and personal idiosyncrasies” of those who do the surveillance for how these factors inform the “form, intensity and regularity” of their responses.

The very failure of panopticism to produce docile subjects is an important point of criticism, where, as Boyne puts it, “that failure is announced in many places: prison riots, asylum sub-cultures, ego survival in Gulag or concentration camp.” In her observation and interviews at intensive management units housed within prisons run by the Washington State Department of Corrections, Lorna Rhodes names aggressive behavior (throwing feces, urine, and other bodily fluids), passive behavior (such as refusals to eat), and self-harm as instances in which the body is used as a means of resistance, and she argues that these acts are expressions of inmates’ struggles with the panopticon. Intensive management units, or special housing units, are solitary confinement units where certain inmates are segregated from the general prison population, spending up to twenty-three hours a day in their individual cells. Prolonged isolation in solitary confinement for many leads to depression, hallucinations, and acts of self-mutilation.

While the prisoner’s body is “the very ground of the panoptical relation,” under such conditions, as Rhodes contends, “it is also its potential undoing; he has within himself the makings of a perverse opacity.” Rhodes cites Lyon here in her naming of this “perverse opacity,” a term that, as Lyon explains, points to the idea that such “resistance may not be liberatory—
Indeed, it invites further control—but it calls in question both the Panopticon and our representations of it.\textsuperscript{38} Like Rhodes and Lyon, Boyne also calls the Panopticon into question, but he advises us not to do away with it completely as a way to understand our contemporary condition. Instead, he suggests that we "draw a line through the terms Panopticon, Panoptical, Panopticism. To place these terms under erasure, drawing a black line through them, allowing the idea to be seen at the same time as denying its validity as description, could be the most honest resolution."\textsuperscript{39}

Unarguably the most cited work in surveillance studies on the Panopticon as a metaphor for disciplinary exercises of power is Foucault's \textit{Discipline and Punish: The Birth of the Prison}, first published in 1974 as \textit{Surveiller et punir: Naissance de la Prison}, with the book's French title alluding more closely to its focus on surveillance. In \textit{Discipline and Punish}, Foucault argues that "discipline makes individuals" and achieves its success by employing "simple instruments": hierarchical observation (the greater over lesser authority, whether through physical structures or choreographed gazes), normalizing judgment (quantitative measurements, comparisons, establishment and adherence to set rules and norms, exclusions), and the examination.\textsuperscript{40} Broadly, Foucault explains that hierarchical observation and normalizing judgment combine in the examination. Hierarchical observation works "as a piece of machinery" designed for "the uninterrupted play of calculated gazes."\textsuperscript{41} With this play of gazes in the disciplinary institution, such as the penitentiary or the school campus, surveillance "functioned like a microscope of conduct" and sought to objectify, transform, and improve individuals through architectural arrangements, registration, examination, and documentation.\textsuperscript{42} Foucault describes normalizing judgment as that which normalizes by singling out and correcting "that which does not measure up to the rule, that departs from it" with a glance, a gaze that classifies, ranks, and measures.\textsuperscript{43} So although disciplinary power is individualizing, by way of normalizing judgment, individual actions are referred "to a whole that is at once a field of comparison, a space of differentiation and the principle of a rule to be followed."\textsuperscript{44} The examination places the individual in a "network of writing" as it is "accompanied at the same time by a system of intense registration and of documentary accumulation."\textsuperscript{45} The examination in the disciplinary institution seeks to objectify and transform individuals through architectural arrangements, registration, and documentation.
Prefiguring Bentham’s design of the Panopticon and the seventeenth-and eighteenth-century disciplinary institutions that Foucault lays out in *Discipline and Punish*, the architectural design, registration, documentation, and examination at slave trafficking forts and ports, through the Door of No Return, and on slave ships during the Middle Passage voyage from Africa to the auction blocks and plantations of the New World were subject defining, but always violent. The violent regulation of blackness as spectacle and as disciplinary combined in the racializing surveillance of the slave system. On this point, Robyn Wiegman states that “the disciplinary power of race, in short, must be read as implicated in both specular and panoptic regimes.”

Here, black children, women, and men were subject to these “simple” but violent instruments—branding irons fashioned out of silver wire, ships’ registers in which African lives were recorded as units of cargo, or listed alongside livestock on slave auction notices, and census categories, estate records, and plantation inventories that catalogued enslaved people as merchandise. The branding of enslaved people as a means of accounting for a particular ship’s cargo, for example, was not only individualizing but also a “massifying” practice that constituted a new category of subject, blackness as saleable commodity in the Western Hemisphere. Plantation rules laid out for overseers the prescribed measures for regulating plantation life and “social death.”

In using Foucault’s schemas of sovereign power, discipline, and normalization, as well as the concept of panopticism, I am mindful of their limitations for theorizing the role of trauma, vulnerability, and violence in the making and marking of blackness as property. However, for the concept of racializing surveillance, Foucault’s contributions to understanding sovereign power and its “policy of terror” and to conceptualizing discipline and the imposition of norms, for example, offer us a way to understand how acts of making the black body legible as property were put to work in the production of the slave as vendable object to be bought, sold, and traded.

Complicating Foucault’s panopticism through the archive of slavery and black feminist scholarship on surveillance is a way of offering a critical reinterpretation of the concept—by “drawing a black line” through it. To do this I now turn to the plan of the slave ship. Drawing a line through panopticism by way of the slave ship is another means of interrupting Foucault’s reading of discipline, punishment, and the birth of the prison, because, as Marcus Rediker put it, the slave ship was “a mobile, seagoing prison at a time when the modern prison had not yet been established on land.”
Through its creative remembering of the brutalities of slavery and its afterlife, Caryl Phillips’s short story “The Cargo Rap” (1989) makes links between the Panopticon, captivity, the slave ship, plantation slavery, racism, and the contemporary carceral practices of the U.S. prison system. Racism is, as Ruth Wilson Gilmore explains, “the state-sanctioned or extralegal production and exploitation of group-differentiated vulnerability to premature death.”

Rudi (or sometimes “Rudy”) Leroy Williams, the protagonist of “The Cargo Rap,” was sentenced to prison at nineteen years of age for the attempted theft of forty dollars. Rudi narrates this slow, state-sanctioned death that is the “negative inheritance” of the slave’s progeny that Stephen Best and Saidiya Hartman alert us to: “the ongoing production of lives lived in intimate relation to premature death (whether civil, social or literal).”

Phillips writes “The Cargo Rap” in epistolary form—as a series of letters penned by Rudi, namely to family members and to his defense committee, over the course of eighteen months. In this way, “The Cargo Rap” follows George L. Jackson’s Blood in My Eye letters, written right before his death on August 21, 1971, in San Quentin State Prison in California. Like Rudi, Jackson was convicted and incarcerated for armed robbery, accused of stealing seventy dollars from a gas station while still a teenager in 1961. On Jackson’s sentence, Foucault had this to say: “ten years in prison for 70 dollars is a political experience—an experience of hostage, of a concentration camp, of class warfare, an experience of the colonized.” In one of his letters written in Soledad Prison on June 10, 1970, Jackson states that for the black man “being born a slave in a captive society and never experiencing any objective basis for expectation had the effect of preparing me for the progressively traumatic misfortunes that led so many black men to the prison gate. I was prepared for prison. It required only minor psychic adjustments.” Both Foucault and Jackson speak of incarceration as a condition of colonization and of captivity.

In “The Cargo Rap” letters, we witness Rudi make sense of the traumatic misfortunes of the world outside of his solitary confinement, where such prolonged isolation makes his life one of constant exposure to fluorescent
light and permanent illumination, living in "neither daytime nor night-time. It is no time," as he put it. To understand this constant and tortuous play of light on the body, Rudi asks his reader to "take a desk lamp and shine it into your face. Try to relax, think, act, concentrate, do everything in this position for twenty-four hours." In an attempt to cope with the deliberate disorientation of "no time," Rudi cultivates an ability to tell time by way of certain noises and silences, as some silences are "closer to dawn than others." Rudi tells of isolation, routinization, inspections, premature death, and the harmful toll of prison life: deteriorating eyesight, The Wretched of the Earth, a ten-by-four-foot cell, a body atrophied, and the suffering of brutalities at the hands of the prison guards. This is a type of corporeal violence that was reported to Loïc Wacquant in his study of the Los Angeles County Jail system as "getting the flashlight treatment," where after violent beatings at the hands of prison guards one would be able to "read the brand of their flashlight" on the prisoner's body. During Rudi's brief sojourn in the general prison population, he writes: "I can have darkness. My eyes can rest easy at night." He writes of his desperation to escape the "high-security barracoons" that holds him and of the travels and works of the black activists, writers, athletes, and artists that sustain him while living a slow-motion death in prison: Muhammad Ali, W. E. B. DuBois, Frantz Fanon, Marcus Garvey, Toussaint L'Ouverture, Paul Robeson, Harriet Tubman, Phillis Wheatley.

Readers of Phillips’s "The Cargo Rap" are not privy to the responses, if any, to Rudi's letters by his family members or his other correspondents. Instead, we are left only with Rudi's thoughts. His letters are, he writes, "a little cargo rap about the children of Africa who arrived in this country by crossing the water." Rudi's first letter is to his mother, Alice, a domestic worker. In it he writes on Darwinism and self-preservation and he relates how unthinkable it is for her to even imagine trading places with the wealthy white women who employ her to work in their homes. With each of his letters, the plantation metaphor becomes even more direct as Rudi's physical and mental conditions deteriorate further. Incarceration is a slow-motion death. Rudi's last letter is dated August 1968, in a year that saw the assassinations of both Martin Luther King Jr. and Robert F. Kennedy, the passing of the Fair Housing Act meant to end discrimination in housing in the United States, riots in over one hundred U.S. cities, student coalitions occupying buildings on university and college campuses demanding education reform, and the black-gloved fists raised in protest by Af-
American American track and field medalists John Carlos and Tommie Smith during their medal ceremony at the Summer Olympic Games in Mexico City. Rudi's last letter is addressed to his by-then-deceased mother. In it he writes, "the plantation is wide and stretches beyond the horizon... We toil from 'can't see' in the morning to 'can't see' at night. The master is cruel, but nobody 'knows' him better than his slaves. There is strength in this." By now disoriented from doing time under the deliberately disorienting conditions of "no time," in this letter Rudi inquires about the crops and tells of his capture by slavers and his hopes for return to Africa. In this plantation cum prison, he says, "Thirty feet above me a man sits on a watchtower with a rifle." This final letter speaks of loss, prison time management, plantation rules, the Panopticon's inspection tower, and survival of the Middle Passage's cargo hold.

I chose an excerpt from Dionne Brand's *A Map to the Door of No Return* as this chapter's epigraph to point to a symbolic moment and space of diaspora and belonging. This door, while located at La Maison des Esclaves (House of Slaves) museum on Goree Island, off the coast of Senegal, stands as a symbolic memorial of forced migrations that led to the mass vending of black people across the Atlantic Ocean. On it, Brand writes, "I think that Blacks in the Diaspora feel captive despite the patent freedom we experience, despite the fact that we are several hundred years away from the Door of No Return, despite the fact that the door does not exist." This captive feeling that Brand describes is one of the vestiges of unfinished emancipations. A key aim of this chapter is to question how what Bob Marley names "the Babylon system," and what Howard Winant situates as "the legacy and lessons of the Atlantic slave system," can help us to think about how blackness is often absented from surveillance studies. "Babylon System" is the fourth track from the album *Survival* by Bob Marley and the Wailers, which was released in 1979. In it, Marley sings of refusal, freedom, and rebellion, with lyrics like, "from the very day we left the shores" and "we've been taken for granted much too long." On the cover of the album is a schematic diagram of a slave ship with tiny figures meant to represent its human cargo. Superimposed on this diagram is the album's title, *Survival*. In 1789, the London Committee of the Society for Effecting the Abolition of the Slave Trade produced and distributed *Description of a Slave Ship* (figure 1.2). Unlike Bentham's blueprint of the Panopticon, this schematic diagram of a maritime prison is populated with tiny figures dressed in loincloths to represent the legally allotted amount of enslaved human cargo that the slave
vessel Brooks (often referred to as Brookes) could transport under the Dolben Act of 1788, an act that regulated slave carrying and overcrowding.

Some background regarding this plan is necessary here. The ship Brooks was built in 1781, commissioned by Liverpool-based slave merchant Joseph Brooks Jr. It was large as slave vessels go, weighing in at around 320 tons and at one point carrying 609 enslaved captives during a 1787 voyage from the Gold Coast of Africa to Kingston, Jamaica. It took its final voyage in 1804 to Montevideo, Uruguay, under Captain William Murdock, where over three hundred people disembarked as slaves after a sixty-two-
day voyage from West Africa. *Description of a Slave Ship* was fashioned by
the London Committee in the hope of making “an instantaneous impres­
sion of horror upon all who saw it.” A similar rendering of a slave ship was
produced in December 1788 by the Plymouth Committee of the Society
for Effecting the Abolition of the Slave Trade. Named the *Plan of an Af­
rican Ship’s lower Deck with Negroes stowed in the Proportion of only One to
a Ton*, this earlier version featured an overview of an African ship’s cargo
hold along with text that laid out the Plymouth Committee’s agenda, in­
cluding the demand that the “cruelty and inhumanity of this trade must be
universally admitted and lamented,” and advocated for “an end to a prac­
tice, which may, without exaggeration be stiled one of the greatest evils at
this day existing upon the earth.” Copies were circulated in and around
Plymouth, with some copies sent to the London Committee. By April 1789
the London Committee had produced their version, which featured seven
different views of the *Brooks*: a cutaway longitudinal view of the ship, cross
sections of the stern deck and midship, and an overview of the plan of the
lower deck with figures of the enslaved lying in a plank position, crammed
into all available space. In a later version, *Stowage of the British Slave Ship
“Brookes” under the Regulated Slave Trade Act of 1788*, the note for “Figure 3”
detailed this cramped configuration: “the stowage of 130 additional slaves
round the wings or sides of the lower deck by means of platforms or shelves
(in the manner of galleries in a church) the slaves stowed on the shelves or
below them have only a height of 2 feet 7 inches between the beams and far
less under the beams.” Two feet and seven inches. The violence of slavery
crude reduced to geometric units, with room allotted for forty women,
twenty-four boys, and sixty men, arranged in a “perfect barbarism,” as abo­
litionist Thomas Clarkson described this formation. This arrangement
was, as W. E. B. DuBois put it, “a foretaste of hell.” Slave trader Theodore
Canot outlined the stowing process:

> The second mate and boatswain descend into the hold, whip in hand,
and range the slaves in their regular places: those on the right side of
the vessel facing forward, and lying in each other’s lap, while those on
the left are similarly stowed with their faces towards the stern. In this
way each negro lies on his right side, which is considered preferable
for the action of the heart.”

Without such “strict discipline,” Canot wrote, “every negro would accom­
modate himself as if he were a passenger.” This spatial arrangement made
for a crushing asphyxia: "The men therefore, instead of lying on their backs, were placed, as is usual, in full ships, on their sides, or on each other. In which last situation they are not unfrequently found dead in the morning." The cargo hold is a slow-motion death. Some cheek-by-jowl, this crude arrangement made known that those crossing the Atlantic Ocean in this manner were not "passengers," as they were allotted "half the room afforded soldiers, emigrants or convicts on ships of the same period," but were instead to disembark, if alive, as slaves and as unfree. Rediker names the slave ship as "containing a war within," in which sailors and other crew would function as prison guards who "battled slaves (prisoners)" when attempts at insurrection and other types of resistance were made. Other forms of resistance to this shipping arrangement came by way of refusals to eat, suicides, with some accounts telling of captives rushing all at once to the leeward end of the vessel "in a gale of wind, on purpose to upset the ship, choosing rather to drown themselves" than be subject to a life in slavery. They died from "grief, rage and despair," C. L. R. James remarks in The Black Jacobins as he describes how some jumped overboard "uttering cries of triumph as they cleared the vessel and disappeared below the surface." Noted on one popular version of the Brooks diagram is this text:

The "Brookes" after the Regulation Act of 1788, was allowed to carry 454 Slaves, She could stow this number by following the rule adopted in this plate. Namely of allowing a space of 6 ft. by 1 ft. 4 in. to each man; 5 ft. 10 in. by 1 ft. 4 in. to each woman, & 5 ft. by 1 ft. 2 in. to each boy, but so much space as this was seldom allowed even after the Regulation Act. It was proved by the confession of the Slave Merchant that before the above Act the Brookes had at one time carried as many as 609 Slaves. This was done by taking some out of Irons & locking them spoonwise (to use the technical term) that is by stowing one within the distended legs of the other.

With women, men, girls, and boys locked spoonwise and segregated by age and sex, the production and containment of gendered difference is apparent. This stowage plan is what Hortense Spillers calls the making of "scaled inequalities." Such accounting and architectural practices highlight the scale of the violence and trauma of the Middle Passage, a passage so named as it formed the middle leg of a triangular journey (the Middle Passage was bracketed between the journey from Europe to Africa and that from the New World to Europe). The London Committee version, Description of a

48 CHAPTER 1
Slave Ship, states that the male cargo would be shackled at the ankles, “two by two; the right leg of one to the left leg of the other, and their hands are secured in the same manor,” while the figures representing women and children were, in that rendering, unshackled, but in closer proximity to the captain’s cabin. The London Committee noted, “The principal difference is in the men. It must be observed, that the men, from whom only insurrections are to be feared, are kept continually in irons, and must be stowed in the room allotted for them, which is of a more secure construction of the rest.” The plan then, in its various versions, highlights the gendering of sexual violence, while diagrammatically and textually absenting the possibilities of women’s leadership and resistance in insurrections, as “only insurrections are to be feared” from men.

The Brooks diagram, “in serving the cause of the injured African,” offers an overview of the stowage plan of the slave merchant’s ship and forces me to reflect on my own surveillance practices in reading the archive of transatlantic slavery. The slave ship schematic is clinical in its architectural logic and provides an almost aerial viewpoint, overlooking the tiny black figures set to represent the enslaved drawn “like so many cartoon figures,” as Spillers describes. What does it mean that I now look to this plan, but not from the elevated and seemingly detached manner as it was first intended to be looked upon? When the plan was first fashioned, this vantage point was meant to be that of the predominantly white and male abolitionists and lawmakers. I am reminded here of what Donna Haraway calls the “conquering gaze from nowhere,” a gaze that is always unmarked, and therefore already markedly white and male, and one that claims a power to “represent while escaping representation.” I am also reminded here of Frantz Fanon’s moment of awareness of a “racial epidermal schema” on that train in France and “battered by tom-toms” and “slave-ships” and “dissected under white eyes, the only real eyes,” when he says, “I took myself far off from my own presence, far indeed and made myself an object.” What this visual representation of the slave ship points to is the primacy given in these abolitionist texts to white gazes and vantage points to the trauma of slavery, where the tiny black figures are made to seem androgynous, interchangeable, and replicable. This is the “god-trick of seeing everything from nowhere,” and, as Haraway warns, “this eye fucks the world.” So it gets a little tricky when I do this looking, seemingly an aerial reconnaissance mission of the archive of surveillance and of slavery. In the versions of the Brooks diagram that were produced in the United States, the slave
ship plan as abolitionist text was made clear. A version published in the periodical *American Museum* in May 1789 noted that it was “published by order of the Pennsylvan­ia Society for promoting the abolition of slavery.” Capitalization of all letters in “abolition” served an express purpose here, from the call for an end to the transatlantic slave trade to one for the abolition of slavery itself. Further, in this version the making of premature death through the stowage arrangements was described in this manner: “and reduced nearly to the state of being buried alive, with just air enough to preserve a degree of life sufficient to make them sensible of all the hor­ror of their situation.” These conditions of premature death left many who traveled the Middle Passage as captives just on the cusp of survival. “Buried alive, with just air enough.” According to Rediker, the mortality rate onboard the *Brooks* was 11.7 percent, which was “high for its own day (average for British ships between 1775 and 1800 was 7.95 percent).” With a closer look at the *Description of a Slave Ship*, one can see that each of the tiny black figures are not replicas of each other; rather, some have variously crossed arms, different gestures, or seem to turn to face one another, while some stare and look back at the gaze from nowhere, and in so being the *Description of a Slave Ship* can also be understood as depicting black looks and the trauma of Middle Passage as multiply experienced and survived, and as hinting at the possible imaginings of what Omise’eke Natasha Tinsley terms “erotic resistance,” that being the same-sex relationships forged because of and in spite of this shipping arrangement, where the formation of such relationships—like the intimate bond of shipmates—itself was an act of resistance to “imperial desires for Africans’ living death.” Such re­sistance was a refusal of the Babylon system, or, as Bob Marley sings in “Babylon System”: “we refuse to be what you want us to be / we are what we are.”

Racializing Surveillance

The historical formation of surveillance is not outside of the historical formation of slavery. Using narratives of ex-slaves, runaway slave adver­tisements, the census, and a set of plantation rules as primary source data, what follows is a historicizing of some of the concepts and concerns that now shape the field of surveillance studies, approached by examining slave surveillance practices. The continuities that this archive reveals offer social
theorists, I argue, new ways of understanding surveillance in contemporary life.

**PLANTATIONS, PASSES, AND RUNAWAYS**

In the ten “General” and nineteen “Particular” rules for overseers recorded in the mid-nineteenth century by Charles William Tait for the governing of enslaved laborers on *Sylvania*, his 6,000-acre plantation in Columbus, Texas, Tait listed the prescribed methods for crop cultivation and clearing land, specified food rations, noted the daily schedule around meals and rest (“they must be ready to go to work by sunrise”), and detailed his punishment regime (“always attempt to govern by reason in the first instance and resort to force only when reason fails”), as well as postnatal procedures and back-to-work legislation for new mothers (“never require field-work of a woman, until the expiration of four weeks after confinement”). With the eighth general rule, Tait noted that “a regular and systematic plan of operation is greatly promotive of easy government. Have all matters therefore, as far as possible reduced to a system.” Tait’s directives on the managerial control of slaves demonstrate how disciplinary power operated by way of set rules, instructions, routines, inspection, hierarchical observation, the timetable, and the examination. The timetable, then, was a means of regimenting enslaved labor through repetition where there was an attempt to account for every moment of enslaved life: “always require the negroes to eat their breakfast before they go to work” and “every negro-cabin to be inspected every Sunday morning to see that it is kept clean. Every negro to appear in the field on Monday morning in clean clothes.” Tait’s fifteenth particular rule prescribed that “no profane or obscene language to be allowed among the negroes.” The seventh general rule on punishment was an explicit directive regarding the overseer’s performance that accompanied the punishment, as Tait wrote, “Never act in such a way as to leave the impression on the mind of the negro that you take pleasure in his punishment, your manner should indicate that his punishment is painful.” So the prescribed punishment must be performed as a pain experienced by the overseer, who is not to express the possibility of pleasure taken in performing acts of violence. That a rule needed to be put in place in order to prevent such displays of violent delight should leave us to question the rates at which such pleasure was really expressed when, as Saidiya Hartman tells us, plantation practices sought to “make discipline a pleasure, and vice versa.” Importantly, this rule shows that for Tait, this pained perfor-
mance by the overseer was a suffering that was meant to be remembered in the mind of the punished. Overseers were instructed by Tait's ninth general rule that "Negroes lack the motive of self-interest to make them careful and diligent," so in order to incentivize enslaved workers, "do not therefore notice too many small omissions of duty." What Tait's rules for overseers also make known is that plantation surveillance was an exercise of both sovereign power and racialized disciplinary power, working simultaneously, discretionarily, and in a prescribed fashion, as both were put to use in plantation societies to render slave life expendable.

In Tait's rules for what he called the "easy government" of his East Texas plantation, the specific rules on bureaucratic management and surveillance of slave mobilities, notably escape, were also made plain with particular rule "17th the negroes are never to be allowed to leave the plantation unless by special permission, and a written pass" and particular rule "18th no strange negro to be allowed to visit the plantation, unless by permission of the overseer, & a written pass from his master." The slave pass system relied on the notion that the slave could be known through a written identification document. Christian Parenti's writings on the kinds of surveillance practices employed during chattel slavery in the southern United States name the "information technologies" of the written slave pass, wanted posters and advertisements for runaway slaves and servants, and organized slave patrols as key features of this system. Parenti situates plantation surveillance as the earliest form of surveillance practiced in the Americas. This was a system of surveillance that was regulated through violence and the written word.

The following accounts from Born in Slavery: Slave Narratives from the Federal Writers' Project, 1936–1938 detailing the slave pass system further this point:

By 1845 there were many laws on the Statute books of Georgia concerning the duties of patrols. . . . Every member of the patrol was required to carry a pistol while on duty. They were required to arrest all slaves found outside their master's domain without a pass, or who was not in company with some white person. He was empowered to whip such slave with twenty lashes.

The patte-rollers was something else. I heard folks say they would beat the daylights almost out of you if they caught you without no pass.

52 CHAPTER 1
In the plantation system, the restriction of the mobility and literacy of the enslaved served as an exercise of power. The racializing surveillance of the slave pass system was a violent regulation of black mobilities. On and off the plantation, black mobility needed to be tightly regulated in order for slave owners to maintain control, so, as ex-slave Anderson Furr put it, one had to “git a pass for dis and a pass for dat.” This was a system that also relied on the publication and circulation of newspaper advertisements for runaway slaves and truant servants that announced not only those who escaped or went missing from plantations, but also those people who left enslavement in private homes and establishments, like shops, inns, and taverns in cities and urban spaces.

Runaway slave advertisements reveal a lot about black flight to freedom, as these notices of escape would not only name those who left enslavement and made their own way, but also provide a physical description and list the monetary rewards, if any, that awaited those who aided in their capture and return. These ads would list their talents, occupations and skills, vices, languages spoken and whether or not they could read or write, strategies they might have used to escape, and what they were wearing and took with them when they made their way. Also listed would be clothing, musical instruments, and other items that could be sold, traded, bartered, or used to support the appearance of being free. An advertisement for a runaway slave might read like so: “RUN away, a Negro Man named Tom, born in Jamaica, but last from Havannah,” “blubber Lips, yellow Complexion, his Hair is neither right Negro nor Indian, but between both,” “His eyes very full, as if they were starting out of his head,” “had on when he went away a felt Hat, a Cotton Cap, a Homespun Coat with brass Buttons, a West-coat without sleeves, an Oznabrigs shirt, Leather Breeches with Brass Buttons, a pair of worsted Stockings and a pair of yarn ones, two pair of peak’d toe’d Shoes,” “his great Toes have been froze, and have only little pieces of nails on them,” “plays well on the Fiddle, and can read and write; perhaps he may have a false pass,” “is plausible and smooth in speaking, and may pass himself for a Sailor, having been used to a boat,” whoever secures said Negro shall have a reward of five pounds.

An unusually long 1762 advertisement for “a Mulatto Servant man named Charles Roberts” states not only his age and height, but the condition of the clothes he carried, “several other Waistcoats, Breeches, and Pair of Stocking; a blue Great Coat, and a Fiddle.” John Holt placed this ad, and in it he states that Roberts spoke “smoothly and plausibly, and generally
with a cringe and a smile,” and was good at arithmetic and accounting, leading Holt to charge that Roberts had probably forged documents to pass as a free man although he had “no legal claim to freedom.” Holt laments that he placed confidence in Roberts, “which he has villainously abused; having embezzled Money sent him to pay for Goods, borrowed money and taken up goods” in Holt’s name, unbeknownst to him. The reward for Roberts’s capture in New York City was five pounds, and if found elsewhere the award would be greater. Anyone who captured him, the ad instructed, was to leave any money found on Roberts’s person with the magistrate and was warned to be careful and “very watchful against an Escape, or being deceived by him, for he is one of the most artful of Villains.” Through their detailing of physical descriptions, the surveillance technology of the runaway slave advertisement was put to use to make the already hypervisible racial subject legible, borrowing again from John Fiske here, as “out of place.”

Runaway slave advertisements were not only about ascribing physical details to the runaway, but also offered the slave owner’s assessment of the fugitive’s character. One example of the role of runaway slave advertisements, and similarly wanted posters, in upholding racial categorization is a March 15, 1783, advertisement in the Royal Gazette offering a “Two Dollars reward” for “a Mulatto, or Quadroon Girl, about 14 years of age, named Seth, and calls herself Sall.” This runaway advertisement states that Seth “sometimes says she is white and often paints her face to cover that deception.” Seth’s duplicity is not limited to her use of the alias “Sall,” as this notice informs its readers, but also to her racial ambiguity, in her apparent choosing to self-identify or pass as white, rather than as “a Mulatto” (one black parent and one white parent) or a “Quadroon Girl” (one black grandparent), which was the racial nomenclature of the one-drop rule arising out of slavery and continuing beyond that institution. This advertisement also remarks that Sall has been “seen dancing” and “is well known in town, and particularly at the Fly-Market, for many wicked tricks.” The Fly-Market in Lower Manhattan served as the city’s market for provisions and other goods up until the early nineteenth century. Sall’s ability to evade surveillance through makeup, wicked tricks, and hiding in plain sight exposes the one-drop rule as a social construction that, for some, could be subverted by performing whiteness. Seth’s, or sometimes Sall’s, hiding in plain sight—by identifying as white and using an alias—was a freedom practice to evade surveillance, and in so being a form of dark sousveillance. An 1836 runaway
advertisement describes Edmund Kenney, who escaped enslavement by passing as white, thus: "he has straight hair, and complexion so nearly white, that it is believed a stranger would suppose there was no African blood in him." An 1845 advertisement boasting a five hundred dollar reward for "a negro woman named Fanny" described her as a Bible-carrying, literate, "intelligent woman" who was "as white as most white women, with straight light hair, and blue eyes, and can pass herself for a white woman."^104

THE CENSUS

In 1848 when Ellen and William Craft made their way out of Georgia and escaped chattel slavery by trains and by ships, they were able to do so through the ways in which Ellen's body was able to trouble the one-drop rule. Born to a black mixed-raced mother and fathered by the white man who owned her mother, Ellen was, at the time, labeled a quadroon but able to pass as white, as sometimes deaf and an "invalid gentleman" named "Mr. William Johnson." She passed as her husband's owner in order to secure his freedom as well as her own. She used a poultice and put it in a white handkerchief "worn under the chin, up the cheeks, and to tie over the head," hoping that this disguise would hide "the expression of the countenance, as well as the beardless chin."^105 Because she could not read or write at the time of her escape, she feigned inflammatory rheumatism and placed her right arm in a sling in order to evade detection if, for example, she were asked to sign her name in a hotel's guest register. With Craft, her passing in terms of race, passing in terms of gender, passing in terms of class, and passing in terms of disability all played a role in her and William's passing into freedom. The Crafts eventually left Boston to later arrive in England, where they lived for nineteen years before returning to the United States, where they opened a school for children and a cooperative farm in Georgia. In the 1850 census, Ellen was listed as residing in Boston and her race is recorded as Black (or rather "ditto," as it was recorded in the column under William's). The 1850 census marked the first time that the federal census included slave schedules for some states in order to enumerate each enslaved person held in a household or dwelling. By the 1890 census, Ellen Craft was recorded as "M" for Mulatto and her occupation as "keeping house" in Bryan County, Georgia.

In the United States, racial nomenclature as a form of population management was made official with the taking of the first federal census in 1790,
which asked questions regarding the number of free white males, free white females, other free people, and slaves in a household. Census enumeration is a means through which a state manages its residents by way of formalized categories that fix individuals within a certain time and a particular space, making the census a technology that renders a population legible in racializing as well as gendering ways. The census is a form of "state stocktaking," as David Theo Goldberg puts it, which discloses "population size, shape, distribution, quality and flow of labor supply, taxation and conscription pools, political representation, voter predictability, and the necessities of population reproduction." While such "state stocktaking" sees the census informant respond to a series of questions, including date of birth, how many people live in a single dwelling, and whether or not the dwelling is rented or owned, it takes the form of racializing surveillance through its very reinscription of racial categories. As an example, in terms of racial categories and the U.S. census form, there has remained a constant, unspecified whiteness as a racial category. Rather than employing an alphabetical order, "White" is always listed first among the boxes from which to choose in order to answer the question of the census informant's race. The proliferation of racial categories from which to choose, or have one's answer assigned, was first reserved for the management of blackness, with other groupings later added to reflect changing immigration patterns. In the 1890 census, Mulatto, Quadroon, and Octoroon appeared as subcategories of "Black," but by the 1900 census these subcategories were "collapsed into the singularity of an unqualified blackness," reflecting the one-drop rule. "Mull" for Mulatto was reintroduced in 1910 and in the 1930 census it was replaced with "Neg" for Negro, a racial category that would fall in and out of favor, depending on each subsequent decennial enumeration. For the 2010 census, "Black, African-Am or Negro" were subsumed under one box and in 2013 the Census Bureau announced that "Negro" would be dropped from its surveys. As Goldberg writes, when the category "Mexican" was first introduced, it was understood as meaning not white unless the census informant "explicitly and accurately claimed white descent." In this way, it was left to the census taker to judge whether the census informant's claim to the category of whiteness was valid, rather than accepting at face value the informant's self-identification as white. The 2010 questionnaire asks if the census informant is "of Hispanic, Latino, or Spanish origin," and, if "yes," the informant can choose "Mexican, Mexican Am., Chicano," Puerto Rican, or Cuban or fill in the blank to specify "another Hispanic, Latino,
or Spanish origin." From its inception, the census has been a technology of disciplinary power that classifies, examines, and quantifies populations.

What It's Like, What It Is:
Controlling Images and Black Looks

In Fighting Words: Black Women and the Search for Justice, while referring not specifically to prison surveillance or plantation slavery but to the post-slavery, segregated southern United States, Patricia Hill Collins writes that while racial segregation was aimed at black people as a group or class and sought to erase individuality by making black people seemingly interchangeable, surveillance "highlights individuality by making the individual hypervisible and on display." As part of the practice of "racial etiquette" in the segregated South, surveillance, Collins tells us, was a way of ensuring that "Blacks would stay in their designated, subordinate places in white-controlled public and private spheres." Collins situates the bodies and lives of black women who labored as domestic workers and the white-controlled private homes in which they were employed as the "testing ground for surveillance as a form of control" that was enacted by way of "techniques of surveillance," including close scrutiny, sexual harassment, assault, violence, or the threat thereof. For the white women who employed them, Collins argues, this arrangement was predicated on the illusion that "the Black women workers whom they invited into their private homes felt like 'one of the family,' even though they actually had second-class citizenship in the family." Yet within these labor conditions of hypervisibility, black domestic workers needed to assume a certain invisibility where, as bell hooks observes, "reduced to the machinery of bodily physical labor, black people learned to appear before whites as though they were zombies, cultivating the habit of casting the gaze downward so as not to appear uppity." Seemingly "invisible to most white people, except as a pair of hands offering a drink on a silver tray," this signifying act was performed by many domestic laborers so that they would be assumed to be readily manageable and nonthreatening. Coupled with this system of scrutinizing black women's domestic labor in private white homes was the controlling image of "the mammy," one of "several interrelated, socially constructed controlling images of Black women, each reflecting the dominant group's interest in maintaining Black women's subordination." The mammy as a
representational practice relies on the circulation of stereotyped images and ideologies of black womanhood that seek to position black women as “the faithful, obedient domestic servant.” The mammy is depicted as caring for the family in which she is employed, often to the sacrifice of her own. This social control mechanism was “created to justify the economic exploitation of house slaves and sustained to explain Black women’s long-standing restriction to domestic service,” representing, as Collins puts it, “the normative yardstick used to evaluate all Black women’s behavior.” In so being, the mammy served as a symbol of “the dominant group’s perceptions of the ideal Black female relationship to elite White male power.” She is content, deferential, forgiving, nurturing, and loyal to the family that she cares for, operating with some authority, however marginal, while still knowing “her ‘place’ as obedient servant.” Such exaggerated representational strategies work to rationalize the economic exploitation and sexual subjugation of black domestic workers and of those who labor in low-paying conditions in the service sector. This mammy image circulates throughout dominant culture, from films such as Gone with the Wind (1939) to The Help (2011), to what Patricia A. Turner calls “contemptible collectibles,” those distorted depictions of blackness that often take the shape of figurines, postcards, kitchen utensils, and lawn ornaments. Simply put, “Mammy is the public face that Whites expect Black women to assume for them.” Of course, many black women who labored in white households forged loving and nurturing relations with their own families, despite the harsh working conditions of white supremacy.

In her discussion of the black gaze and looking relations during slavery and during the racial apartheid of Jim Crow in the southern United States, hooks notes that although black people “could be brutally punished for looking, for appearing to observe the whites they were serving, as only a subject can observe or see,” the violent ways in which blacks were denied the right to look back “had produced in us an overwhelming longing to look, a rebellious desire, an oppositional gaze.” “Black looks” were politicized and transformative when, as hooks states, “by courageously looking, we defiantly declared: ‘Not only will I stare. I want my look to change reality.’” This stare is the type of “eyeballing disposition” that disrupts racializing surveillance where, as Maurice O. Wallace discusses, such looks challenge the “fetishizing machinations of the racial gaze.”

Disruptive staring is the focus of Pan’s Opticon, a fifteen-panel photograph by South African artist Robin Rhode (figure 1.3). In it, Rhode’s sub-
ject, a black man and Rhode’s doppelgänger, is smartly dressed in a fashion similar to that of the subjects that South African photographer Ernest Cole documented in his 1967 book *House of Bondage* as they toiled, were relocated or banished, defied, and survived under passbook laws and the racist repression of apartheid South Africa. It can also be said that Rhode’s subject gestures to the *tsotsi* aesthetic popularized by Soweto youth and those in other townships of Johannesburg in the 1940s, a style and fashioning of masculinity that reflected working-class township life: a dark pinstriped jacket, white-collared shirt, and a straw boater hat. His back is to the camera as he faces a concrete wall. His stare is accessorized with inside calipers—like compasses, but with the needles at each end curving outward—that appear to jut out from each of his eyes. The inside caliper first appeared around the sixteenth century as a measuring device often used to determine the dimensions of an aperture, that being the space through which light rays pass and come into focus on an image surface. In photography, the aperture’s diameter regulates the amount of light that reaches the image surface. The smaller the aperture size, the darker the surface will appear. For the astronomical telescope, the aperture is the optical element that gathers light and brings the atmosphere into focus. No telescope, so far, can make dark matter visible.

Rhode’s subject in the *Pan’s Opticon* series is suited up with a prosthetic look. His ocular interrogation confronts the Panopticon and the architecture of surveillance—corners, shadows, reflections, and light—covering the wall with dark matter. On the subject of walls and architecture, Rhode writes that “when one speaks of walls, one speaks of security, privacy, and demarcation.” Rhode’s *Pan’s Opticon* is a play on Bentham’s Panopticon. Rhode’s naming of his series of photographs with the possessive noun *Pan’s* is a claiming of Bentham’s eighteenth-century plan for “obtaining power of mind over mind.” Rhode’s black subject is not backed into a corner, but facing it, confronting and returning unverified gazes. That Rhode is a South African artist based in Germany points to the ways that disruptive staring can be transnational, as transnational as the structures that it disrupts. The stenciled circumferences of incomplete circles of black spray paint seemingly emanate from his eyes onto the wall’s surface. With each frame of the storyboard, the circles refracted by the subject’s eyes multiply, overlapping each other like disorganized Venn diagrams until the corner is completely covered in dark matter. In one frame, no neat stenciled circles appear, just two solid but smaller black circles of spray paint dripping down from the calipers onto the concrete wall, suggesting, perhaps, a peephole for a cu-
rious spectator's stolen vision, or the excesses of black looks that bleed outside stenciled borders, color outside the lines, and are out of place.

The disruptive stare of the subject in Adrian Piper's video installation *What It's Like, What It Is #3* (figure 1.4) is one such act of courageous looking. At the center of this installation is a four-sided column, like the Panopticon's inspection tower, but with each side of the column fitted with a television screen. Each screen plays prerecorded video of the front, back, and profile views of a black man (actor John L. Moore) who stares at those watching Piper's installation as he states his refusals of the stereotypes placed upon blackness: "I'm not pushy. I'm not sneaky. I'm not lazy. I'm not noisy." After listing four such refusals, he turns to face another direction and then lists four more: "I'm not vulgar. I'm not rowdy. I'm not horny. I'm not scary." He looks directly at the viewers of this installation, who can be either standing or seated on the bleacher-like seating that surrounds the center column. The installation is all-white and through its use of mirrors, the video is reflected throughout. In this setting like a lecture hall, viewers
of this installation are then instructed by the lists of refusals of the critique coming from the bodiless head in the column. In this way, *What It's Like, What It Is #3* can be read as confronting the surveillance imposed upon black life. The soundtrack to the nearly five-minute video of the installation is the Commodores' song "Zoom" (1977), playing in the background while the subject tells what it's like to live with antiblack racism, racial stereotyping, and the scrutiny of white supremacy coming from all sides: "I'm not shiftless. I'm not crazy. I'm not servile. I'm not stupid." His list of what black people are not is looped in repetition, leaving a space for alternative imaginings of what blackness really is and could be, while the voice of Commodores lead singer Lionel Richie croons in the background track, singing, "Zoom. I'd like to fly far away from here... where everybody can be what they want to be" and "I wish the word they call freedom someday would come." The song's lyrics express hope for escape, freedom, and a new way of being. In this way, Piper's piece offers us a look at oppositional gazing and talking back to the normalizing judgment and hierarchical observa-
tion of disciplinary, controlling images. Talking back is, as hooks puts it, "the expression of our movement from object to subject" and a "gesture of defiance that heals, that makes new life and new growth possible." Talking back, then, is one way of challenging surveillance and its imposition of norms.
Day 2: Mass Surveillance and Social Media
Surveillance is not, in and of itself, a terrible activity.

Parents surveil their children in order to make sure they don't hurt themselves. Police officers surveil the population to catch criminals. Companies surveil their employees to catch thieves and cheaters. Journalists surveil powerful institutions to expose abuses.

But the modern era of dragnets marks a new type of surveillance: suspicionless, computerized, impersonal, and vast in scope. Some people believe this surveillance will keep society safer. Others believe it will usher in a police state.

To understand the worst-case scenario, I visited the world's best-kept archives of pre-electronic surveillance—the Stasi archive in Berlin. I wanted to see how the files kept by the Stasi, the East German secret police during the Communist era, compared with the information collected by today's commercial and governmental surveillance operations.

The Stasi was the largest secret police operation—on a per capita basis—in the history of the world. Famously repressive, it kept files on 4 million East Germans—or about one-quarter of a total population of nearly 16.7 million. The Stasi didn't have the advantage of today's technology—it had to steam open mail and listen to phone calls manually—but it had an extensive network of informants. In 1989, roughly one in fifty East
Germans between the ages of eighteen and eighty worked for the Stasi in some capacity.

As the East German regime was collapsing in November 1989, the Stasi began shredding the files they had kept on citizens. Outraged that the evidence of the regime’s oppression was being destroyed, residents stormed the Stasi headquarters to halt the destruction of files. As a result, today’s citizens can request to see files kept about them, and researchers have access to some files, with the names of the people who were monitored removed.

On a trip to Berlin in 2011, I stopped by the Stasi archive—formally known as the Federal Commissioner Preserving the Records of the State Security Service of the former German Democratic Republic—which is incongruously located in a cheerful, glass-paned office building in the heart of the city.

The Stasi records administrator assigned to my request, Günter Bormann, was immediately enthusiastic about my idea of comparing Stasi and modern surveillance. As I filled out the paperwork to obtain a set of Stasi records, he asked me what a typical Western data gatherer knows about me. So I asked if I could use his computer to show him a bit of what is known about me online.

I logged on to my Gmail account and navigated to the settings, where Google allowed me to view my previous Web searches, including books I had researched and photos I had viewed. It also listed the ninety-three people that I’d e-mailed or instant-messaged using Gmail.

Standing over me, Bormann was impressed. Social network mapping, he told me, “was very difficult for the Stasi.” He sat down at his conference table and started drawing a few circles with connecting lines. “They tried to do social network mapping,” he said, but even with all their informants they had a hard time building robust maps.

Inspired, I clicked on to my LinkedIn page—where I had installed a special plug-in that allows me to see a visualization of my social network. It was a beautiful map with nearly two hundred points strung together with colored lines. My New York work colleagues were all clustered in one corner in yellow, other media colleagues were clumped in a blue corner, and my connections from my time in California are on the other side of the map in a sea of orange and gray dots.
Bormann was even more impressed. “The Stasi would have loved this.”

Three months later, a packet of documents arrived at my desk in New York. Inside were more than a hundred pages containing two files in German. After a bit of searching, I found some Stasi experts to help me translate and interpret the files.

The surprising thing was how crude the surveillance was. “Their main surveillance technology was mail, telephone, and informants,” said Gary Bruce, an associate professor of history at the University of Waterloo and the author of The Firm: The Inside Story of the Stasi.

The first file revealed a low-level surveillance operation called an im-forgang aimed at recruiting an unnamed target to become an informant. (The names of the targets were redacted; the names of the Stasi agents and informants were not.) In this case, the Stasi watched a rather boring high school student who lived with his mother and sister in a run-of-the-mill apartment. The Stasi obtained a report on him from the principal of his school and from a club where he was a member.

The Stasi didn’t have much on him—I’ve seen Facebook profiles with far more information—but they still tried to recruit him as an informant. He turned them down, citing some nonspecific health reasons. He was lucky that he was young and boring. Most people who were asked to be informants felt that they couldn’t say no to the Stasi when presented with evidence of a minor infraction—such as watching West German television.

The second file documented a surveillance operation known as an OPK, for Operative Personenkontrolle, of a man who was writing oppositional poetry. It was a medium-size operation: the Stasi deployed three informants against him but did not steam open his mail or listen to his phone calls.

Stasi officers received bonuses when they launched OPKs, and an even more generous bonus if OPK was fruitful—in producing either an arrest or a new informant. Ultimately, however, the OPK of the poet was fruitless because the regime collapsed before the Stasi could do anything about him.

Six months later another, smaller packet arrived. This one contained
about fifteen pages documenting specific Stasi surveillance tactics that I had requested.

In one file, Stasi agents recorded the movements of a forty-year-old man for two days—September 28 and 29, 1979. They watched him as he dropped off his laundry, loaded up his car with rolls of wallpaper, and drove a child in a car “obeying the speed limit,” stopping for gas and delivering the wallpaper to an apartment building. The Stasi continued to follow the car as a woman drove the child back to Berlin.

“The targets were extremely circumspect . . . ,” the Stasi officer, Lieutenant Colonel Fritsch, wrote. “Presumably . . . [they had been] tipped off . . . that observations were being conducted in the vicinity.”

The agent appears to have started following the target at 4:15 p.m. on a Friday evening. At 9:38 p.m., the target went into his apartment and turned out the lights. The agent stayed all night and handed over surveillance to another agent at 7:00 a.m. Saturday. That agent appears to have followed the target until 10:00 p.m. From today’s perspective, this seems like a lot of work for very little information.

The second file was simply a hand-drawn social network. On a single page of paper, agents had drawn forty-six connections, linking a target to various people (an “aunt,” “Operational Case Jentzsch,” presumably Bernd Jentzsch, an East German poet who defected to the West in 1976), places (“church”), and meetings (“by post, by phone, meeting in Hungary”).

This was an impressive document. It had only one-quarter of the data compared to my two-hundred-plus contacts on my LinkedIn profile, but they were likely more relevant to the investigation than my far-flung network.

The Stasi would likely have conducted surveillance of everybody on the map, who were known as “secondary individuals,” according to Gary Bruce. “You didn’t have to do anything particularly oppositional to end up with a Stasi file,” he said.

The problem was that a Stasi file—no matter how large—could affect whether a person got demoted or promoted, how long they would have to wait to get a car or an apartment, or whether their application to visit relatives in the West would be approved. As a result, even though the Stasi had files on only a quarter of the population, fear of becoming a target was pervasive.

In a 1990 survey, right after the fall of the Communist regime, 72.6
percent of former East German citizens described the Communist experience as “complete surveillance.” In 1992, when asked to consider the statement, “One felt spied upon. You couldn’t trust anyone,” 43 percent described it as “True, that’s exactly how it was.”

In a study of psychological effects of Stasi surveillance, Babett Bauer interviewed about thirty individuals who had had direct encounters with the secret police. She found that their fear of another Stasi encounter had prompted them either to become model citizens or to withdraw from society. Bauer concluded that people who encountered the Stasi internalized repression into “the body’s wrinkles and the brain’s mechanisms.”

The power of observation to be repressive was the foundational idea of the “Panopticon”—a prison design proposed by Jeremy Bentham in 1787. His idea was that a perfect prison would allow prisoners to believe they were being watched at all times but allow the watchers to remain unseen. He designed a circular prison with a guard tower in the middle, but it was never built during his lifetime.

In 1975, the French philosopher Michel Foucault popularized Bentham’s idea, describing the Panopticon as a “marvelous” instrument of power. “The more numerous those anonymous and temporary observers are, the greater the risk for the inmate of being surprised and the greater his anxious awareness of being observed,” he wrote in his book Discipline and Punish.

Now that we live in a world of extensive surveillance, it would make sense that Foucault’s “anxious awareness” would be our collective mental state. But it seems Foucault was only partially correct. As Babett Bauer discovered in her interviews with East Germans, people cope with surveillance as much by changing their behavior as through increased anxiety.

In 2011, Finnish researchers installed extensive monitoring equipment—video cameras; microphones; and computer, smartphone, and TV monitoring devices—in ten households for a year, to determine the long-term effect of ubiquitous surveillance. They found that the subjects of the study—who had obviously volunteered—“gradually became accustomed to surveillance” over the course of the study. However, the responses varied. One participant dropped out after six months, stating that the
surveillance had curtailed his or her computer usage and affected his or her relationships. (The researchers did not reveal genders or identifying details of the subjects.)

Although the subjects knew that the data from the surveillance was not being disclosed to anyone except the researchers, and that they could turn off the system at any time, they still found the monitoring to be a source of “annoyance, concern, anxiety and even rage,” the researchers wrote. The most hated monitors were the computer monitoring and the video cameras (which two participants admitted to turning off regularly).

Most participants changed their routines, particularly to be more cautious about where they undressed (cameras were not placed in the bedrooms or bathrooms) and where they held sensitive conversations.

“Two subjects started to spend more time in the bedroom, which was not covered by the microphones. Two others said that they would go to a café to discuss personal matters,” the authors wrote. “One subject mentioned avoiding inviting many people home.”

The lead author of the paper, a computer science researcher named Antti Oulasvirta, said that although people’s overt concerns about privacy plateaued after three months, they all adjusted their behavior to adapt to the situation. But their adaptations were easily disturbed. “The required changes made the home fragile,” he said. “Any unpredicted social event would bring the new practices to the fore and question them, and at times prevent them from taking place.”

Another way to cope with ubiquitous surveillance is painted by the science fiction author David Brin, in his prescient 1998 book *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?*

The book opens with a “tale of two cities.” Both cities have surveillance cameras installed on “every lamppost, every rooftop and street sign.” In the first city, all the images are piped into the central police station. In the second city, every citizen can access any camera through a wristwatch television.

Both cities are crime-free. But the first city is a police state, while the second city enjoys some freedom: “A late-evening stroller checks to make
sure no one lurks beyond the corner. . . . An anxious parent scans the area to find which way her child wandered off. . . . A shoplifter is taken into custody gingerly . . . because the arresting officer knows that the entire process is being scrutinized.”

Brin argues, convincingly, that the proliferation of cameras—and other surveillance technology—is the inevitable result of the progress of technology. To him, the important question is: Who controls the cameras? As he sees it, mutual surveillance—the citizens and the state watching each other—can transform ubiquitous surveillance from oppression to mutual accountability. And there is some evidence to support this view.

During the Cold War, mutual surveillance played an important part in preventing the United States and the Soviet Union from dropping nuclear bombs on each other.

After the Soviet Union launched Sputnik in 1957, America was consumed by a fear of the Soviet Union’s capabilities and their implications. In 1958, Senator John F. Kennedy claimed that the United States was falling behind the Soviets and predicted that “by 1960 the United States will have lost . . . its superiority in nuclear striking power.”

It wasn’t until the United States successfully launched photoreconnaissance spy satellites that it was able to measure the missile gap. The images captured by the satellite showed that the true missile gap ran the other way: in 1961, the Soviets had just four intercontinental ballistic missiles, compared to America’s stockpile of 170.

However, the United States still failed to notice the Soviet missile buildup in Cuba during the summer of 1962, an intelligence failure that brought the United States and the Soviet Union to the brink of a nuclear war. As a result, building better spy satellites became an important part of the Cold War race.

In 1972, the United States and the Soviet Union codified their spying in the Anti-Ballistic Missile Treaty, when each side agreed to use “national technical means” to verify the other’s compliance with the treaty. Six years later, President Jimmy Carter acknowledged the importance of the spy satellites in a speech at the Kennedy Space Center. “Photoreconnaissance satellites have become an important stabilizing factor in world affairs in the monitoring of arms control agreements,” he said.

Indeed, overt surveillance can be effective at changing human behavior. Studies have repeatedly shown that the simple suggestion of being
watched can encourage people to behave more cooperatively—even if there is no actual surveillance being conducted.

The belief that another person is present triggers a state of "psychological arousal," even if that "person" is not real, according to Ryan Calo of the University of Washington. In one study, people who stared at a photo of a bug-eyed robot donated 30 percent more money into a communal pool in a computer game than those who felt they weren't being watched.

In 2011, researchers at Newcastle University in Britain hung posters of staring human eyes at eye level in random locations in the campus cafeteria for thirty-two days. They found that people were twice as likely to clean up after themselves when they finished eating, compared to the locations where posters of flowers or other benign images were displayed. The following year, a similar group of researchers at the university posted signs near the bicycle racks around campus that said, "Cycle Thieves: We Are Watching You," with text printed over a photograph of human eyes. Bicycle thefts decreased by 62 percent in the locations with the new posters, but they increased in those locations without posters (by 65 percent), suggesting that the thieves had moved their activities to "safer" locations. "The effectiveness of this extremely cheap and simple intervention suggests that there can be considerable crime-reduction benefits to engaging the psychology of surveillance, even in the absence of surveillance itself," the researchers wrote.

Surveillance theater—the pretense of surveillance, conducted by humanlike eyes or robots—does appear to cause people to treat each other better. But the jury is still out about whether surveillance conducted by cameras deters crime.

A 2008 analysis by the California Research Bureau of forty-four studies of closed-circuit television surveillance found that 43 percent of the studies showed no effect on crime, while 41 percent showed statistically significant crime reduction.

In 2011, the Urban Institute analyzed camera surveillance systems in Baltimore, Chicago, and Washington, D.C., and found similarly conflicted results. In Baltimore, the authors found that a network of five hundred cameras that was monitored around the clock by a team of trained retired police officers contributed to a 35 percent drop in incidents of overall crime per month in one neighborhood. But cameras in other
neighborhoods proved less successful. Similarly, in Chicago, which has installed a multimillion-dollar surveillance program with more than eight thousand cameras, the Urban Institute found that the cameras contributed to a 12 percent drop in crime in Humboldt Park but provided no statistically significant decline in crime in West Garfield Park. And in Washington, D.C., the Urban Institute found that surveillance cameras had no statistically significant impact on crime.

One reason for the conflicting results: many factors can contribute to a drop in crime, and it's difficult to isolate camera surveillance from other factors, such as increased police patrols or improved lighting.

In 2004, Leon Hempel and Eric Töpfer, writing from the Center for Technology and Society in Berlin, analyzed studies of closed-circuit television (CCTV) use in Europe and found that many of the studies lacked control groups to compare crime trends in the areas where cameras were installed to crime trends in the wider areas without cameras, and lacked analysis of the displacement of crime from the target areas to other areas.

The few studies that have used control groups show little support for the theory that cameras can prevent crime. Another Urban Institute study from 2011 analyzing the impact of surveillance cameras on crime in parking lots—and using a randomized controlled trial method—showed that the cameras made no real difference. The study compared a year's worth of car-related crime in twenty-five parking lots near Metro stations in Washington, D.C., that had installed motion-activated cameras with identical crimes in twenty-five similar "control" parking lots with no cameras installed. Although these were digital still cameras, researchers posted signs that gave the impression of constant camera surveillance of the parking lot. The study found that "the cameras had no discernable impact on crime."

And some evidence even suggests that simple streetlights may be as good at deterring crime as surveillance cameras. In 2004, the criminologists Brandon Welsh and David Farrington analyzed thirty-two studies conducted in the United States, Canada, and Britain to determine whether CCTV deterred crime more effectively than simple streetlights. Their conclusion: streetlights and CCTV were equally effective in deterring property crime—and neither one was very good at deterring violent crime. They theorized that cameras and streetlights both "act as a catalyst
to stimulate crime reduction through a change in perceptions, attitudes and behavior of residents and potential offenders.”

The authors of the Urban Institute study speculated that cameras are effective only when they are actively monitored by law enforcement agents, who act quickly upon the information obtained by the cameras. “The technology is only as good as the manner in which it is employed,” they wrote.

In other words, surveillance cameras work to influence human behavior only when people are convinced that a human being is on the other side of the camera watching them.

It is also not clear that surveillance conducted by computer data analysis helps catch terrorists before they strike.

After all, several terrorist plots have slipped through the surveillance dragnets. Since 9/11 there has been a series of attempted terrorist attacks. The most notable include:

- **The Shoe Bomber.** In 2001, Richard Colvin Reid tried and failed to detonate a bomb in his shoe while on a flight from Paris to Miami.
- **The LAX Shooter.** In 2002, Hesham Mohamed Hadayet, an Egyptian, opened fire at the El Al ticket counter in Los Angeles International Airport, killing two and wounding several others.
- **The Fort Hood Shooter.** In 2009, U.S. Army major Nidal Malik Hasan entered a deployment center at Fort Hood in Texas, jumped on a desk, shouted “Allahu Akbar,” and opened fire with two pistols. He killed thirteen people and injured forty-three others.
- **The Underwear Bomber.** On Christmas Day 2009, Umar Farouk Abdulmutallab attempted to detonate explosives sewn into his undergarments aboard a flight to Detroit from Amsterdam. His device did not explode, but simply ignited—wounding Abdulmutallab and two other passengers.
- **The Times Square Bomber.** In 2010, Faisal Shahzad, who had trained with terrorists in Pakistan, tried but failed to detonate a car bomb in New York’s Times Square.
- **The Boston Marathon Bombers.** In 2013, Tamerlan and Dzhokhar Tsarnaev allegedly deposited homemade bombs near the finish line of
the Boston Marathon. The explosions injured hundreds of people and killed three, including an eight-year-old boy.

Surveillance advocates point out that these statistics don’t take into account the attacks that were prevented—many of which remain secret. However, for the first time, we do have some evidence of deterred attacks.

In the wake of the Snowden leaks, General Keith Alexander, the director of the NSA, disclosed that the agency’s controversial phone and Internet dragnets had “contributed to our understanding, and, in many cases, helped enable the disruption of terrorist plots” in fifty-four cases.

He didn’t specify the exact cases—although he did say most of them were foreign—but he did highlight the case of Najibullah Zazi. In 2009, Zazi was arrested just days before he and friends were allegedly planning to carry out a suicide bombing in the New York City subway.

According to Alexander, Zazi was swept up in a dragnet called “Operation High-Rise.” The NSA found e-mails from Zazi among e-mails between the United States and Pakistan that it was monitoring under the PRISM dragnet that sweeps up the U.S. end of international e-mails.

Within those communications, the NSA also found a telephone number. It then used the Patriot Act dragnet of all telephone calls placed in the United States to locate other numbers that were connected to the first number. “We found Zazi was talking to a guy in New York who had connections to other terrorist elements,” Alexander said.

Once the FBI was alerted, its agents used traditional law enforcement techniques. They followed Zazi as he drove to New York City from his home in Colorado. When he arrived, the FBI asked the Port Authority to stop Zazi at a checkpoint on the George Washington Bridge, but nothing was found in his car. Zazi was allowed to drive away, but he was spooked by the surveillance. A few days later, he flew back to Denver without carrying out his plot.

Zazi was arrested in Colorado and later pleaded guilty to charges including conspiracy to use weapons of mass destruction and providing material support to al-Qaeda. He has not yet been sentenced.

But it is not clear that the government needed dragnets to catch Zazi. If Zazi was e-mailing with terrorists under surveillance, a search warrant would have sufficed to capture his communications. Similarly, once
his phone number was identified, a judge would most likely have approved pulling the calling records for that phone.

When closely questioned by the Senate about whether the dragnets were “critical” to catching Zazi, General Alexander hedged. He said phone records were not critical and didn’t answer whether the e-mail dragnets were critical to catching Zazi. And even President Obama was lukewarm when describing the use of NSA dragnets in catching Zazi. “We might have caught him some other way,” he said in a television interview with Charlie Rose. “But at the margins, we are increasing our chances of preventing a catastrophe like that through these programs.”

Is mass surveillance worth it when its fiercest advocates can only say that it “contributed to our understanding” of cases “at the margins”?

Dragnets are also a double-edged sword. If intelligence agencies pick up a lead but don’t pursue it, they are often blamed in the event of an attack. That’s what happened in the cases of the underwear bomber, the Fort Hood shooter, and the Boston Marathon bombers. The perpetrators had all been flagged as terrorist threats at some time prior to their attacks.

In their book Enemies Within: Inside the NYPD’s Secret Spying Unit and Bin Laden’s Final Plot Against America, the journalists Matt Apuzzo and Adam Goldman chronicle how the New York Police Department’s indiscriminate surveillance of Muslims in New York City failed to catch Najibullah Zazi and his friends, as they dreamed up their terrorism plot in Queens. The NYPD’s “rakers” had surveilled Zazi’s neighborhood restaurants, his mosque, and even the travel agency where he bought his airline tickets to Pakistan. “After years of raking, the NYPD knew where New York’s Muslims were,” Apuzzo and Goldman wrote. “But they still didn’t know where the terrorists were.”

The father of Umar Farouk Abdulmutallab, the underwear bomber, had warned the American embassy in Nigeria of his son’s radical views and that his son had disappeared and might have traveled to Yemen. A White House investigation found that “several agencies” had obtained information about Abdulmutallab prior to the attempted attack but had not placed him on a watch list.

An FBI field office had been monitoring Fort Hood shooter Nidal Malik Hasan’s communications with radical Islamic cleric Anwar al-
Awlaki but hadn’t taken further action before he opened fire at Fort Hood. And the future Boston Marathon bomber Tamerlan Tsarnaev had been in the National Counterterrorism Center’s database for at least a year prior to his attack.

Some research suggests that collecting vast amounts of data simply can’t predict rare events like terrorism. A 2006 paper by Jeff Jonas, an IBM research scientist, and Jim Harper, the director of information policy at the Cato Institute, concluded that terrorism events aren’t common enough to lend themselves to large-scale computer data mining.

After all, Zazi was buying nail-polish remover to build an acetone explosive, Abdulmutallab was sewing explosives into his underwear, and Hasan was sending fan mail to al-Awlaki. Each event had its own distinct patterns. By comparison, data mining for patterns works well in pursuing credit card and insurance fraud, where fraud is more common. Credit card companies develop “red flags”—such as transactions in foreign countries, that can alert them to a possible fraud. “Unlike consumers’ shopping habits and financial fraud, terrorism does not occur with enough frequency to enable the creation of valid predictive models,” Jonas and Harper conclude.

In 2008, the National Academy of Sciences convened dozens of experts to study counterterrorism data mining. The group reached a similar conclusion: “Highly-automated tools and techniques cannot be easily applied to the much more difficult problem of detecting and preempting a terrorist attack, and success in doing so may not be possible at all.”

Some intelligence officials have hinted that they share the same pessimism about their ability to sort through vast amounts of data to predict the next attack. In a 2012 speech, Matthew Olsen, the director of the National Counterterrorism Center, said, “If there is another attack, the likelihood is that you could look back retrospectively and find some hint or some clue in the vast amount of data that we have access to.”

And after the Boston Marathon bombings, the city’s police commissioner, Ed Davis, went even further, telling Congress that more technological surveillance wouldn’t have helped. “There’s no computer that’s going to spit out a terrorist’s name,” he said. Instead, the best leads come from people who alert “law enforcement when something awry is identified. That really needs to happen and should be our first step.”
So what can we conclude about life in a state of surveillance?

The evidence suggests that human surveillance, or perceived surveillance through pictures of human eyes or cameras actively monitored by humans, can modify behavior to promote positive social habits, such as clearing up dishes in a communal cafeteria, and sometimes can deter property crimes. However, there is some evidence that suggests that street lighting may be just as effective. Mutually assured surveillance also appears to have helped prevent mutually assured destruction during the Cold War.

However, surveillance does not appear to be good for predicting terrorism, as many terrorist events have slipped through the dragnets. Even the Stasi failed to predict the collapse of the East German regime in 1989. And the flood of surveillance data can be overwhelming and confounding to those who are charged with sorting through it to find terrorists.

But ubiquitous, covert surveillance does appear to be very good at repression. People who were indiscriminately and secretly monitored—whether in East Germany or in the Finnish study—were found to censor their behavior and speech.

The question then becomes: Are the benefits of ubiquitous, indiscriminate, dragnet surveillance worth living in a culture of fear?
DRAGNET NATION

A QUEST FOR PRIVACY, SECURITY, AND FREEDOM IN A WORLD OF RELENTLESS SURVEILLANCE

JULIA ANGWIN

ST. MARTIN'S GRIFFIN  NEW YORK
Two decades ago, the US intelligence community worked closely with Silicon Valley in an effort to track citizens in cyberspace. And Google is at the heart of that origin story. Some of the research that led to Google's ambitious creation was funded and coordinated by a research group established by the intelligence community to find ways to track individuals and groups online.

The intelligence community hoped that the nation's leading computer scientists could take non-classified information and user data, combine it with what would become known as the internet, and begin to create for-profit, commercial enterprises to suit the needs of both the intelligence community and the public. They hoped to direct the supercomputing revolution from the start in order to make sense of what millions of human beings did inside this digital information network. That collaboration has made a comprehensive public-private mass surveillance state possible today.

The story of the deliberate creation of the modern mass-surveillance state includes elements of Google's surprising, and largely unknown, origin. It is a somewhat different creation story than the one the public has heard, and explains what Google cofounders Sergey Brin and Larry Page set out to build, and why.

But this isn't just the origin story of Google: It's the origin story of the mass-surveillance state, and the government money that funded it.

**Backstory: The intelligence community and Silicon Valley**
In the mid 1990s, the intelligence community in America began to realize that they had an opportunity. The supercomputing community was just beginning to migrate from university settings into the private sector, led by investments from a place that would come to be known as Silicon Valley.

The intelligence community wanted to shape Silicon Valley's efforts at their inception so they would be useful for homeland security purposes.

A digital revolution was underway: one that would transform the world of data gathering and how we make sense of massive amounts of information. The intelligence community wanted to shape Silicon Valley's supercomputing efforts at their inception so they would be useful for both military and homeland security purposes. Could this supercomputing network, which would become capable of storing terabytes of information, make intelligent sense of the digital trail that human beings leave behind?

Answering this question was of great interest to the intelligence community.

Intelligence-gathering may have been their world, but the Central Intelligence Agency (CIA) and the National Security Agency (NSA) had come to realize that their future was likely to be profoundly shaped outside the government. It was at a time when military and intelligence budgets within the Clinton administration were in jeopardy, and the private sector had vast resources at their disposal. If the intelligence community wanted to conduct mass surveillance for national security purposes, it would require cooperation between the government and the emerging supercomputing companies.

To do this, they began reaching out to the scientists at American universities who were creating this supercomputing revolution. These scientists were developing ways to do what no single group of human beings sitting at work stations in the NSA and the CIA could ever hope to do: gather huge amounts of data and make intelligent sense of it.

A rich history of the government’s science funding

There was already a long history of collaboration between America's best scientists and the intelligence community, from the creation of the atomic bomb and satellite technology to efforts to put a man on the moon.

The internet itself was created because of an intelligence effort.

In fact, the internet itself was created because of an intelligence effort: In the 1970s, the agency responsible for developing emerging technologies for military, intelligence, and national security purposes—the Defense Advanced Research Projects Agency (DARPA)—linked four supercomputers to handle massive data transfers. It handed the operations off to the National
Science Foundation (NSF) a decade or so later, which proliferated the network across thousands of universities and, eventually, the public, thus creating the architecture and scaffolding of the World Wide Web.

Silicon Valley was no different. By the mid 1990s, the intelligence community was seeding funding to the most promising supercomputing efforts across academia, guiding the creation of efforts to make massive amounts of information useful for both the private sector as well as the intelligence community.

They funded these computer scientists through an unclassified, highly compartmentalized program that was managed for the CIA and the NSA by large military and intelligence contractors. It was called the Massive Digital Data Systems (MDDS) project.

**The Massive Digital Data Systems (MDDS) project**

MDDS was introduced to several dozen leading computer scientists at Stanford, CalTech, MIT, Carnegie Mellon, Harvard, and others in a white paper that described what the CIA, NSA, DARPA, and other agencies hoped to achieve. The research would largely be funded and managed by unclassified science agencies like NSF, which would allow the architecture to be scaled up in the private sector if it managed to achieve what the intelligence community hoped for.

“Not only are activities becoming more complex, but changing demands require that the IC [Intelligence Community] process different types as well as larger volumes of data,” the intelligence community said in its 1993 MDDS white paper. “Consequently, the IC is taking a proactive role in stimulating research in the efficient management of massive databases and ensuring that IC requirements can be incorporated or adapted into commercial products. Because the challenges are not unique to any one agency, the Community Management Staff (CMS) has commissioned a Massive Digital Data Systems [MDDS] Working Group to address the needs and to identify and evaluate possible solutions.”

Over the next few years, the program's stated aim was to provide more than a dozen grants of several million dollars each to advance this research concept. The grants were to be directed largely through the NSF so that the most promising, successful efforts could be captured as intellectual property and form the basis of companies attracting investments from Silicon Valley. This type of public-to-private innovation system helped launch powerful science and technology companies like Qualcomm, Symantec, Netscape, and others, and funded the pivotal research in areas like Doppler radar and fiber optics, which are central to large companies like AccuWeather, Verizon, and AT&T today. Today, the NSF provides nearly 90% of all federal funding for university-based computer-science research.

**The CIA and NSA’s end goal**

The research arms of the CIA and NSA hoped that the best computer-science minds in academia could identify what they called “birds of a feather.” Just as geese fly together in large V shapes, or
flocks of sparrows make sudden movements together in harmony, they predicted that like-minded groups of humans would move together online. The intelligence community named their first unclassified briefing for scientists the “birds of a feather” briefing, and the “Birds of a Feather Session on the Intelligence Community Initiative in Massive Digital Data Systems” took place at the Fairmont Hotel in San Jose in the spring of 1995.

The intelligence community named their first unclassified briefing for scientists the “birds of a feather” briefing.

Their research aim was to track digital fingerprints inside the rapidly expanding global information network, which was then known as the World Wide Web. Could an entire world of digital information be organized so that the requests humans made inside such a network be tracked and sorted? Could their queries be linked and ranked in order of importance? Could “birds of a feather” be identified inside this sea of information so that communities and groups could be tracked in an organized way?

By working with emerging commercial-data companies, their intent was to track like-minded groups of people across the internet and identify them from the digital fingerprints they left behind, much like forensic scientists use fingerprint smudges to identify criminals. Just as “birds of a feather flock together,” they predicted that potential terrorists would communicate with each other in this new global, connected world—and they could find them by identifying patterns in this massive amount of new information. Once these groups were identified, they could then follow their digital trails everywhere.

**Sergey Brin and Larry Page, computer-science boy wonders**

In 1995, one of the first and most promising MDDS grants went to a computer-science research team at Stanford University with a decade-long history of working with NSF and DARPA grants. The primary objective of this grant was “query optimization of very complex queries that are described using the ‘query flocks’ approach.” A second grant—the DARPA-NSF grant most closely associated with Google’s origin—was part of a coordinated effort to build a massive digital library using the internet as its backbone. Both grants funded research by two graduate students who were making rapid advances in web-page ranking, as well as tracking (and making sense of) user queries: future Google cofounders Sergey Brin and Larry Page.

The research by Brin and Page under these grants became the heart of Google: people using search functions to find precisely what they wanted inside a very large data set. The intelligence community, however, saw a slightly different benefit in their research: Could the network be organized so efficiently that individual users could be uniquely identified and tracked?

This process is perfectly suited for the purposes of counter-terrorism and homeland security efforts: Human beings and like-minded groups who might pose a threat to national security can be uniquely identified online before they do harm. This explains why the intelligence community
found Brin's and Page's research efforts so appealing; prior to this time, the CIA largely used human intelligence efforts in the field to identify people and groups that might pose threats. The ability to track them virtually (in conjunction with efforts in the field) would change everything.

It was the beginning of what in just a few years’ time would become Google. The two intelligence-community managers charged with leading the program met regularly with Brin as his research progressed, and he was an author on several other research papers that resulted from this MDDS grant before he and Page left to form Google.

The grants allowed Brin and Page to do their work and contributed to their breakthroughs in web-page ranking and tracking user queries. Brin didn't work for the intelligence community—or for anyone else. Google had not yet been incorporated. He was just a Stanford researcher taking advantage of the grant provided by the NSA and CIA through the unclassified MDDS program.

The MDDS research effort has never been part of Google's origin story, even though the principal investigator for the MDDS grant specifically named Google as directly resulting from their research: “Its core technology, which allows it to find pages far more accurately than other search engines, was partially supported by this grant,” he wrote. In a published research paper that includes some of Brin's pivotal work, the authors also reference the NSF grant that was created by the MDDS program.

Instead, every Google creation story only mentions just one federal grant: the NSF/DARPA “digital libraries” grant, which was designed to allow Stanford researchers to search the entire World Wide Web stored on the university's servers at the time. “The development of the Google algorithms was carried on a variety of computers, mainly provided by the NSF-DARPA-NASA-funded Digital Library project at Stanford,” Stanford's Infolab says of its origin, for example. NSF likewise only references the digital libraries grant, not the MDDS grant as well, in its own history of Google's origin. In the famous research paper, “The Anatomy of a Large-Scale Hypertextual Web Search Engine,” which describes the creation of Google, Brin and Page thanked the NSF and DARPA for its digital library grant to Stanford. But the grant from the intelligence community's MDDS program—specifically designed for the breakthrough that Google was built upon—has faded into obscurity.

Google has said in the past that it was not funded or created by the CIA. For instance, when stories circulated in 2006 that Google had received funding from the intelligence community for years to assist in counter-terrorism efforts, the company told Wired magazine founder John Battelle, “The statements related to Google are completely untrue.”

Did the CIA directly fund the work of Brin and Page, and therefore create Google? No. But were Brin and Page researching precisely what the NSA, the CIA, and the intelligence community hoped for, assisted by their grants? Absolutely.
The CIA and NSA funded an unclassified, compartmentalized program designed from its inception to spur something that looks almost exactly like Google.

To understand this significance, you have to consider what the intelligence community was trying to achieve as it seeded grants to the best computer-science minds in academia: The CIA and NSA funded an unclassified, compartmentalized program designed from its inception to spur the development of something that looks almost exactly like Google. Brin’s breakthrough research on page ranking by tracking user queries and linking them to the many searches conducted—essentially identifying “birds of a feather”—was largely the aim of the intelligence community’s MDDS program. And Google succeeded beyond their wildest dreams.

**The intelligence community’s enduring legacy within Silicon Valley**

Digital privacy concerns over the intersection between the intelligence community and commercial technology giants have grown in recent years. But most people still don’t understand the degree to which the intelligence community relies on the world’s biggest science and tech companies for its counter-terrorism and national-security work.

Civil-liberty advocacy groups have aired their privacy concerns for years, especially as they now relate to the Patriot Act. “Hastily passed 45 days after 9/11 in the name of national security, the Patriot Act was the first of many changes to surveillance laws that made it easier for the government to spy on ordinary Americans by expanding the authority to monitor phone and email communications, collect bank and credit reporting records, and track the activity of innocent Americans on the Internet,” says the ACLU. “While most Americans think it was created to catch terrorists, the Patriot Act actually turns regular citizens into suspects.”

When asked, the biggest technology and communications companies—from Verizon and AT&T to Google, Facebook, and Microsoft—say that they never deliberately and proactively offer up their vast databases on their customers to federal security and law enforcement agencies: They say that they only respond to subpoenas or requests that are filed properly under the terms of the Patriot Act.

But even a cursory glance through recent public records shows that there is a treadmill of constant requests that could undermine the intent behind this privacy promise. According to the data-request records that the companies make available to the public, in the most recent reporting period between 2016 and 2017, local, state and federal government authorities seeking information related to national security, counter-terrorism or criminal concerns issued more than 260,000 subpoenas, court orders, warrants, and other legal requests to Verizon, more than 250,000 such requests to AT&T, and nearly 24,000 subpoenas, search warrants, or court orders to Google. Direct national security or counter-terrorism requests are a small fraction of this overall group of requests, but the Patriot Act legal process has now become so routinized that the companies each have a group of employees who simply take care of the stream of requests.
In this way, the collaboration between the intelligence community and big, commercial science and tech companies has been wildly successful. When national security agencies need to identify and track people and groups, they know where to turn – and do so frequently. That was the goal in the beginning. It has succeeded perhaps more than anyone could have imagined at the time.

Sign up for the Quartz Obsession email
THE SURVEILLANCE GAP: THE HARMS OF EXTREME PRIVACY AND DATA MARGINALIZATION

MICHELE GILMAN and REBECCA GREEN

ABSTRACT

We live in an age of unprecedented surveillance, enhanced by modern technology, prompting some to suggest that privacy is dead. Previous scholarship suggests that no subset of the population feels this phenomenon more than marginalized communities. Those who rely on public benefits, for example, must turn over personal information and submit to government surveillance far more routinely than wealthier citizens who enjoy greater opportunity to protect their privacy and the ready funds to secure it. This article illuminates the other end of the spectrum, arguing that many individuals who may value government and nonprofit services and legal protections fail to enjoy these benefits because they reside in a “surveillance gap.” These people include undocumented immigrants, day laborers, homeless persons, and people with felony conviction histories suffering collateral consequences of their convictions. Members of these groups often remain outside of the mainstream data flows and institutional attachments necessary to flourish in American society. The harms that surveillance gap residents experience can be severe, such as physical and mental health injuries and lack of economic stability, as well as data marginalization and resulting invisibility to policymakers. In short, having too much privacy can be as injurious as having too little.

The sources of the surveillance gap range from attempts to contain and control marginalized groups to data silos to economic exploitation. This article explores the boundaries of the surveillance gap, evaluates how this emerging concept fits within existing privacy paradigms and theoretical frameworks, and suggests possible solutions to enhance the autonomy and dignity of marginalized people within the surveillance gap.

∞ Venable Professor of Law and Director, Clinical Legal Education, University of Baltimore School of Law. For their helpful feedback, the authors wish to thank the participants at the Privacy Law Scholars Workshop at the U.C. Berkeley School of Law in 2017, including danah boyd, Matt Cagle, Danielle Citron, Gautam Hans, Anna Lauren Hoffman, Margaret Hu, Sarah Igo, Mary Madden, Aaron Massey, Charles Raab, Andrew Selbst, and Luke Stark. We also thank Laura Heymann.

∞∞ Professor of Practice; Co-Director of the Election Law Program, William & Mary Law School.

253
I. INTRODUCTION

Although we live in a highly surveilled society, some people among us are functionally invisible. For example, low-wage workers—many of whom are undocumented immigrants—toil out of sight in an underground economy. A lack of a conventional paper trail or pay stub system linking workers to employers exposes these workers to potential wage theft and dangerous working conditions. While these workers are perilously out of reach of government and nonprofit organizations that could otherwise provide assistance, they are also subject to heightened forms of surveillance, typically under the increasingly watchful eye of agencies like Immigration and Customs Enforcement. Likewise, homeless persons' lives are defined by extremes: although they tend to live their lives in public, they are simultaneously governed by laws that criminalize their behavior, steadily pushing them out of view. Tellingly, when former Governor of Virginia Terry McAuliffe sought to restore the ability to vote to constituents who had committed felony crimes, his office was unable to find thousands of people—people who at one point spent time in the prison and parole systems where their whereabouts were always known to authorities. These examples illustrate that

1. See Stephen Lee, Policing Wage Theft in the Day Labor Market, 4 U.C. IRVINE L. REV. 655, 659–60 (2014) (“A coarse definition of day labor is temporary work in which the work, and often the workers, lack documentation.”).

2. Infra Part II.B.

3. See Howell v. McAuliffe, 788 S.E. 2d 706, 710 (2016) (“McAuliffe’s Executive Order stated that it removed the political disabilities of approximately 206,000 Virginians who had been convicted of a felony but who had completed their sentences of incarceration and any periods of supervised release, including probation and parole.”); ACLU OF VA., ACLU OF VIRGINIA
marginalized people experience privacy differently than most Americans. Specifically, they experience privacy extremes—being seen or tracked too much or too little.

Existing privacy scholarship has largely focused on the harms derived from too little privacy, and, in this vein, several scholars have highlighted the particularly intense surveillance of low-income people. This article examines the other end of the spectrum—the surveillance gap. Life in the surveillance gap can be isolating, stigmatizing, dangerous, and harmful to a person’s physical and mental health. For one, legal protections available to other members of society remain out of reach to those in the surveillance gap. People also lose out on potential sources of economic and social support, because those who seek to provide services to disadvantaged members of our society often find it nearly impossible to reach them. Moreover, those who fall within the surveillance gap are not included within big data streams that ultimately shape public policy, thus leaving out their experiences and needs from the calculus that goes into creating policy. Frustratingly, the challenges facing these groups remain invisible, further entrenching these groups’ marginalization.

The surveillance gap has multiple causes, ranging from data silos to poor data sharing, and from benign neglect to administrative systems that purposefully exclude certain people. This article seeks to identify and understand the causes, contours, and consequences of the surveillance gap and to outline legal and policy tools for addressing it. Part II provides case studies of populations living in the surveillance gap, including undocumented immigrants, day laborers, homeless persons, and people with felony conviction histories. Part III situates the surveillance gap within several scholarly streams. First, it assesses the surveillance gap through the lens of scholarship that differentiates between privacy harms experienced by varying groups. Second, it builds on insights from feminist legal theory involving the public/private binary and the harms associated with having too much privacy, wrestling with the tensions identified by feminists between
liberalism’s ideals and individuals’ lived realities. Third, it examines notions
of “choice” and “consent” in consumer and criminal privacy law, testing whether
such frameworks are meaningful with regard to marginalized groups. Fourth, it
adds a new dimension to emerging concepts of privacy as contextual. Fifth, it
reviews fundamental rights theory’s impact on the surveillance gap, positing that
the gap cannot be found in legal regimes that view privacy as a fundamental
human right, such as in the European Union. Part IV suggests ways to address
harms that arise in the surveillance gap while also respecting desirable forms of
privacy and the dignity and autonomy of marginalized persons.

II.
LIFE WITHIN THE SURVEILLANCE GAP

The rise of the surveillance state is well documented. Both state and non-
state institutions routinely record individual actions to an unprecedented degree.
Americans have famously been warned: “[p]rivacy is dead, get over it.” The so-
called death of privacy stems from two main sources. First are the increasingly
sophisticated tools that the government uses to monitor and track the populace.
Fear of the government’s abuse of these tools has prompted some federal and state
laws to protect Americans’ privacy, although government surveillance at all
levels is ever expanding and broader than most people realize. The second source
derives from the private sector. To say that companies have come to appreciate
the value of consumer data is a gross understatement. Companies now regularly
collect, aggregate, buy, and sell consumer data on virtually every aspect of
people’s lives, including buying preferences, health status, criminal and voting
histories, and physical whereabouts. For the modern citizen, this level of
surveillance can be a form of control; it can be benign, helpful, or harmful, often

6. See generally MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON (1977);
DAVID GARLAND, THE CULTURE OF CONTROL: CRIME AND SOCIAL ORDER IN CONTEMPORARY
SOCIETY (2001); Kevin D. Haggerty & Richard V. Erickson, The Surveillant Assemblage, 51 BRITISH
J. SOC. 605 (2000).

7. See Jeffrey Bellin, eHearsay, 98 MINN. L. REV. 7, 18 (2013) (discussing source of the quote);
see also Mary Kay Mallon & Eugene Scott, Comey: ‘There Is No Such Thing as Absolute Privacy
in America’, CNN (Mar. 9, 2017), http://www.cnn.com/2017/03/08/politics/james-comey-privacy-
cybersecurity/index.html [https://perma.cc/F6XG-9ULF]; Marshall Kirkpatrick, Facebook’s
Zuckerberg Says the Age of Privacy Is Over, READWRITEWEB (Jan. 9, 2010, 9:25 PM),
https://readwrite.com/2010/01/09/facebooks_zuckerberg_says_the_age_of_privacy_is_over/ [https:
/perma.cc/T537-NKJD].

8. See, e.g., the Privacy Act, 5 U.S.C. § 552a, and the Electronic Communications Privacy Act,
3121–26 (2012)), and their state equivalents.

9. See generally JENNIFER STISA GRANICK, AMERICAN SPIES: MODERN SURVEILLANCE, WHY
YOU SHOULD CARE, AND WHAT TO DO ABOUT IT 9–26 (2017).

10. See generally DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE
depending on the perspective of the surveilled. Increasingly, large-scale data sharing between different levels of government and private industry blurs public/private distinctions. For instance, marketers build profiles of Americans using data from public databases and individual online browsing histories, while government agencies such as law enforcement purchase predictive analytic systems from private companies, which build their algorithms using combined public and private sources of data. Together, government and private-sector surveillance have created the sense that Americans are universally tracked and that few—except those living purposely “off the grid”—are able to evade government or private-sector surveillance.

While this lack of privacy has raised increasingly vocal concerns, the contemporary phenomenon of non-surveillance—that is, systemic invisibility of large portions of certain classes of people living in the United States—has received less attention. We call this the “surveillance gap,” although we acknowledge that the term is imperfect. While the concept of surveillance is commonly associated with government control of its citizenry, some of the harms that we identify occur in the private sphere. Indeed, we adopt a broader notion of “surveillance” altogether, including all “focused, systematic, routine attention to personal details for purposes of influence, management, protection or direction.” This article thus tracks gaps within a variety of public and private surveillance systems, some of which overlap. We address our attentions to populations that remain outside seemingly omnipresent surveillance systems. The surveillance gap is a condition of invisibility in relation to mainstream society, as well as a difference in how marginalized groups experience privacy.

The phenomenon of “the uncounted” is not new. For decades, certain groups have been left out of this country’s most basic counting exercise: the U.S. Census. Since its inception, the census has suffered from not just inaccuracies, but also what is referred to as the “differential undercount,” or the routine counting of some classes of people more accurately than others. Historically, the classes of

14. By “gap” we do not refer to a space that must be bridged—indeed, for many individuals, the surveillance gap provides a crucial coping mechanism and resistance against oppression. As we discuss infra Part IV, the solution for the surveillance gap is not increased surveillance, but rather opportunities for marginalized groups to exercise greater autonomy and enhance their dignity.
individuals who have received a less accurate count included children, renters, residents of large cities, and racial minorities. This differential undercount is the census equivalent to the surveillance gap. In recent years, the Census Bureau has been forthright about such data collection problems for certain groups, even identifying in a 2016 report a list of groups that present the greatest challenge to its data collection efforts. The Census Bureau uses statistical extrapolation to “count” many who fall in one or more of these categories.

Data marginalization in the U.S. Census has real consequences for policy-making in this country, because it impacts federal and state resource allocation, environmental priorities, and even the power of the ballot. The federal government uses census data to allocate hundreds of billions of dollars each year. Education, welfare, transportation, and a myriad of other federal programs allocate funds based on census figures. A perfect example of this reality relates to the core purpose of the U.S. Census: apportionment, or the allocation, based on

---


17. The full list of categories includes: children, homeless people, lower-income individuals, those with lower education, non-English-speaking people and/or people who do not have social security numbers, members of racial or ethnic minorities, people who do not have smart phone or Internet access, older individuals, people who live in rural areas, persons with disabilities, people who are angry with the government, and people who live in group quarters. See Memorandum from Director John H. Thompson to Chair Ditas Katague, U.S. Dep’t of Commerce, U.S. Census Bureau (Oct. 26, 2016), https://www2.census.gov/cac/nac/reports/2016-10-responses-admin_internet-wg.pdf [https://perma.cc/X84J-QP8B].


a state’s population size, of representatives in the U.S. House of Representatives. When, as is routinely the case, populations are regularly left out of the count, those populations are, by definition, under-represented. As Samuel Issacharoff and Allan Lichtman explain, “[i]t is evident that problems surrounding the undercounting of identifiable groups have predictable political consequences . . . The undercount results in the underrepresentation of areas of minority concentration, particularly inner-city neighborhoods, to the benefit of wealthier suburban and some rural areas.”

The “undercount” problem—and controversy over how best to cure it—has consistently plagued census data. In the lead-up to the 2020 Census, the Census Bureau convened a working group focused on improving counting of “Hard to Count” (HTC) groups. The working group considered (1) making greater use of local data and imagery, (2) encouraging respondents to use the Internet and telephone, and (3) using administrative records and third-party private-sector databases. Tellingly, the working group ultimately recommended against using third-party databases and administrative records to find HTC populations, citing “racialized disparities” in those databases to conclude that they might exacerbate the problem. Mistrust and fear of government, particularly in minority and

---

22. Issacharoff & Lichtman, supra note 21, at 4.
26. U.S. DEP’T OF COMMERCE, U.S. CENSUS BUREAU ADMINISTRATIVE RECORDS AND THIRD PARTY DATA USE IN THE 2020 CENSUS WORKING GROUP FINAL REPORT 9 (2014), https://www2.census.gov/cac/nac/reports/2014_2020census_wg.pdf [https://perma.cc/YF3J-2TEL] (“The currently available and/or tested government administrative records (AR) exacerbate racialized disparities in the quality of data available to the Census Bureau. Such racialized disparities may be attributed to both ‘coverage’ issues and ‘response’ issues in the AR databases’ quality. Such administrative records databases better ‘cover’ the White population than racial minority populations and are also more likely to produce cross-database response agreement for the White population than for racial minority populations.”). The working group also acknowledged that the census’s use of administrative or other third-party records might violate the privacy interests of people who had shared their data with third parties:

Individuals disclose information within a particular purpose or context with rules in mind at the time of disclosure. When interacting with a firm, a website, another individual, individuals reveal information with an understanding as to who can see that information, how it might be used, and the context in which it is revealed. Disclosure of information is not synonymous with information being public—disclosure is done within expectations of privacy.

Id. at 10.
immigrant communities, seem likely to create additional problems for the count in 2020.27

Putting the undercount dilemma aside, this section examines several populations that evade, avoid, or (by design) fall outside the surveillance radar and discusses why. Though people living in the surveillance gap suffer differing experiences and harms, the case studies discussed below reveal several commonalities. First, the surveillance gap impacts some of the most marginalized and politically powerless groups in American society—undocumented people, day laborers, homeless persons, and people with felony conviction histories. Second, just as surveillance is used as a tool to “exert influence and reproduce power relations,” the surveillance gap can also serve as a social control mechanism.28 Torin Monahan explains that, when it comes to oppressed populations, “surveillance plays an important role in policing bodies and maintaining boundaries between inside and outside, self and other.”29 In other words, careful watching plays a social sorting function.30 The same can be said of the extreme privacy that characterizes the surveillance gap. Third, people resist surveillance systems in subtle and empowering ways,31 quietly reclaiming their humanity and asserting their rights. Fourth, people in the surveillance gap often lack fundamental legal rights or access to remedies that protect rights.

27. See Hansi Lo Wang, Run-Up to 2020 Census Raises Concerns over Security and Politics, NAT’L PUB. RADIO (Mar. 28, 2017), http://www.npr.org/sections/thetwo-way/2017/03/28/521789446/run-up-to-census-2020-raises-concerns-over-security-and-politics [https://perma.cc/RSK9-PE36] (“[T]he Census Bureau is facing its longstanding challenge of building up public trust. Kenneth Perritt, a former director of the Census Bureau who served under the Clinton administration, says he’s concerned that the immigration debate could determine the questions asked on the Census.”); Danny Vinik, Trump’s Threat to the 2020 Census, POLITICO (Apr. 9, 2017), http://www.politico.com/agenda/story/2017/04/trumps-threat-to-the-2020-census-000404 [https://perma.cc/C7DK-RVEC] (“If you imagine that the federal government is asking for personal information and you feel that the federal government is hostile and that if you were to answer this, perhaps they would use this against you,” said Terry Ao Minnis, director of the census and voting programs at Asian Americans Advancing Justice.”). Some believe that traditionally undercounted communities will be particularly aggressive advocates for getting counted in the 2020 round. See, e.g., Nick Visser, The U.S. Won’t Tally LGBT People in 2020 Census, HUFFINGTON POST (Mar. 29, 2017), http://www.huffingtonpost.com/entry/us-census-lgbt-americans_us_58db3894e4b0cb23e65c6ed9 [https://perma.cc/5E4E-PALJ] (suggesting that undercounted groups plan to fight for their representation).


29. Id.

30. See id. (“[S]urveillance is a mode of ‘social sorting’, of categorizing populations according to perceived risk or value and treating those respective groups differently.”) (internal citation omitted).

31. For example, some “welfare recipients resist by underreporting income, taking side jobs, engaging in barter economies, paying babysitters by letting them use their electronic benefit transfer (EBT) food-stamp cards, and so on . . . as ways for individuals to contest the stigmatized subjectivities that the state and others force upon them.” Id. at 193.
of privacy, Americans forgo the civic protections that a fundamental rights-based orientation offers. This lack of civic and legal protection plagues members of the surveillance gap. The next part explores potential ways to address the surveillance gap’s worst consequences.

IV.

BRIDGING THE SURVEILLANCE GAP

One potential fix for the harms that stem from the surveillance gap—at least if Europe’s experience is a guide—is surely out of reach: wholesale adoption of a fundamental rights theory of privacy. Socio-cultural norms are undoubtedly too ingrained to undo American aversion to state surveillance and cataloging of the populace. Nevertheless, a dignity-based understanding of privacy may allow for a reduction of the ill effects of the surveillance gap, as described below.

Closing the surveillance gap is difficult significantly because Americans want their liberty to be let alone.299 For many Americans, the existence of the surveillance gap is a manifestation of liberty. They may see the surveillance gap not as a problem, but as an outgrowth of a value that Americans hold dear: the right to disappear.

Additionally, the surveillance gap is a complex space, and one set of solutions is unlikely to address the contextualized harms that arise within it. It exists for multiple reasons, ranging from bias on the part of government actors, to economic advantage for employers, to the choice to remain by surveillance gap residents in the face of oppressive state systems or societal neglect. People in the surveillance gap constitute a huge cross-section of American society and hold diverse goals and interests. Even within the same sub-category of surveillance gap inhabitants, interests may diverge. For example, while many Virginians with felony conviction histories are thrilled to be “found” when it comes to regaining the right vote, others prefer to eschew all interaction with the state—including voting.300 Indeed, being counted is not necessarily a solution to extreme privacy because it can bring people into systems that are themselves harmful without transforming those systems.301

Finally, “solutions” to the surveillance gap are difficult to pinpoint because the causes of the surveillance gap are wildly intractable. Poverty, discrimination,
economic subjugation, and social control all feed the surveillance gap’s existence. If the surveillance gap is a consequence of these much larger forces, perhaps it is no more “solvable” than these large and deeply embedded social ills.

With these complexities in mind, this section offers measures that might, at least at the margins, address the ill effects of the surveillance gap. Our suggestions hinge on the dual concepts of resilience and resistance. With regard to resilience, Martha Fineman has explained how vulnerability is a universal and inevitable human condition; for instance, we all face periods in life when we are children, ill, or victims of accidents or disasters. Fineman thus urges creation of a “responsive state” that actively invests in enhancing the resilience of its vulnerable citizens. In her view, resilience is “what provides an individual with the means and ability to recover from harm, setbacks, and the misfortunes that affect her or his life.” Resilience is “largely dependent on the quality and quantity of resources or assets that he or she has at their disposal or command.” In turn, these resources are “accrued . . . within an array of social structures and institutions over which individuals may have little, if any control.” Currently, people in the surveillance gap show tremendous resilience in staying afloat, often through family and community support and sharply honed survival skills. Yet from a societal perspective, they are denied resources—such as education, job access, affordable housing, fair pay, or a voice in our democracy—that would build their resilience and ability to live with dignity, without fear or hardship. People in the surveillance gap currently develop resilience in the face of a restrained state, not with the support of a responsive state.

Resistance is another key element of bringing privacy into balance. Scholars have long noted how heavily-surveilled populations resist in subtle ways. Gilliom in his study of Appalachian welfare mothers described how welfare recipients resist government surveillance by seeking cash-only jobs to supplement their

303. Id. at 5, 19. (“Our current system has been built upon myths of autonomy and independence and thus fails to reflect the vulnerable as well as dependent nature of the human condition.”).
304. Id. at 13–15.
306. Id.
307. Id. at 623.
308. As an example, Fineman points to LGBT youth, who suffer high rates of homelessness, child welfare placements, and suicide due in part to a legal system that “valoriz[es] family privacy, parental rights, individual liberty, and choice.” Martha Albertson Fineman, Vulnerability, Resilience, and LGBT Youth, 23 TEMP. POL. & C.R. L. REV. 307, 309, 322 (2014); id. at 313 (“Looking at the child within the family from a vulnerability perspective makes it apparent that it is time to rend this veil of privacy and bring the child into focus as a political and legal subject who, independent of the family, deserves the attention and protection of law and policy.”).
income, accepting gifts such as diapers from family and friends, and taking similar steps to "quietly meet the needs of their dependents through daily actions that defy the commands of the state."\footnote{Gilliom, supra note 4, at 111.} Similarly, studies find that call-center employees resist surveillance by pretending to talk on the phone, leaving call lines open without customers on the line, and misleading customers.\footnote{Class Differential, supra note 4, at 1409–10.} Gilliom envisions a future in which "[e]veryday tactics of evasion, subterfuge, and concealment, then, may very well become a defining form of politics in the surveillance society."\footnote{Gilliom, supra note 4, at 101.} These tactics also describe daily survival in the surveillance gap. However, resistance within the surveillance gap can also look diametrically different; it often means coming into the sunshine. To climb out of the surveillance gap, marginalized groups benefit from organizing and demanding that they be seen. Some examples are illustrative. For day laborers, one of the most effective forms of resistance to the surveillance gap has been organizing through worker centers,\footnote{See generally Kimberly M. Sánchez Ocasio & Leo Gertner, Fighting for the Common Good: How Low-Wage Workers' Identities Are Shaping Labor Law, 126 Yale L.J. Forum 503 (2017), www.yalelawjournal.com/forum/fighting-for-the-common-good [https://perma.cc/ZV5Q-DS9N] (discussing successful organizing strategies for day laborers).} "community-based and community-led organizations that engage in a combination of service, advocacy, and organizing to provide support to low-wage workers."\footnote{Janice Fine, Worker Centers: Organizing Communities at the Edge of the Dream, 50 N.Y. L. Rev. 417, 419 (2005–2006).} Worker centers fill a regulatory and union gap. There are at least 150 of them, and they aim to engage workers in collective action within a social justice frame.\footnote{Id. at 431, 438; see also Héctor R. Cordero-Guzmán, Worker Centers, Worker Center Networks, and the Promise of Protections for Low-Wage Workers, 18 J. Lab. & Soc'y 31, 45 (2015).} One common strategy is to target employers who engage in wage theft by "calling employers and asking them to pay, filing wage claims, and picketing when they don't."\footnote{Fine, supra note 313, at 434.} These actions have targeted small employers as well as major chains such as Taco Bell, which was the subject of a boycott to improve working conditions and wages for tomato pickers.\footnote{Id. at 435.} Worker-center efforts have also been successful in coordinating enforcement with government agencies and enacting beneficial local and state legislation, such as a New York Unpaid Wages Law that increased the penalties on employers for wage theft.\footnote{Id. at 436–37.}

Most recently, a worker center in Jackson Heights, New York developed a smartphone app called Jornalera, which means "day laborer," that allows workers to track their hours and pay, take and upload pictures of work sites and employers, and share this information for legal and advocacy efforts.\footnote{Liz Robbins, New Weapon in Day Laborers' Fight Against Wage Theft: A Smartphone App, N.Y. Times (Mar. 1, 2016), https://www.nytimes.com/2016/03/02/nyregion/new-weapon-in-
a particularly powerful way to increase the autonomy of day laborers, who are in
the best position to gauge the level of privacy that they want to retain or shed.319
Overall, worker centers “provide the necessary mechanisms to increase the
transparency of the hiring process, effectively monitor employment conditions,
and provide opportunities for worker incorporation into the formal economy.”320
Day laborers who take advantage of worker centers are also associated with higher
rates of social inclusion and reduced isolation.321 Despite these successes, the vast
majority of day laborers are not served by worker centers, and worker centers
struggle to maintain funding.322 Further, the Trump administration is expected to
impose restrictions on worker centers to limit their effectiveness, such as
limitations on protest activities.323 Still, traditional organizing tools and new
technologies hold promise for day laborers in resisting the surveillance gap.

Additional, powerful examples of resistance to the surveillance gap arise in
the context of homelessness. Homeless people have used their visibility as a way
to fight the surveillance gap. For instance, in Seattle, a coalition of shelters and
tent camps called SHARE/WHEEL fought the city’s proposed HMIS mandatory
tracking system by threatening to move all residents into public parks.324 HMIS,
which gathers data about homeless persons for the ostensible purpose of assessing
needs and coordinating services, has been critiqued for presuming that
homelessness is a personal pathology created by poor life choices that requires
state intervention and management.325 Moreover, while HMIS captures data about

319. See Julia Ticona, New Apps Like Jornalero Aim to Protect Low-Income Workers. Here’s
How They Could Backfire, SLATE: FUTURE TENSE (Mar. 21, 2016, 11:18 AM),
http://www.slate.com/blogs/future_tense/2016/03/21/new_apps_like_jornalero_aim_to_protect_lo
w_income_workers_here_s_how_they.html [https://perma.cc/5WKA-XJBD] (pointing out that
potential shortcomings to this approach include a lack of consistent Internet access, unrealistic
expectations of documentation for all wage theft claims, and potential capture of data by government
surveillance).

320. VALENZUELA, THEODORE, MELÉNDEZ & GONZALEZ, supra note 73, at 836. Worker centers
also have a positive impact on wages. See id. at 849.

321. M. Anne Visser, From Economic Integration to Socioeconomic Inclusion: Day Labor
Worker Centers as Social Intermediaries, 38 URB. GEOGRAPHY 243, 260 (2017).

322. See Cordero-Guzmán, supra note 314, at 52; Lee, supra note 1, at 661; ON THE CORNER,
supra note 68, at 22–23 (citing a 2002 survey showing that only ten percent of day laborers in the
New York metropolitan area have turned to worker centers for assistance). Worker centers also face
the risk that if they are too successful, “they will be categorized as labor organizations and subjected
to the restrictions imposed by the labor laws.” Marion Crain & Ken Matheny, Beyond Unions,

323. Chris Opfer & Jasmine Ye Han, Worker Centers May Get Closer Look Under Trump,
[https://perma.cc/5ZZK-EG8L].

324. See Sparks, supra note 105, at 843.

325. See id. at 852. “What is more, appearing unkempt, carrying one’s belongings, and sleeping
on park benches have long been considered lifestyle choices, rather than survival strategies.”
Landegger, supra note 121, at 1039.
services used, it does not allow homeless persons to identify their own needs.326
Thus, for the Seattle movement, members sought "to maintain a space outside the
gaze of the state wherein the presumption of the pathology could be both avoided
and contested."327 The homeless individuals were less concerned about data
privacy (a pre-occupation of wealthier Americans when it comes to big data
collection), than about evading the stigma of homelessness. For this reason, Tony
Sparks argues that privacy rights are not simply carried by individuals; they also
populate physical space.328 Ultimately, the protest was successful. After lengthy
mediations, the city adopted an "opt-in" version of HMIS that did not require
individuals to offer information to receive services or require shelters to
participate as a funding condition.329

A project in Ann Arbor, Michigan involved having homeless people
photograph their everyday lives "as a way to document their struggles and
strengths . . . and to reach policy makers and the broader public about issues of
concern to homeless people."330 This project was part of a health-promotion
strategy called photovoice—with roots in feminist theory, documentary
photography, and critical education—which helps people to see connections
between their individual situations and root causes and to devise strategies for
change.331 Participants were recruited from local shelters and trained not only in
photographic methods, but also in the ethics and power dynamics involved in
photographing other people.332 After the photo shoots, participants discussed the
content and context of their photographs, and the photos they selected were
featured in local media, a gallery exhibition, and a forum at a public theater.333
Policy makers were surprised to learn that people living in shelters sometimes held
multiple jobs,334 and they had to confront the way that homeless people perceived
the building of a new homeless shelter on the outskirts of town.335 This process of
making their lives visible was powerful for the homeless participants—they
reported improvements to their self-esteem and quality of life and spoke of the

326. See Sparks, supra note 105, at 853.
327. Id. at 855.
328. See id. at 854–55.
329. See Sparks, supra note 105, at 857–58. The victory is "bittersweet" given that the outcome
might lessen federal funding for homeless services in Seattle. See id. at 858.
330. Caroline C. Wang, Jennifer L. Cash & Lisa S. Powers, Who Knows the Streets as Well as
the Homeless? Promoting Personal and Community Action Through Photovoice, 1 HEALTH
PROMOTION PRAC. 81, 81–82 (2000).
331. See id. at 82.
332. See id. at 83.
333. See id. at 84.
334. See id. at 85.
335. See id. ("The photovoice project did not substantively affect these plans [to build a
homeless shelter on the outskirts of town] but enabled board members, planners, community people,
and community leaders to rethink issues from the perspective of the homeless.").
ability to define their own lives outside the parameters that society placed on them.336

Homeless people’s visibility has led to the development of formal tactics to render them invisible. Nevertheless, from within the surveillance gap, homeless persons have resisted by re-asserting their visibility. In turn, “the presence of visible poverty forces society to confront inequality of income, education, health care, and criminal justice.”337 Ultimately, homeless people need autonomy to set their own privacy boundaries, a power that wealthier Americans already possess. “[W]hat homeless people . . . need more of is both publicity—through which their needs can be recognized as legitimate—and privacy—through which they can protect themselves from absorption and de-legitimization from the public.”338

Striking this balance is essential for other people in the surveillance gap as well. Marginalized people tend to live at privacy’s extremes. At either end of the spectrum, people lack control over their personal information and the degree to which they interact with mainstream institutions. Strategies that give people the autonomy to assert or shed privacy are essential to their individual dignity and to fulfilling our communal, democratic promise. The examples above show that grassroots organizing, driven by the objectives and insights of affected groups, can be powerful in enhancing autonomy. Professionals working with marginalized populations, such as social workers, lawyers, and community organizers, can assist in these grassroots movements by providing support to a group’s self-defined goals. Education about legal rights, remedies, and risks can help people in the surveillance gap make wise decisions about how to live their lives. For instance, many ex-felons in Virginia are unaware that they have the restored right to vote; without that knowledge, they cannot exercise an informed opinion about whether to register. Likewise, new technologies—as simple as a smartphone application—can be effective in helping people strike a privacy balance that calibrates to their needs.

In addition, some states have been receptive to building the resilience of undocumented persons. Consider, for instance, the twelve states, along with the District of Columbia and Puerto Rico, that allow undocumented immigrants to receive driver’s licenses and obtain insurance, so that they can drive, to work and elsewhere, without breaking the law.339 Certain states and localities are limiting

336. See id. at 85–86.
337. Rankin, supra note 105, at 52.
their law enforcement cooperation with federal immigration authorities “in
furtherance of important state interests involving their immigrant
communities.” These jurisdictions believe that their sanctuary stance enhances
public safety by encouraging immigrants to report crimes and by allocating
spending toward crime fighting rather than illegal-immigrant search
expeditions. In the current polarized political climate, advocacy at the state and
local level can sometimes be more fruitful in law reforms that aid marginalized
communities.

Lawyers should continue to develop robust visions of positive, constitutional
social rights, despite the current conception of a Constitution that protects
individuals only against government interference and thus fails those living in
the surveillance gap. In the 1960s and 1970s, a legal movement for constitutional
social and economic rights led the Court to adopt procedural due process rights
to protect governmental benefits and to invoke statutory interpretations that
increased access to benefits. While the Court became more conservative and
ultimately pulled back from an emerging theory of minimum social entitlements,
the future may cycle back, giving way to a more responsive state that pulls marginalized persons into the mainstream.

The first step in tackling the problems of the surveillance gap is to recognize
its existence and to acknowledge the harms it produces. From there, we can
integrate it into privacy discussions and create tools that enable residents of the
surveillance gap to fight against its worst consequences and to access social
supports on their own terms.

of its undocumented immigrant beneficiaries, enabling them to drive without fear of being stopped
by state or local police, arrested, detained, or fined, and thereby facilitating their daily access to
work, friends, and family.” Id. at 836.

MICH. ST. L. REV. 1197, 1199 (2016). Four states and about 633 counties have these policies. Jasmine
C. Lee, Rudy Omri & Julia Preston, What Are Sanctuary Cities?, N.Y. TIMES (Feb. 6, 2017),
WY1H].

341. See Armacost, supra note 340, at 1201.

342. See generally Sotirios A. Barber, Fallacies of Negative Constitutionalism, 75 FORDHAM

Present, 39 TULSA L. REV. 597, 606–12 (2013) (describing the Court’s doctrine in this era and
influence of legal scholars Frank Michelman and Charles Reich).

344. Id. at 612.

345. Cf. Goodwin Liu, Rethinking Constitutional Welfare Rights, 61 STAN. L. REV. 203, 210,
247 (2008) (arguing that the legitimacy of judicial enforcement of welfare rights depends on
evolving societal norms).
V. CONCLUSION

The current narrative within privacy law is that privacy is dead, or at least on life support. The loss of privacy threatens people’s sense of self and engagement in self-expression. Poor people and members of minority groups face great privacy incursions and may be subject to increasing forms of big-data discrimination. This article shines a light on a countervailing reality—the harms of having too much privacy in a society in which attachment to mainstream data streams, resources, and institutions is necessary to thrive. Many undocumented persons, day laborers, homeless persons, people with conviction histories, and others live within a surveillance gap, yet this phenomenon is rarely acknowledged in privacy discourse. The harms within the surveillance gap are serious, encompassing physical and mental injuries, big-data marginalization, economic instability, and loss of democratic participation. Like surveillance, the surveillance gap is a form of social control. It keeps people down.

In response, people living in the surveillance gap have shown incredible resilience, surviving day-to-day by engaging in multiple forms of resistance. But small triumphs do not transform the structural inequalities that perpetuate the gap. Accordingly, a vision of privacy and a framework for privacy law that balances the privacy interests of all persons and that does not simply reflect the assumed desires and needs of elites is needed. Marginalized communities should have a role in shaping a balanced vision of privacy that recognizes both the benefits and costs of privacy in differing contexts. Too little privacy is bad, but so is too much. The key going forward is to get the balance right.
In a world where nearly everything is being monitored, it is easy to feel hopeless about privacy. Often, when I tell people I have just met that I write about privacy, their immediate response is, “I’ve given up. Privacy is dead.”

In truth, I had kind of given up, too. For three years, I had been writing about the privacy invasions that technology had made possible. But I hadn’t done much to try to protect myself. I told myself that it was because I was too busy, but in fact I was overwhelmed by the impossibility of it.

After many such conversations, I started to feel guilty. Was my reporting about privacy invasions actually contributing to the hopelessness?

I am a natural optimist: I wanted to believe there was hope. I am also a born contrarian: I wanted to disprove the doubters. And finally, I am stubborn: I determined that I would find some hope.

So I decided, against all odds, to try to evade the dragnets. I would attempt to avoid being monitored during everyday activities such as reading and shopping. I would obscure my location—at home and while out and about. I would seal my e-mails and texts with the digital equivalent of hot wax. I would find ways to freely associate with people and ideas. I would try to find a way to protect my kids from building a digital trail that would haunt them later in their lives.
It was a daunting task. "I can't do it," I told a close friend. "How would I live without a credit card? Without a cell phone? It would be irresponsible to my children."

But I realized that my questions were exactly what I needed to examine: Was it possible to live in the modern world and evade the dragnets? Had I somehow consented to ubiquitous surveillance—trading my data for free services or security—as the people in the surveillance business contend? What would happen if I tried to withdraw my consent?

My first step was to identify the threats to my privacy.

In the computer security industry, identifying your adversaries is called building your "threat model." The idea is that you can protect yourself only against known threats. The computer security industry expert Bruce Schneier calls this the first lesson of security: security is a trade-off. "There's no such thing as absolute security," he wrote in the introduction to his book *Schneier on Security*. "Life entails risk, and all security involves trade-offs. We get security by giving something up: money, time, convenience, capabilities, liberties, etc." What you give up depends on what you are trying to protect and whom you are trying to protect it from.

Focusing on the wrong adversary can be disastrous. Consider the case of General David Petraeus, the former director of the Central Intelligence Agency.

In 2012, the FBI uncovered General Petraeus using a rather low-tech technique to conduct an extramarital affair with his biographer Paula Broadwell. Critics decried him for using a shared Gmail account, in which he and Broadwell left draft e-mails for each other—*Foreign Policy* magazine dubbed it "old spycraft." But the real problem was that the general had misjudged his adversary.

He and his mistress were trying to hide their affair from their spouses. In that case, a shared Gmail account, accessed from computers not in their homes, was sufficient protection. But they had not envisioned that the FBI would begin investigating Broadwell for sending threatening e-mails to a volunteer event planner in Tampa, Florida, named Jill Kelley. The FBI obtained the computer IP addresses from which the e-mails had been sent, most likely through a subpoena to Broadwell’s e-mail provider.
FBI agents traced those IP addresses to a variety of public unsecured Wi-Fi connections, including several hotels, and then sought hotel guest lists for the dates the e-mails had been sent. The FBI soon found that Paula Broadwell was the common guest at those hotels on those dates. And from there it was a short step to search Broadwell’s e-mail, via either a search warrant or subpoenas—and to discover her affair with Petraeus.

If the general and his mistress had attempted to outsmart the FBI, they would have at the very least needed to take steps to mask the IP addresses from which they logged in to their accounts, to use encryption, and to make sure their accounts were under fake names. Even then, there’s no guarantee they wouldn’t have been caught.

After all, perfect privacy is not possible, even if you identify your adversary correctly.

Consider another case: Theodore J. Kaczynski, the Unabomber. For a decade, Kaczynski lived as a hermit in a one-room cabin—with no electricity, plumbing, or telephone—in a remote area of Montana while conducting a series of bombings through the mail that killed three people and injured twenty-two others. But even the hermit could not evade the FBI forever. The FBI eventually tracked him down in his cabin due in large part to the fact that his brother stepped forward to provide an essay Kaczynski had written as a young man that could be compared to a linguistic analysis of his current writing.

And that is a good thing: society was better off when the FBI caught Kaczynski and ended his bombing spree. But the rest of us would be better off building our threat models.

What is my threat model?

I’m a working journalist with a son in preschool and a daughter in elementary school. My husband is a professor who travels overseas often for his research.

If I were to describe my family in one simple word it would be “busy.” We are always running in a million different directions. Privacy and security are exactly the kinds of things that fall through the cracks when you’re always in a rush.

And yet I want to protect myself and my children from indiscriminate
tracking. I want us to have the freedom to associate with people and places and ideas, without worrying about how those associations might constrain our future prospects.

I also want to protect myself against targeted threats against journalists. After all, the Obama administration has been extremely aggressive at prosecuting people who pass sensitive material to journalists. Since 2009, the administration has charged eight government whistle-blowers with allegations of violating the Espionage Act, a law that had been used just three times over the previous ninety-two years against government officials accused of providing classified information to journalists.

My concern is less about myself because it seems that the journalists don’t end up in jail too often. Sadly, it is the people who leak information to journalists who end up in jail. I want to be able to give my sources a pledge of confidentiality that I can honor.

So, really, I have two threats: indiscriminate tracking and targeted attacks against journalists and their sources.

When building a threat model, it’s also important to assess your own strengths and vulnerabilities.

My strength is that I have been writing about privacy and technology for several years, so I have an army of experts I can call on for help and guidance. I am also lucky that I do not have any privacy issues that I have to “clean up.” A few years ago, when my book about the social network MySpace was published, I worked to make my online reputation bulletproof. I conferred with search-engine optimization consultants who helped me build a website and sanitize my social network profiles so that my Google search results would be dominated by items I had written about myself, rather than items written by others about me.

Also, my kids are young and their data are not yet publicly available. The kids don’t have cell phones or computer access. They have limited access to the iPad and they don’t have any social media accounts (except for the ones that my daughter’s school has set up for her within their walled garden). So I don’t have a lot to “clean up” on their front, either.

But I have plenty of vulnerabilities. Probably my biggest issue is that I have no patience. I often take shortcuts instead of hunkering down to
figure out why my technology tools aren’t working. As a result, I am liable to leave myself vulnerable to exposure.

Another huge issue: my home address is known to the world. When my husband and I bought and renovated our home, I succumbed to the pleas of a colleague at the *Wall Street Journal* and blogged about the renovation for the newspaper’s online real estate section. Although I never published the exact address of our house, at least one blog identified it from the photos. So one basic building block of privacy is already gone.

My husband also doesn’t care about privacy. He is a professor, and he always jokes that if somebody broke into his files, the number of readers of his papers would double. Not only does he not care about privacy, but also his field of work is essentially privacy-invading. He is a mechanical engineer, and one of his projects is to install remote sensors to monitor energy usage. In fact, he installed energy sensors in our home without asking me. I only found out the day we were moving in and one of his graduate students was in the house finishing up the wiring for the system.

That said, the real-time energy monitors that he installed are actually kind of cool—we can see how much energy we’re using at any given time, and we can learn from our patterns of usage. Of course, it’s a little weird that his grad students are also monitoring our energy usage.

“What do you do on Fridays?” one of his students asked him one day. “Energy usage spikes on Fridays.” It turns out that our cleaning lady comes on Fridays and runs the vacuum cleaner.

My kids also don’t care about privacy. To them, “privacy” is just a word that means “no.” Privacy is why they can’t post videos on YouTube. Privacy is why I won’t let them sign up for kids’ social networks. Privacy is why I complain to their teachers about posting pictures of them on a non-password-protected blog.

In fact, my daughter thinks that privacy is something to be defeated. She delights in trying to guess my passwords. Once, she figured out my iPhone password, accessed my phone, changed the password, and then forgot what she changed it to, leaving me locked out and forcing me to do a factory reset to gain access to the device.

So I will be fighting this fight alone, at least on the home front. My fellow soldiers will be a ramshackle network of technologists, hackers, and concerned citizens around the world.
Now I needed a battle plan for how to defend myself. And I needed to determine how far I was going to go: Was I going to live in a bunker? Was I going to change my name?

I read a few books about protecting privacy and they were startlingly extreme. In *How to Be Invisible: Protect Your Home, Your Children, Your Assets, and Your Life*, J. J. Luna writes that “your journey to invisibility must begin with the first step: separating your name from your home address.” If your address is already publicly known, he advises moving.

Luna suggests setting up a limited liability company in New Mexico that owns your assets—house, car, and so on. He goes on to suggest that you cannot send your children to public school because that will reveal your address. “There are only two remedies for this danger,” he writes. “Either homeschool your kids or put them in a private school willing to guarantee their privacy.”

I can’t afford to put my kids in private school or to quit my job and homeschool my children. Nor do I want to pursue either of those options.

Luna’s privacy threat model? Private investigators. And even if you follow all of his advice, he says, a private investigator with unlimited funds will still be able to find you eventually.

In *One Nation, Under Surveillance*, Boston T. Party, the pen name of Kenneth W. Royce, writes that “the law no longer works because America has spun off her legal axis.” He advises readers to hoard their guns, grow their own food, homeschool their children, and boot up their computers from a CD containing an operating system called Puppy Linux.

His threat model is a hostile government that he perceives to be ready to strike at civilians.

I’m not that paranoid yet. I don’t believe that the government is a lost cause. I still believe in the legal system and that our system of checks and balances is mostly working. I’m not ready to start hoarding guns and growing my own food (aside from a few tomatoes and basil in the backyard each summer). And I’m not planning to start homeschooling, or to move to an all-cash economy.

I am trying to defend against a different threat: the rise of indiscriminate tracking—the dragnets that aim to capture every element of our lives
in a permanent record. I worry that this indiscriminate tracking will prevent me from associating with certain ideas and people, that it will cause me economic distress, and that it will create a culture of fear. At its worst, I am concerned that indiscriminate tracking could enable the creation of a totalitarian surveillance state.

To build my threat model, I consulted with experts of all kinds—from high-level government officials with security clearances to hackers who build anti-surveillance tools. Each had a different suggestion. For example, some advised me to use different computers for different purposes—one for banking, one for personal, one for professional; others recommended running software that would separate my single computer into three separate compartments, emulating a three-computer setup; others said there was no point in trying to compartmentalize, as my data would end up getting mixed up anyway. After many such conversations, I came to realize that there was no silver bullet.

I would have to come up with my own battle plan. I built a spreadsheet, outlining the threats and my proposed tactics to counter each threat. Some threats would likely be relatively easy to counter; to avoid online ad tracking, I would install different types of anti-tracking software and evaluate which one worked best. But other threats were trickier; I didn’t know a good tactic to counter automated license plate readers that would photograph my car’s plate when I drove past. One expert suggested that I could cover my license plate with a spray or a glass that could foil the infrared cameras. But in New York, where I live, it’s illegal to cover a license plate in a way that “distorts a recorded or photographic image of such number plates.”

I realized that before I chose my tactics, I needed to develop some guidelines to govern my behavior. So I developed my own rules of engagement.

**DON’T BREAK THE LAW.** I am not trying to evade taxes or break the law. So I will engage only in actions that are legal. That means not obscuring my license plate.

Sometimes it’s not clear what is legal. Consider fake driver’s licenses.
I asked Mark Eckenwiler, a former surveillance lawyer at the U.S. Department of Justice, for advice about whether fake IDs are legal.

Mark pointed me to the statute that makes it illegal to use someone else’s identification to commit a crime. But he also pointed me to a 2009 Supreme Court ruling that interprets the statute to mean that the offender must know that he is misusing the credentials of an actual person. That could imply that it’s acceptable to use a fake driver’s license for a fictitious person. But then he pointed me to the mail fraud and wire fraud statutes that state that it is illegal to engage in “any scheme” to obtain money or property by “false or fraudulent promises.”

Not surprisingly, Mark declined to give me official advice about whether to get a fake ID. However, the cases seemed to indicate that I probably would be safe with a fake ID in a fictitious name if I didn’t use it for any type of fraud.

But even so, I decided not to get a fake ID. I’d rather be on the safe side of the law.

CONTINUE TO LIVE IN THE MODERN WORLD. I am not interested in disconnecting from technology. I believe technology has empowered people to make great changes in the world. I simply want to limit the harmful downsides of a technology-saturated life.

As a result, I won’t be able to achieve perfect privacy. With a talented and determined adversary, almost any measure can be circumvented. John J. Strauch, a former CIA agent who is now a security consultant, told me a story about how he was hired to break into the headquarters of a well-protected financial entity that had three rings of guards stationed outside. So he smuggled in an infiltrator in the trunk of an unsuspecting employee’s car.

Similarly, most of the actions I will take can be circumvented. For instance, if I use codes to scramble the contents of an e-mail, an adversary could still install software on my computer that captures my keystrokes before they are encrypted.

My goal is not to win at all costs. My goal is simply to force my adversary to work harder. I may not be able to prevent myself from being surveilled on public streets, but perhaps I can force my adversary to watch hours of videotape rather than simply track my location through a series of easily analyzed GPS coordinates.
USE CONVENTIONAL TOOLS. In his delightful book about industrial food, *The Omnivore's Dilemma*, Michael Pollan prepares a meal by hunting and gathering. He kills a pig, hunts mushrooms in the forest, and picks cherries from a neighbor’s tree. He calls it the “perfect meal.”

Some of my hacker advisers take a similar approach to technology. They don’t trust tools they can’t build, modify, or design themselves. They circumvent the software installed on their phones in order to run software of their choosing. They boot their computers from CDs rather than running a traditional operating system.

This may be the “perfect” way to protect one’s data, but it is sadly out of reach for me. I am tech-savvy enough to manage my own website, but I don’t trust myself to start modifying my phone software. Nor do I think that it is the right approach. The beauty of the modern era is that these powerful technologies are finally simple enough for regular people to enjoy their benefits.

And so, as a corollary to my guiding principle of living in the modern world, I am also going to eschew some of the most extreme measures taken by the kill-your-own-food hacker crowd. Instead, I will use conventional tools that are within reach of most people with some amount of tech savvy. (I will not pretend that your grandmother can do everything that I’m going to do. But certainly your teenager will be able to.)

AIM FOR ZERO DATA RETENTION. The best way to protect my data is not to give it away. And the best way to do that is to use services that don’t store data.

Of course, such services are rare, but they do exist. Consider my doctor’s office, which is located in a midtown Manhattan skyscraper. Like most New York buildings post 9/11, the doormen demand identification from visitors. But my doctor’s office wants to protect patient privacy. So the doctor’s office assigns each patient a code to give to the doorman instead of identification. That way, the doormen are appeased and yet they have zero data stored about the patients.

During my journey, I will seek to do business with companies that store the least amount of data that is sufficient to complete their task. In some lucky cases, that will be zero data. In other cases, it will be minimal data.
**USE THE MUD-Puddle TEST.** One way to determine whether I have minimized my data trail is to use what some security engineers call the “mud-puddle test.” It goes like this: imagine you drop your device in a mud puddle, slip in the mud, and crack your head so that you forget your password to access your data. Now, can you get your data back from the service you were using? If the answer is yes, then you have left a data trail. If the answer is no, you have successfully avoided leaving a data trail. Of course, you also don’t have your data.

The problem with the mud-puddle test is that you lose either way. But it’s a good reminder that if you are using a service that lets you recover your lost password, then the service has access to your data. I will use the mud-puddle test to evaluate the services that I use.

**ENGAGE IN DATA POLLUTION.** When I can’t minimize my data trail, I can try to pollute it by using fake names and providing misinformation.

It’s embarrassing to admit that lying is hard for me. It makes me physically uncomfortable to lie—even if I am just putting a fake name into a Web form. I start to feel hot and my pulse starts racing.

But the fact is that I have nothing to be ashamed of. Until recently, anonymous transactions were the norm for many daily activities. We paid cash. We called from phones that didn’t have caller ID. We sent letters that sometimes didn’t have return addresses.

So I vow to remind myself that the people asking me to fill out forms online in order to accomplish simple tasks don’t always deserve truthful answers. It’s a difficult path for a girl who was such a Goody Two-shoes in elementary school that I used to stay in at recess and clean chalkboards for the teachers.

But I will try to make data pollution a key part of my privacy arsenal.

**PROTECT MY TRAFFIC.** I plan to work hard to protect myself against analysis of my “traffic,” that is, the people with whom I e-mail, call, and instant message.

People worry about the contents of their e-mails, texts, and instant messages being intercepted. But traffic analysis can often reveal as much or more than the contents of a message. If I am exchanging six messages a day with a drug dealer, do you really need to know what we are saying?
The volume of messages alone will land me on a list of suspected affiliates of drug dealers.

Computers are also much better at analyzing lists of to/from to find patterns than they are at sorting through huge amounts of text for patterns. As a result, indiscriminate trackers will almost always focus on traffic patterns first. So I will put a top priority on defending my traffic patterns.

**USE REAL-TIME COMMUNICATIONS.** The Wiretap Act requires police officers to get a "super-warrant"—which is harder to get than a regular search warrant—before intercepting real-time communications such as phone calls, video chats, and instant messages in the United States.

Once those communications are stored, however, the data can often be obtained without a search warrant. So a good way to avoid being tracked is to use real-time communications and not store the communications. (Unless, of course, you are actually a criminal suspect and the police have obtained a super-warrant to intercept your real-time communications—in which case, good luck to you.)

It's not easy to turn off storage of texts and instant messages, particularly because you often can't control whether the recipient is storing the information. But, luckily, most voice and video discussions are not stored by default.

As a result, plain old-fashioned domestic telephone calls are still one of the most private ways to communicate.

**SPREAD DATA AROUND.** The only thing worse than losing a credit card is losing your entire wallet. Similarly, losing some data is not as bad as losing all of your data. So I will endeavor to spread my data around—in order to minimize the damage from inevitable leaks, data breaches, government spying, and so forth.

For example, I will have to choose which among Google's many services I will retain—e-mail, search, maps, and Android phone. Considering that in the last half of 2012 alone, the government made 21,389 requests for information to Google, it makes sense not to store all of my valuable data on Google's computers.

Of course, there is no way to completely avoid having some data stored
in a vulnerable database—unless I decide to store all my data at home. But I hope that by spreading my data around, I can mitigate the risk of exposure.

**PAY FOR PERFORMANCE.** Many of the hackers who build privacy-protecting technology are adherents of the free software movement. They believe that users should be able to build and modify the software that they use, so that they are not trapped in systems they do not control.

Theoretically, free (as in freedom to modify) software does not need to be free (as in price). But in reality, most profit-seeking companies prefer not to open up their code to outside tinkering. And so most free-to-modify software ends up being free-in-price.

The unfortunate result is that without a revenue stream, much of this software withers from neglect when the programmers who built it for free in their spare time move on to other hobbies. So in my quest to protect my privacy, I will aim to support (through donations or purchasing software) projects that pay their programmers a living wage, in the hope that the project will continue.

**TRANSPARENCY RULES.** Trackers who let me see the data they have about me are less offensive than trackers who will not let me view my data.

Transparency is the key. I feel better about my credit report because I have a chance to review it and dispute any errors I find. But most companies that track my movements won’t show me the data they hold about me. That feels unfair. So I plan to take a more generous approach toward trackers that provide transparency. And I will be even kinder to trackers who let me delete my data, correct it, or download it and take it with me.

**PRIVACY AS PROTEST.** I always ask for a pat-down instead of going through the body scanners at the airport. The pat-down is very invasive: one time the screener stuck her hand a little too deep into my pants when patting down my waistband; another time, the scanner pulled my waistband away from my back with such force that I almost fell over. In many ways, it’s more invasive than the automated scanners.

But my purpose in opting out of the scanner is simply to register my protest against the procedure. The body scanners are the rare form of indiscriminate tracking that is not covert, and so I take the opportunity
to contribute my voice to the opposition. I view it as similar to recycling at home. The cans and bottles that I dutifully separate are not likely to change the fate of the planet. The miles that I drive in my car are much worse, ecologically speaking. But recycling is a kind of gateway drug; it makes larger changes seem within reach.

It is my hope that my small privacy protests will make larger changes seem within reach.

**DON’T SUCCUMB TO FEAR.** It’s likely that taking steps to protect my privacy could land me on a “red flag” list of possible suspects.

Federal prosecutors have argued in an Arizona case that the defendant had no reasonable expectation of privacy because he used a fake name to sign up for a prepaid wireless card.

And NSA documents revealed by Edward Snowden show that the NSA is storing encrypted communications of U.S. citizens, even though its own guidelines say that “domestic communications will be promptly destroyed.” But messages that contain “secret meanings” can be retained, meaning that my encrypted e-mails are likely placing me on some kind of red flag list at the NSA.

But I don’t want to succumb to fear that my privacy-protecting actions will land me on a watch list. Instead, I plan to count those red flags as part of my political protest against the dragnets.

In some ways, this new world that I am entering is familiar to dissidents in repressive regimes: a world where quiet conversations in a café are safer than phone calls, e-mails, and other electronic communications.

To understand the life I was embarking on, I reached out to a man who has deeply examined the challenges faced by dissidents—Mike Perry, a developer at the Tor Project, which makes software designed to help people evade censorship and surveillance. After 9/11, Perry was outraged at the privacy invasions of the Bush administration, so he started volunteering as a computer programmer for Tor. He began taking his privacy seriously.

When he was looking at technical material on Amazon with his boss and the director of engineering, he was bothered that he was seeing personalized recommendations for books on political and personal topics.
He decided that even Amazon recommendations were too “personal” for him, so he began erasing his data trail.

Perry and I met in a park in San Francisco. (Public places are apparently good places to have private conversations as long as you don’t use trigger words such as “bomb” that cause people to listen carefully, according to John Strauchs.) Perry looked like your basic issue hacker—skinny, slightly pale, and clad in all black. He told me some of the basics of his operational security (although not all, since that would compromise his security).

Perry describes himself as a “surveillance vegan”—by which he means that he is as strict about avoiding surveillance as vegans are about avoiding animal products. (His two exceptions: he still books plane tickets and sometimes stays in hotels under his own name.)

Even his closest friends don’t know where he lives, although some of them have tracked him to the city block on which he lives. (His family visited once but they don’t have the exact address.) One friend even dropped a prepaid cell phone enabled with GPS into his bag in a fruitless effort to locate him.

He receives mail in several places, including a Laundromat, a UPS box, and a “business box” that allows him to get packages under other names. He also uses multiple disposable phones. He pays cash for prepaid phones that are designated for different relationships. One is for official business, one is for personal business, and another is for communicating with Tor. “I try to keep different topics to different phones,” he told me. He tries to remove the batteries from the phones when he is not using them.

Perry believes in using multiple disposable identities that are specific for each relationship. That means that he sets up multiple e-mail and instant messaging addresses. After our talk, he set up a dedicated instant messaging address for me to reach him. He said he would delete it after our conversations were complete.

Perry’s life sounded challenging. I asked how it had affected him.

“To be honest,” he said, “it’s affected my ability to have close relationships.” He said his surveillance-avoidance techniques contributed to breakups with two girlfriends and made it difficult to keep in touch with several friends who didn’t want to keep a dedicated encrypted chat program open in order to talk to him.
This was starting to sound like a young man’s game. After all, Perry is a single man who works from home. I’m a mom with two kids who goes into an office every day. It was going to be hard for me to run my life out of a Laundromat, with multiple phones for each person with whom I communicate.

But in his gentle way, Perry assured me that he was probably doing it all wrong anyway and that I didn’t have to be a surveillance vegan. “Some people are only ‘surveillance flexitarian,’ and that’s cool too,” he said.

Then he took the muni train with me to my destination. He walked me out of the station to my parking garage. Then he went back inside the subway, heading home—wherever that might be.
You should know your data,” Michael Sussmann told me, over a late breakfast at a café near Capitol Hill.

Sussmann, a former federal prosecutor in the Department of Justice’s computer crimes and intellectual property section, had been out late the night before. A devoted Bruce Springsteen fan, he had driven two and a half hours with his wife to see the Boss play in Charlottesville, Virginia. Sussmann was bleary-eyed but had kindly agreed to help me build my threat model.

“It’s boring,” he admitted, but audits are usually the first thing he does for his clients. Sussmann is now a partner at the law firm Perkins Coie, where he advises companies such as Google on Internet privacy issues. “We start with an org chart and then begin to find out every bit of data this company collects, from every source,” he told me.

He raised a good point: if I didn’t know where my data was, how could I protect it? For me, however, the challenge was not to locate my data internally; it was to locate it externally. So I decided to begin my privacy quest by trying to find my data.
I started with the most obvious sources of data—Google, Facebook, and Twitter, the companies I’ve called the Freestylers. What did they know about me?

To find my Google data, I visited the website of the Data Liberation Front, a quirky Google project that lets users download the data that they have stored with Google. Using the Data Liberation Front’s “take-out” menu, I downloaded the contacts for 2,192 people whom I have e-mailed since I started using Gmail in 2006. I also got a few photos I had stored on Picasa (Google’s photo service, which I had forgotten I used). And I pulled down twelve documents that I had shared with people using Google Drive (but not all 204 that had been shared with me by others).

But that was about it. When I tried to download the history of websites I have visited, the Data Liberation Front declared: “There is no current way to escape from Google Web History.”

I found a bit more information on my Google Dashboard—a page that contains information about my activity on various Google services that was buried in my Gmail account settings. The Dashboard noted that of the 2,192 people I’ve contacted on Gmail, the person I contact the most is—not surprisingly—my husband. It also noted that I have had 23,397 e-mail and chat conversations on Gmail.

Strangely, my Web search history wasn’t on my dashboard. It was hidden away in a section of my account called “Other Tools.” There, I found that Google had apparently been logging my Web searches from the time I opened my account in 2006. Apparently, I conduct hundreds, and sometimes thousands, of Google searches per month!

Google had helpfully sorted my searches by date and by category (maps, travel, books, etc.), and they were a horrifying insight into what Buddhists call the “monkey mind,” leaping from place to place restlessly.

Consider November 30, 2010: I started the day reading some technology news. Then, suddenly, I was searching for “Pink glitter tiny toms” for my daughter. Then I was off to the thesaurus to look up a word for an article I was writing, then to OpenTable to book a restaurant reservation, and then a visit to Congress to download the text of privacy legislation. Phew.

My searches not only illuminated my inner thoughts, but they also revealed my whereabouts. A bunch of searches for “Berlin city map” were conducted during my trip to Berlin; “Hyatt Regency Pune” was in the midst
of my annual trip to see my in-laws in India; my search for “DFW airport, Irving, TX → 3150 Binkley Ave., Dallas, TX 75205” was during a business trip to Dallas.

This was more intimate than a diary. It was a window into my thoughts each day. I felt nostalgic perusing my searches for nursing pillows after my son was born and my searches for good Mexican restaurants during a family vacation in Arizona.

I really wanted to download the data. But there was no way to easily get it. A Google spokesman, Rob Shilkin, told me, “There are lots of products that are not a part of Takeout—we started with five products in 2011 and have been steadily adding.” He added that I could delete my Web history. But once I had seen it, I didn’t want to delete it. I wanted to own it.

Facebook was considerably less forthcoming with my data. I clicked on “Download a copy of my data,” and Facebook sent me an archive that was notable for what it did not include. It did not include my list of friends, my posts, likes, or comments on other people’s posts. Instead, my Facebook archive contained a few photos I thought I had deleted, friends I had deleted, and a comprehensive list of when and from where I had logged in to my Facebook account (mostly my home, my office, and a few business trips). It turns out that the posts and likes are in another section of Facebook called the “Activity Log.” But it, too, was weirdly incomplete. My activity log contained only a few posts, no likes, and no comments. And it couldn’t be downloaded.

My Facebook data were a pale shadow of what Max Schrems got when he obtained his data from Facebook in 2011. Schrems, a law student in Vienna, requested his data from Facebook under European privacy laws and received 1,222 pages of personal data. Not only did it list all his friends, his posts, and so forth. It also had a lot of data that Schrems thought he had deleted—friend requests that he had rejected, pokes he had removed, and wall posts and status updates that he had deleted.

In August 2011, Schrems filed a complaint with the Irish Data Protection Commission (Facebook’s European offices are in Ireland) alleging that much of the data stored by Facebook violates European Union data protection laws. The European Union requires holders of personal data to be transparent about their data collection practices and to keep data only as long as necessary for the purpose for which it was collected.
As a result, the Irish commission reviewed Facebook’s practices and recommended some “best practices,” including better explanations of its policies around deleted content. A year later, Facebook changed its data use policy and stated explicitly that “information associated with your account will be kept until your account is deleted.” In 2012, the Irish commission reviewed Facebook’s compliance and found that the company had implemented “most” of its suggestions. But the agency found that Facebook was still not providing fully verified account deletion “beyond all doubt.”

In short, it seemed that Facebook planned to keep my data—whether or not I deleted it. But I wasn’t likely to obtain a comprehensive set of my Facebook data anytime soon.

Getting my data from Twitter was easy. I simply pressed a button labeled “Request your archive.” Twitter promptly sent me an e-mail with a handy Excel spreadsheet containing my 2,993 tweets since I opened my account in 2008.

It wasn’t always this easy. Twitter didn’t give users an opportunity to download their entire archive of tweets until 2012—even though since 2010 it had been offering similar data to companies who paid to subscribe to the entire Twitter stream in order to monitor trends.

My tweets were less intimate than my Google searches. Many were an extension of my work—tweeting articles by colleagues or myself and live-tweeting at events. But there were some tweets I had forgotten. On March 9, 2009: “My first night of real sleep in an entire year—baby finally slept thru the night. Hallelujah.”

In total, the Freestylers had compiled a pretty revealing portrait of my life over the past few years. It was far more comprehensive than any of the files I had reviewed from the Stasi archive.

And yet, as creepy as it was, much of it made me nostalgic. This was a digital record of my life.

It reminded me of the time that I ran into a friend and her husband at the playground in our neighborhood in Manhattan. As we watched our daughters—who are the same age—play on the jungle gym, the husband asked me about the articles I had been writing regarding privacy.

“I used to care more about privacy,” he said. I braced myself for the usual “I have nothing to hide” argument. But he surprised me with an entirely different approach. He said he realized that he “liked the idea of
leaving artifacts” about his life more than he worried about his privacy. In short, he said, all this data were providing “immortality.”

Looking at my old tweets and Google searches, I couldn’t help but think of my talk with my friend’s husband. Of all the arguments for ubiquitous data collection, immortality did seem like a good one.

I got another glimpse at immortality when I peeked at the information that data brokers have about me. This happened when I was sitting on Mike Griffin’s deck overlooking Chesapeake Bay in the Baltimore suburbs. Mike is a “repo” man who stumbled into the automobile surveillance business. He is tall and thin and filled with nervous energy. He seems to subsist entirely on coffee and cigarettes.

I was doing research for an article about the rise of automated license plate readers and decided to pay Mike a visit. He runs one of the largest private license plate snapping operations in the United States. His fleet of ten camera-equipped cars logs three hundred to four hundred miles a day, scanning plates in the Baltimore and Washington, D.C., metropolitan areas. Each month, his two shifts of drivers collect data about the location of one million plates.

Mike primarily uses the data to spot cars that are wanted for repossession. The technology has boosted his captures to fifteen cars a night, up from about six per night without the cameras. But Mike says his ultimate goal is to sell access to his data to bail bondsmen, process servers, private investigators, and insurers. “In the next five years, I hope my primary business will be data gathering,” he told me.

He mused about one possible buyer for the data: a company called TLO. I had been hearing about TLO for years. The founder, Hank Asher, was legendary. A former drug smuggler turned law enforcement buff, Asher was the most flamboyant guy in the data brokerage business.

Asher made millions through owning a business that painted high-rise buildings in Florida and retired at thirty. He moved to Great Harbor Cay in the Bahamas, drove a fast boat, flew a twin-engine Aerostar, and developed a cocaine habit. Eventually, after agreeing to fly a few loads of cocaine to Florida, he realized he’d gone too far. He quit cold turkey and decided he wanted to clean up drug smuggling on the island.
He started working with the U.S. Drug Enforcement Administration and noticed that the agency needed better databases. In 1992, he launched a product called AutoTrack that would change the data-collection industry.

AutoTrack was a better way to search public records: Asher bought data from the Florida Department of Motor Vehicles and made it easily searchable. Suddenly police could look up a person’s driving and vehicle records just by searching an address or part of a social security number or fragment of a name. Previously, police had to enter a person’s entire name, gender, and birth date to obtain a plate. AutoTrack changed the way police investigations were done. Journalistic investigations, too. I’ve used AutoTrack many times to find the names and addresses of people I was investigating.

Eventually, however, Asher’s flamboyance and drug history caught up with him, and his company bought him out for $147 million. Undeterred, Asher soon started another company with a very similar product called Accurint. After 9/11, he put together a program called MATRIX that would create a “High Terrorist Factor” list, but it ran aground on privacy concerns. Again, Asher resigned from his company under pressure.

In 2009, Asher made another run at the business, founding a database company called TLO, standing for The Last One, as in the last one he planned to launch. He turned out to be right about that; he died at age sixty-one in 2013.

Mike said TLO’s data were good and cheaper than data provided by LexisNexis, which years earlier had bought Asher’s two previous firms. TLO charged only 25 cents to conduct a simple search and $5 for an advanced search. By comparison, LexisNexis’s PeopleWise service charged $1.95 for a basic report and $24.95 for a premium report.

“Can I see my report?” I asked.

“Sure,” he said.

In less than a minute I was holding a four-page report, containing all my previous addresses—dating back to the number on my dorm room in college: #536B. There was not a single piece of inaccurate information in the report.

It took my breath away. I had forgotten the number on my dorm room, the address of the group house in Washington, D.C., that I had shared with five other recent college graduates, and my brief tenure in a New
York City studio before moving in with my husband. Each address brought back a wave of memories.

This was, in some ways, even deeper than the data the Freestylers had about me. After all, this was my real life, dating back decades. Talk about immortality.

As I sought out my information from other data brokers, my love affair with immortality lost steam. I compiled a list of more than two hundred commercial data brokers, and I was pretty sure I hadn’t identified all of them. This wasn’t immortality, this was prostitution.

Some of them were well-known names, like the credit-reporting agency Experian. But most were tiny outfits in the voyeuristic “look-up” business—websites that let people look up information about other people for a small fee, or sometimes for free in return for selling advertising.

There are very few barriers to entry in the lookup business. Consider the story of BeenVerified.com. In 2007, Josh Levy and Ross Cohen decided to offer cheap online background checks. The two set up shop with a $200,000 investment. By 2011, the company said it had revenues of $11 million, and just sixteen employees. Not bad work if you can get it.

The U.S. data business is largely unregulated, which is not the case in most western European countries. Those countries require all data collectors to provide individuals with access to their data, the ability to correct errors in the data, and, in some cases, the right to delete the data.

After reading the fine print on 212 websites, I learned that only 33 of them offered me a chance to see the data they held about me. But upon closer examination, not all of them were real offers. Some required me to set up accounts in order to see my data.

I contacted twenty-three data brokers and received my data from thirteen of them. Some asked me to send my requests by postal mail, along with a copy of my driver’s license. Others allowed e-mail requests. Most of the responses I got were from the biggest players in the industry.

Epsilon, one of the largest direct marketers, with more than $3 billion in annual sales, sent me a sparse two-page report identifying my name, address, age, and political affiliation. It listed recent purchase categories in extremely broad categories—apparel, media, business, health, home office, and sports. The most specific information was a description of my
household interests: cycling, running, and sports. For someone who hasn’t
gotten on her bike in five years, that is more aspiration than reality.

I was shocked that Acxiom, the data-gathering giant with annual sales
of around $1.1 billion, asked me to send a $5 check as a processing fee to
obtain my data. But I sent it in, gritting my teeth. One month later, Acxiom
sent me a nine-page report with my social security number, birth date,
voter registration, and addresses dating back to childhood. None of the
information that Acxiom sells about my interests was provided. Acxiom’s
reluctance to share was particularly galling, since it brags in its annual
report that it has more than “3,000 propensities for nearly every U.S. con-
sumer.” One of its main products is the PersoniX database, which lumps
people into seventy “clusters” within twenty-one “life stage groups.”

Thanks to the journalist Dan Tynan, who does great work covering
privacy issues, I found a page on Acxiom’s website that lets you enter
your age, marital status, income, and age of children to determine your
PersoniX cluster. When I entered my real information (which was a bit
scary), Acxiom reported back that I was in a cluster called “Fortunes and
Families”—“one of the most educated and wealthy of all the groups.” Peo-
ple in this cluster are more likely to have attended graduate school (yep)
and be Asian (yep, that’s my husband). Also true: “Their busy lives make
Internet shopping a necessity rather than a preference.” However, the
stock photo on the “Fortunes and Families” cluster was a little absurd—a
picture of a man and a woman standing in front of a private jet. We’re not
private-jet wealthy. We’re not even business-class wealthy. We are strictly
coach class.

Other Acxiom clusters have names like “Truckin’ and Stylin’,” “Mar-
rried Sophisticate,” “Urban Scrambler,” “Rural Rover,” and “Lavish Life-
style.” However, it’s not clear which cluster Acxiom has actually assigned
me to, since its demonstration website doesn’t ask for names. Acxiom
later introduced an online service that would let people see their data if
they entered their name, address, birth date, e-mail address, and last four
digits of their social security number. I was reluctant to hand over so
much sensitive information but, once again, I gritted my teeth and sub-
mitted my information. The resulting demographic data were remarkably
poor: Acxiom said I was a single Asian parent, with a seventeen-year-old
child, who drives a 2009 Toyota Corolla—all of which is incorrect. How-
ever, the shopping data were impressive: it correctly flagged that I prefer
online shopping over off-line shopping and identified categories in which I had spent money, such as linens, housewares, and “women’s apparel—underwear and hosiery.”

Datalogix, which claims to have data on “almost every U.S. household and more than $1 trillion in consumer transactions,” took three months to respond to my request. But one day a FedEx envelope arrived containing two sheets of paper from Datalogix listing my “interest segments.” It was a mishmash. Yes, I am a “mom” and a “foodies” and an “online buyer” of “women’s fashion & apparel,” but calling me a “fashionista” and “young and hip” is likely a bridge too far.

Similarly, my family does buy energy-efficient lightbulbs and organic milk, but I was surprised that this qualified us as “green consumers” and “health food” purchasers. And some data were outright wrong: we have no pet and no television, thus we have never purchased any “pet supplies” nor have we watched “Spanish language television.”

Other Datalogix categories were deliberately obscure. “Political views” and “political geography” were among my interest categories, but the report did not disclose what views they believe I hold. Similarly, my household income and home value were listed as categories but not disclosed.

Infogroup merely sent me an e-mail containing my name and address—the same information that I had provided in order to access my dossier. Gee, thanks.

I got better results from LexisNexis, another giant in the field. Four days after I submitted my request, LexisNexis mailed me a free ten-page “Accurint Person Report,” containing every address I’ve lived at since 1989.

Like the TLO report, it was disturbingly accurate. It had captured the one month I spent at my parents’ house while looking for an apartment in San Francisco in 1996. It grabbed the two months that I spent living in my boss’s attic while interning at the Washington Post in 1992. Under “Possible Associates,” it listed my husband and his mother, and dates that she had visited him in his New York apartment.

Thomson Reuters’s Westlaw was the most generous, kindly sending me two free reports: a thirty-four-page “summary” that was mostly correct except for listing my brother as the head of my household and an eight-page “comprehensive” report that listed my license plate, mortgage information, and employer. The Westlaw comprehensive report was the only
report I saw that listed the sources from which it obtained my historical addresses—all were from credit-reporting agencies.

Some companies’ offers of access seemed to be little more than window dressing. Intellius, one of the largest of the online people-search sites, which had $150 million in sales in 2010 (the last year that this information was publicly available), offered a website called TrueRep.com that allows users to see their data. However, the service was not advertised on any of the Intellius sites that I found. And when I visited TrueRep to find my data, it didn’t work. After I contacted the company, it fixed the “bug” and I was able to access my data—first I had to answer a set of personal questions, such as when my house was built and what model car I drive. Strangely, once I passed those questions, the report didn’t provide any details about my house and car. Obviously, Intellius must have more information that it is not disclosing, though it did report the correct names of my parents, husband, and brother. But it had two incorrect addresses for me—one in the Bronx and one at the United Nations.

Still, on average, the data brokers were largely correct about me. They correctly located most of my addresses and relations. And in large part they correctly identified me as a harried working mom, prone to choose convenience over thrift.

I hoped I would find even more accurate information in the one realm of commercial data brokerage that is regulated—the credit scoring industry.

The Fair Credit Reporting Act, enacted in 1970, requires anyone who uses a credit report, and some other types of reports, to provide people with notice if they suffer an “adverse action” such as being turned down for a job, insurance, or a loan because of data in the report. That notice must provide information about the data gatherer who provided the information. However, until recently, people couldn’t easily access their reports before being turned down for something.

In 2003, Congress passed a law requiring the big three credit-reporting agencies—TransUnion, Experian, and Equifax—to provide free annual access to credit reports from AnnualCreditReport.com. However, those free reports do not include the actual credit “score” on which consumers are judged.

When I requested a free copy of my credit report from TransUnion,
my first clue that the data were wrong was when I couldn’t correctly answer the security question designed to verify my identity: “Which two of the following five employers have you worked for?” I had worked for only one of the companies on the list, but I couldn’t get past that question until I clicked on two companies. So I chose one at random and got into my report anyway. Hmm, so much for security. (Turns out I wasn’t the only one to notice that the security questions were easy to circumvent. In March 2013, it was revealed that hackers had answered security questions and obtained credit reports for public figures ranging from First Lady Michelle Obama and FBI director Robert Mueller to celebrities Beyoncé and Paris Hilton, which were then posted online.)

When I got into my credit report, I saw that it listed me as working for a company called Borjomi 1 Inc. as of 1/30/2011. A quick Web search suggested that Borjomi 1 Inc. was a Brooklyn-based distributor of bottled mineral water from the republic of Georgia. It also listed a garbled previous address for me: “304 06920304 T75 Apt 79.”

My experience was not unusual. The latest review of credit report accuracy by the Federal Trade Commission determined that 26 percent of people found at least one significant error on at least one of their three reports.

I soon found even worse data about myself in an unregulated corner of the data broker industry—the data-scoring business.

I stumbled on this arena when I received my data from a company called eBureau. It was a one-page report that indicated that I had no children, had not completed high school, and had an income of $35,000—all of which are far from the truth.

With a bit of research, I discovered that eBureau was a hot new startup in the field of data scoring—where companies use widely available personal data to create new categorizations of people. There are companies that analyze the popularity of your tweets and Facebook posts to determine if you are “influential.” And there are a bunch of companies aiming to use new sources of data—such as personality or mobile phone behavior—to develop alternative credit scores.

Based in Chicago and founded in 2004, eBureau is trying to build a better credit score and has raised $38 million from venture capitalists for
its predictive “scoring” system. The company says it analyzes information about people and predicts their “contactability” and “lifetime customer value” so that marketers can decide whom to target. eBureau promotes its scores as helping people with limited banking and credit histories obtain financial services and allowing debt collectors to predict the likelihood of collecting on an account. In a marketing sheet for its “income estimator,” eBureau says its scores can be used to evaluate “newly admitted hospital patients for charity care program eligibility.”

When I contacted eBureau about the inaccuracy of my data, I received an e-mail from “eBureau Compliance” noting that some of its data was labeled as estimates. In addition, the company noted that it “secures its information from third-party sources and neither eBureau nor its information providers, vendors, licensors, agents or affiliates warrant that the information is accurate or error free.” It said that if my information was inaccurate, I could opt out; I availed myself of the offer.

Even creepier was a company called PYCO, which claimed it might be able to determine my personality type based on just my name and address. In its marketing materials, PYCO says it has created an “algorithm to reverse-engineer the data on a person’s behavior—relationships, transactions, activities, interests, hobbies, purchase behavior, and so on.” PYCO obtains data from the big data brokers and analyzes certain life decisions and translates what they might mean about your personality. For example, getting married can mean willingness to make a commitment. It then uses that data to determine things such as if you are extroverted or introverted or if you are a leader or a follower.

PYCO says it has built profiles for 181 million U.S. adults. But it said it didn’t have one for me.

Finally, I sought to extract my data from the U.S. government. Obviously, the National Security Agency was not going to give me my files (others have tried and failed to get those), but some other agencies might.

The Privacy Act, passed in 1974, gives individuals the right to see their government files and to correct the information in those files if it is incorrect. But the Privacy Act has a giant loophole; agencies can exempt themselves from provisions of the law.

As a result, it’s not easy for individuals to obtain their files. Consider
the story of an Ohio resident named Julia Shearson who was flagged as “armed and dangerous” and a “suspected terrorist” when she drove up to a U.S. Customs and Border Protection checkpoint after a weekend in Canada in 2006. Federal agents detained her and her four-year-old daughter for several hours before releasing them.

Shearson, who is a convert to Islam, wanted to know why she had been placed on a terrorist watch list. So she requested her files from Customs and from the Department of Homeland Security under the Freedom of Information Act and the Privacy Act. But the data she received did not include the reason she was targeted. So she sued the agencies for violating the Freedom of Information Act and the Privacy Act. They responded that they were exempt from providing information about the watch list.

Shearson obtained some documents in 2008 but was never able to find out why she was flagged. In 2011, the U.S. Court of Appeals for the Sixth Circuit ruled that if the government had unlawfully maintained records of First Amendment protected activity, it could be held liable for damages. The case was remanded to a lower court. Shearson settled for damages in 2013, after more than seven years of legal battles.

Still, I figured I would see what I could get about myself. I requested my FBI files and was informed that it had no records for me (phew!) but that this response “neither confirms nor denies the existence of your subject’s name on any watch lists.”

My request to the U.S. Customs and Border Protection agency proved more fruitful. About three months after I filed my request, I received a fat envelope full of data—a fairly speedy response by government standards.

For help interpreting the files, I called Edward Hasbrouck, a San Francisco–based independent travel writer who worked in the travel industry for fifteen years. He had requested his own records after the U.S. Customs agency revealed in November 2006 that it had begun using a system of records called the Automated Targeting System (ATS), which compiled travel records for U.S. citizens for the purpose of “risk assessment.” He initially submitted a request for ATS records in 2007 and renewed his request in 2009. A year later, he sued the agency, alleging that its refusal to turn over his complete Customs files was a violation of the Privacy Act. He lost when a federal court said that it was legitimate for Customs to retroactively exempt his files from the Privacy Act, even after he
requested them. Hasbrouck agreed to look at my files and help me decode them.

The first eight pages were from the TECS database—an updated and modified version of the former Treasury Enforcement Communications System—which is a kind of super-database that includes data from various parts of the Treasury Department and the Department of Homeland Security. My TECS file contained information about my international arrivals and departures dating back to 1990. For each crossing, it noted the airport, date and time, and a blacked-out category called “result” that Hasbrouck said was likely to be an indication of whether I was sent for secondary screening.

It was a limited peek at my travel history. The airline flights included my arrival time in the customs hall, but not where I was flying to or arriving from. There was only one “VEH” vehicle crossing—when I crossed into Canada at Niagara Falls in 2003.

A much more robust view of my travel was contained in a second set of documents—thirty-one pages of detailed international travel reservation information from a database called PNR, which stands for Passenger Name Records.

PNRs didn’t used to be in government hands. They are commercial records held by the airlines. But after the 9/11 terrorist attacks, Congress hastily passed the Aviation and Transportation Security Act, which required the airlines to provide their commercial reservation data to the Customs agency “upon request.” In typical fashion, “upon request” soon became codified as requiring the airlines to give the agency electronic access to the entire airline reservation databases.

Now, airlines routinely contribute their customers’ international travel reservations to Customs and Border Protection’s Automated Targeting System—which assesses the “risk” that individual travelers pose to the United States. The agency says that it uses the reservation data for five years but stores it for counterterrorism purposes for fifteen years.

After 9/11, European governments objected to this change, arguing that it violated European privacy laws. After a protracted legal and diplomatic battle, during which the European Court of Justice briefly invalidated the agreement, the Europeans eventually gave in and signed a deal. After all, they didn’t want their citizens to lose the right to visa-free travel to the United States. And they did win some concessions—there are limits
on how long the United States can store and use PNR data, and sensitive data may be accessed only on a “case-by-case” basis.

I understood that battle once I looked at my files. Each PNR was incredibly detailed, containing every single interaction, from the initial making of the reservation to the boarding of the plane.

My full credit card number was in there several times, as were my e-mail address, my birth date, my passport number, and all of my phone numbers—work, home, and cell. My fellow travelers’ information was there as well—my husband’s e-mail address, my children’s birth dates, and all of our passport numbers. My children’s names (they were identified as CHD 1 and CHD 2) and our meal requests were the only information that appeared to be redacted.

Hasbrouck deciphered the cryptic instructions that the airlines use to communicate in their mainframe systems. “OSIY TCP-4PAX-RELOC 5CLMWQ/5BUOEM” was an all-system message alerting airline staff that my family wanted to sit together to complete a party (TCP) of four passengers (4PAX) despite having two separate reservations in two different record locators (RELOC).

It appeared that my corporate travel agency was also contributing information to the federal government. For a trip to London, the agency sent Customs my hotel reservation (Bloomsbury Hotel, queen bed), my corporate credit card number and expiration date, my employee ID number, my department budget code, and an internal code indicating that I was “NOT VIP.”

Even more troubling, the agency had sent the government the “purpose of travel” field that reporters fill out when booking a trip. That description is forwarded to a reporter’s boss for approval.

Luckily, I am super-paranoid, so I write only “conference” or “reporting trip” in those fields. But I’m sure some of my colleagues might have written more extensive descriptions of their plans. It’s not at all far-fetched to imagine that some reporters have written in that field something like: “reporting trip to meet government whistle-blower John Smith in Maryland.”

I called up our attorneys at the Wall Street Journal, and they were surprised that reporters’ travel plans were being sent to the government. After looking into it, a spokeswoman told me that the problem was inadvertent and isolated to international travel on one particular air carrier. The Journal suspended travel on that carrier until the technical glitch
could be fixed. "We are working closely with our travel agency to resolve this matter as quickly as possible," she told me.

In the meantime, detailed information about my reporting trips was sitting in government files and being analyzed for my terrorism risk. And there was nothing I could do to remove it.

My audit was deeply unsettling. I had obtained only a tiny amount of the information available about myself. And even this tiny amount was disturbingly comprehensive. It included:

- Every address I had lived at dating back to college.
- Every phone number I had ever used.
- The names of nearly all my relatives (as well as in-laws).
- A list of nearly three thousand people with whom I exchanged e-mail in the past seven years.
- Records of about twenty-six thousand Web searches I had conducted every month dating back seven years, neatly sorted into categories such as "maps" and "shopping."
- A glimpse of my shopping habits.
- My internal communications with my employer, the Wall Street Journal, about reporting plans.

Most of my data were held by commercial data brokers. But all of it could be easily swept into government dragnets.

I couldn't help but compare my data to the Stasi files I had reviewed, with their rudimentary surveillance and limited windows into people's lives. Even in their wildest dreams, the Stasi could only fantasize about obtaining this amount of data about citizens with so little effort.
DRAGNET NATION

A QUEST FOR PRIVACY, SECURITY, AND FREEDOM IN A WORLD OF RELENTLESS SURVEILLANCE

JULIA ANGWIN

ST. MARTIN'S GRIFFIN NEW YORK
I don't use Facebook. I'm not technophobic — I'm a geek. I've been using email since the early 1990s, I have accounts on hundreds of services around the net, and I do software development and internet protocol design both for work and for fun. I believe that a globe-spanning communications network like the internet can be a positive social force, and I publish much of my own work on the open web.

But Facebook and other massive web companies represent a strong push toward unaccountable centralized social control, which I think makes our society more unequal and more unjust. The Cambridge Analytica scandal is one instance of this long-running problem with what I call the "surveillance economy." I don't want to submit to these power structures, and I don't want my presence on such platforms to serve as bait that lures other people into the digital panopticon.

But while I've never "opted in" to Facebook or any of the other big social networks, Facebook still has a detailed profile that can be used to target me. I've never consented to having
Facebook collect my data, which can be used to draw very detailed inferences about my life, my habits, and my relationships. As we aim to take Facebook to task for its breach of user trust, we need to think about what its capabilities imply for society overall. After all, if you do #deleteFacebook, you'll find yourself in my shoes: non-consenting, but still subject to Facebook's globe-spanning surveillance and targeting network.

There are at least two major categories of information available to Facebook about non-participants like me: information from other Facebook users, and information from sites on the open web.

When you sign up for Facebook, it encourages you to upload your list of contacts so that the site can "find your friends." Facebook uses this contact information to learn about people, even if those people don't agree to participate. It also links people together based on who they know, even if the shared contact hasn't agreed to this use.

For example, I received an email from Facebook that lists the people who have all invited me to join Facebook: my aunt, an old co-worker, a friend from elementary school, etc. This email includes names and email addresses — including my own name — and at least one web bug designed to identify me to Facebook's web servers when I open the email. Facebook records this group of people as my contacts, even though I've never agreed to this kind of data collection.

Similarly, I'm sure that I'm in some photographs that someone has uploaded to Facebook — and I'm probably tagged in some of them. I've never agreed to this, but Facebook could still be keeping track.

So even if you decide you need to join Facebook, remember that you might be giving the company information about someone else who didn't agree to be part of its surveillance platform.

Information from sites on the open Web

Nearly every website that you visit that has a "Like" button is actually encouraging your browser to tell Facebook about your browsing habits. Even if you don't click on the "Like" button, displaying it requires your browser to send a request to Facebook's servers for the "Like" button itself. That request includes information mentioning the name of the page you are visiting and any Facebook-specific cookies your browser might have collected. (See.) This is called a "third-party request."

This makes it possible for Facebook to create a detailed picture of your browsing history — even if you've never even visited Facebook directly, let alone signed up for a Facebook account.

Think about most of the web pages you've visited — how many of them don't have a "Like" button? If you administer a website and you include a "Like" button on every page, you're helping Facebook to build profiles of your visitors, even those who have opted out of the social network. Facebook's “Share” buttons on other sites — along with other tools — work a bit
differently from the “Like” button, but do effectively the same thing.

The profiles that Facebook builds on non-users don't necessarily include so-called "personally identifiable information" (PII) like names or email addresses. But they do include fairly unique patterns. Using Chromium's NetLog dumping, I performed a simple five-minute browsing test last week that included visits to various sites — but not Facebook. In that test, the PII-free data that was sent to Facebook included information about which news articles I was reading, my dietary preferences, and my hobbies.

Given the precision of this kind of mapping and targeting, "PII" isn't necessary to reveal my identity. How many vegans examine specifications for computer hardware from the ACLU's offices while reading about Cambridge Analytica? Anyway, if Facebook combined that information with the "web bug" from the email mentioned above — which is clearly linked to my name and e-mail address — no guesswork would be required.

I'd be shocked if Facebook were not connecting those dots given the goals they claim for data collection:

> We use the information we have to improve our advertising and measurement systems so we can show you relevant ads on and off our Services and measure the effectiveness and reach of ads and services.

This is, in essence, exactly what Cambridge Analytica did.

**Consent**

Facebook and other tech companies often deflect accusations against excessive data collection by arguing "consent" — that they harvest and use data with the consent of the users involved.

But even if we accept that clicking through a "Terms of Service" that no one reads can actually constitute true consent, even if we ignore the fact that these terms are overwhelmingly one-sided and non-negotiable, and even if we accept that it's meaningful for people to give consent when sharing data about other people who may have also opted in — what is the recourse for someone who has not opted into these systems at all? Are those of us who have explicitly avoided agreeing to the Facebook terms of service simply fair game for an industry-wide surveillance and targeting network?

**Privilege**

I don't mean to critique people who have created a Facebook profile or suggest they deserve whatever they get.

My ability to avoid Facebook comes from privilege — I have existing social contacts with whom I know how to stay in touch without using Facebook's network. My job does not require that I use Facebook. I can afford the time and expense to communicate with my electoral representatives and political allies via other channels.
Many people do not have these privileges and are compelled to "opt in" on Facebook's non-negotiable terms.

Many journalists, organizers, schools, politicians, and others who have good reasons to oppose Facebook's centralized social control feel compelled by Facebook's reach and scale to participate in their practices, even those we know to be harmful. That includes the ACLU.

Privacy should not be a luxury good, and while I'm happy to encourage people to opt out of these subtle and socially fraught arrangements, I do not argue that anyone who has signed up has somehow relinquished concerns about their privacy. We need to evaluate privacy concerns in their full social contexts. These are not problems that can be resolved on an individual level, because of the interpersonal nature of much of this data and the complexities of the tradeoffs involved.

**Technical countermeasures**

While they may not solve the problem, there are some technical steps people can take to limit the scope of these surveillance practices. For example, some web browsers do not send "third-party cookies" by default, or they scope cookies so that centralized surveillance doesn't get a single view of one user. The most privacy-preserving modern browser is the Tor Browser, which everyone should have installed and available, even if it's not the browser they choose to use every day. It limits the surveillance ability of systems that you have not signed up for to track you as you move around the web.

You can also modify some browsers — for example, with plug-ins for Firefox and Chrome — so that they do not send third-party requests at all. Firefox is also exploring even more privacy-preserving techniques.

It can't be denied, though, that these tools are harder to use than the web browsers most people are accustomed to, and they create barriers to some online activities. (For example, logging in to some sites and accessing some web applications is impossible without third-party cookies.)

Some website operators take their visitors' privacy more seriously than others, by reducing the amount of third-party requests. For example, it's possible to display "share on Facebook" or "Like" buttons without sending user requests to Facebook in the first place. The ACLU's own website does this because we believe that the right to read with privacy is a fundamental protection for civic discourse.

If you are responsible for running a website, try browsing it with a third-party-blocking extension turned on. Think about how much information you're requiring your users to send to third parties as a condition for using your site. If you care about being a good steward of your visitors' data, you can re-design your website to reduce this kind of leakage.
Opting out?

Some advertisers claim that you can "opt out" of their targeted advertising, and even offer a centralized place meant to help you do so. However, my experience with these tools isn't a positive one. They don't appear to work all of the time. (In a recent experiment I conducted, two advertisers' opt-out mechanisms failed to take effect.) And while advertisers claim to allow the user to opt out of "interest-based ads," it's not clear that the opt-outs govern data collection itself, rather than just the use of the collected data for displaying ads. Moreover, opting out on their terms requires the use of third-party cookies, thereby enabling another mechanism that other advertisers can then exploit.

It's also not clear how they function over time: How frequently do I need to take these steps? Do they expire? How often should I check back to make sure I'm still opted out? I'd much prefer an approach requiring me to opt in to surveillance and targeting.

Fix the surveillance economy, not just Facebook

These are just a few of the mechanisms that enable online tracking. Facebook is just one culprit in this online "surveillance economy," albeit a massive one — the company owns Instagram, Atlas, WhatsApp, and dozens of other internet and technology companies and services. But it's not the only player in this space. Google's business model also relies on this kind of surveillance, and there are dozens of smaller players as well.

As we work to address the fallout from the current storm around Facebook and Cambridge Analytica, we can't afford to lose sight of these larger mechanisms at play. Cambridge Analytica's failures and mistakes are inherent to Facebook's business model. We need to seriously challenge the social structures that encourage people to opt in to this kind of surveillance. At the same time, we also need to protect those of us who manage to opt out.
Day 3: Biometrics and Algorithms
Stop! Right now, think of how many passwords and personal identification number (PIN) codes you have to remember. How often do you forget them? It is very inconvenient to remember those codes. Now do you have your fingers, eyes, voice, and face with you? The answer hopefully is yes! Have you ever forgotten any of those body parts? Not very likely! What if you could use those body parts instead of passwords and PIN codes to verify who you are? Would that not be more convenient? It also seems logical that it could be a more secure way of authenticating a person.

PAUL REID, BIOMETRICS FOR NETWORK SECURITY

Biometrics are celebrated as perfect identification technologies. They will secure your laptop, identify terrorist threats, and reduce crime by stabilizing the mercurial identities of criminalized individuals. As in the epigraph that begins this chapter, biometric scientists imagine these technologies as more highly evolved, efficient, and accurate versions of older techniques of identification. Why have to remember a password or PIN code when your body can easily replace it—a body that can now be digitalized? Isn’t it logical that digital technologies function better than their analog counterparts? Much is made of the potential benefits biometric technologies can bring to the knowledgeable consumer in this textbook, published in 2004:

With the cost of biometric technology falling, it will soon be reliable and cheap enough for everyday use. For example:

- Enter your favorite coffee shop in the morning, and your coffee order is waiting for you at the counter.
- Your daughter's boyfriend, whom you do not like, comes to the house and the door won't open to let him in.
- Your own little personal identification device recognizes someone you have not seen in years and provides you with his/her name. This could result in no more embarrassing blank looks on your face. (P. Reid 2004:231)

In these examples biometric technologies are able to supply simple solutions to domestic problems, from patriarchal protection to the limits of long-term memory. Not restricted to the high-stakes tasks of securing the border or ending crime, biometrics are able to additionally (and seamlessly) break down the quotidian into moments for market, as scientists imagine these technologies to work perfectly, identifying and verifying individual bodies without error while providing a new range of consumer services. And yet biometric technologies do not work in the straightforward manner such discourse would have us believe, whether industry representations, government accounts, or laws and policies mandating their deployment. Although biometrics are explicitly sold to us as able to circumvent problematic human assumptions about race, gender, class, and sexuality; in fact, this book demonstrates that it is upon rigid and essentialized understandings of race and gender that these technologies rely.

In this chapter I analyze the science constructing biometric technologies and show how they rely upon outdated and erroneous assumptions about the biological nature of identity. In investigating the scientific principles upon which biometrics are based, I ask whether these new identification technologies perpetuate existing forms of inequality. I start with the way the biometric industry describes how the technologies work, then examine the assertions about the alleged potential of these technologies. In contextualizing these claims I demonstrate that biometric technologies are the latest in a long line of identification technologies claimed to be impartial and objective. Considering the ways that culture is always encoded into technology, I revisit the central question of this book: What happens when biometrics fail? I show that although biometrics were marketed on the basis of their ability to avoid human pitfalls, these very same human assumptions about the biological nature of identity are encoded right into these new identification technologies.
Defining Biometrics

Biometrics is the science of using biological information for the purposes of identification or verification.\(^\text{1}\) Although the term biometrics dates back to the early twentieth century and was used to refer to mathematical and statistical methods applied to data analysis in the biological sciences, the focus of this book is on digital biometrics. A biometric attribute is defined as a “physical or psychological trait that can be measured, recorded, and quantified” (P. Reid 2004:5). The process of acquiring the information about the physical or behavioral trait—whether a digital fingerprint, iris scan, or distinctive gait—and then storing that information digitally in a biometric system is called enrollment (P. Reid 2004:6; Nanavati, Thieme, and Nanavati 2002:17). A template is the digital description of a physical or psychological trait, usually containing a string of alphanumeric characters that expresses the attributes of the trait (P. Reid 2004:6). Before the biometric data are converted to a digital form, they are referred to as raw data (Nanavati, Thieme, and Nanavati 2002:17). Raw biometric data are not used to perform matches—they must first be translated into a biometric template before they can be utilized—a process that is achieved with the help of a biometric algorithm. Biometric algorithms are frequently described as recipes for turning a person’s biological traits into a “digital representation in the form of a template” (P. Reid 2004:6). This recipe is usually proprietary, and it is what a biometric technology company sells, arguing that their recipe for creating a template from raw biometric data is better than another company’s recipe.

Vendors represent biometric technologies as able to answer two questions. The first question refers to identification and asks, Who am I? Often described as a 1:N matching process, the presentation of a biometric template created in real time (called a live biometric) is checked against a database of stored biometric templates. Used more commonly in security and law enforcement applications, this process allows for one person to be checked against a list of persons (P. Reid 2004:14). The second question that biometric technologies are imagined to be able to answer concerns verification: Am I who I say I am? Referred to as a 1:1 matching process, verification checks the presentation of the live biometric with the person’s template stored in the database to determine if they match. If the live biometric is the same as the stored biometric, there is a match and the
identity is verified. Verification is held up in biometric discourse to be a much quicker process than identification, since it must check only one live biometric against one stored biometric, rather than checking a particular biometric against an entire database. Biometric technologies that rely on verification are more commonly used in physical and informational access applications, including secure building and computer network access (14).

The industry claims that a central innovation provided by the technology is that biometric information can neither be stolen from nor forgotten by the individual, as it depends on the measurement of physical or behavioral traits. As biometric technologies measure bodies and bodily behavior (such as gait), the “provider of the trait always has them with him or her” (P. Reid 2004:3) and cannot substitute another’s information. Industry representatives thus claim that biometric technologies provide convenience, security, and accountability (Nanavati, Thieme, and Nanavati 2002:4–5).

The biometric industry does acknowledge that errors do occur and cites three errors as particularly common (P. Reid 2004; Nanavati, Thieme, and Nanavati 2002). One is the false acceptance rate, in which a person who is not you is accepted as you. The false rejection rate occurs when you are not accepted as you. This is usually given as a percentage of the chance of somebody else erroneously being identified as you. Another type of error is the failure to enroll, often given as a percentage of the possibility of someone failing to be enrolled in the system at all (P. Reid 2004:6). In Biometrics for Network Security Paul Reid asserts that current problems with biometric technologies “will be solved with time, money and technological advances” (121).

Biometric technologies are broken down into two categories: active biometrics and passive biometrics. Active biometric technologies depend on the user actively submitting information to a biometric scanner. For example, finger scanning relies on the person actively placing a finger on the plate in order to have the print captured. Passive biometric technologies allow for the covert collection of biometric data, as in the case of smart surveillance cameras able to secretly capture a person’s facial biometrics. Biometric technologies currently in use include fingerprint imaging, hand geometry, iris scanning, voice biometrics, and facial recognition technology. Other biometric technologies in development for commercial use include gait and vein recognition, signature and keystroke technolo-
gies, and the use of DNA for the purposes of identification or verification, and the industry has endorsed a number of futuristic technologies, from olfactory recognition to recognition based on thought patterns (brain mapping).

**Biometric Objectivity**

As conversations on whether the state is racially profiling particular communities shift to whether racial profiling is an important and necessary state practice (Bahdi 2003), biometric discourse admits that racial profiling is occurring, but suggests that it can be overcome using new technologies. For example, media and scientific reports regularly depict biometrics as able to circumvent discrimination. One industry representative, Frances Zelazny, director of corporate communications for Visionics (a leading U.S. manufacturer of biometric systems), asserts that the corporation’s newly patented iris-scanning technology “is neutral to race and color, as it is based on facial features recognized by the software” (Olsen 2002). Zelazny suggested that biometric technologies’ impartiality helps to protect the privacy of individual citizens: “That the system is blind to race is a privacy enhancing measure” (Olsen 2002).

Similarly Bill Todd, a Tampa police detective, praised the closed circuit television (CCTV) system installed in Ybor City, Florida, specifically because, in his view, it is unable to discriminate on the basis of racial, ethnic, or gendered identity. Ybor City’s biometric system uses facial recognition technology to identify suspects by using smart CCTV cameras installed in the city’s Latin Quarter. Todd asserted that one of the primary benefits of installing the thirty-five cameras was that, unlike the police force itself, smart CCTV cameras are “race and gender neutral” (Lewine 2001). The allegedly arbitrary choice of this particular test site for facial recognition technology is problematized by Kelly Gates (2004), who highlights the tensions associated with choosing this neighborhood to test out a new biometric profiling technology given its raced and classed identity.

Claims of biometric neutrality are codified in book-length technical briefs (Pugliese 2005; Murray 2009). In their guide to the development and use of biometrics for businesses, John Woodward, Nicholas Orlans, and Peter Higgins (2003) argue that biometric technologies are beneficial because of their lack of bias: “The technological impartiality of facial recognition offers a significant benefit for society. While humans are adept at recognizing facial features, we also have prejudices and pre-
conceptions.” Woodward and his collaborators offer contemporary con­
traversies concerning “racial profiling [as] a leading example.” Contrast­
ing human recognition with biometric recognition, they argue that facial recognition technology is incapable of profiling based on identity because “facial recognition systems do not focus on a person’s skin color, hair­style, or manner of dress, and they do not rely on racial stereotypes. On
the contrary, a typical system uses objectively measurable facial features, such as the distances and angles between geometric points on the face, to recognize a specific individual. With biometrics, human recognition can become relatively more 'human-free' therefore free from many human flaws” (254).

Biometrics companies sell their technologies on the strength of these claims. For example, AcSys, a Canadian company dedicated to developing biometric facial recognition technology, promotes their product as “com­pletely race independent—eliminating risk of racial profiling” (AcSys Bio­metrics Corp. 2007). Even if companies acknowledge that one type of biometrics, such as finger imaging, is not “race neutral,” they suggest that a different biometric technology is the solution to this problem. For exam­ple, Doug Carlisle is a board member at A4Vision, a biometric company dedicated to developing 3D facial-imaging technology. He asserts that the bias associated with biometric fingerprinting can be fixed by using facial recognition technology: “Fingerprint technology . . . is difficult to imple­ment due to physiological differences across varying ethnic groups as well as some cultural prejudices that resist fingerprinting. Using the shape of one's face and head is less invasive, more accurate and the most promis­ing going forward for identification purposes” (Sheahan 2004).

Assumptions concerning the ability of biometrics to work with me­chanical objectivity or within frameworks of “knowledge engineering” (Lynch and Rodgers n.d.), in which scanners eliminate subjective human judgment and discrimination, have made their way from media and sci­entific reporting into commonsense assertions about the neutrality of biometric technologies. Thus in an online discussion on the use of iris scanners at the U.S.-Canada border, one discussant claimed he would prefer “race-neutral” biometric technologies to racist customs border offi­cials: “If I was a member of one of the oft-profiled minorities, I'd sign up for sure. Upside—you can walk right past the bonehead looking for the bomb under your shirt just because of your tan and beard. . . . In short, I'd rather leave it up to a device that can distinguish my iris from a terrorist's,
than some bigoted lout who can't distinguish my skin, clothing or accent from same” (“Airport Starts Using Iris Screener” 2005). Here we see what Sherene Razack (2008) terms “race thinking,” that is, that the state can justify the surveillance and suspension of the rights of othered communities in the interests of national security. The belief is that new technologies will circumvent forms of “race thinking” and racial profiling by replacing the subjective human gaze with the objective gaze of the state.

Institutions investing in biometric technologies use these assumptions about the technical neutrality of these new identification technologies to justify their adoption. These claims are interesting in a number of ways, not least in that they reveal tacit assumptions around race and gender discrimination by those who might not ordinarily acknowledge prejudice in the systems of which they are a part. It is relatively rare to hear a police officer argue for new technologies because his own task force is prone to racist and sexist assumptions, as did Bill Todd of Ybor City (Lewine 2001). Institutional players adopting biometrics represent them as the answer to institutional forms of discrimination and inequality such as racial profiling. And yet biometrics have failed, calling into question industry and scientific assertions about the objectivity of these new identification technologies.

Biometrics Unraveling

At the unveiling of a new iris scanner at Edmonton International Airport, Deputy Prime Minister Anne McLellan moonlighted as public relations manager for the biometric industry. McLellan demonstrated the operation of a new scanner designed to showcase the accuracy and efficiency of these new identification technologies and to promote CANPASS, a program that replaces border personnel with biometric scanners. As we will see in greater detail in chapter 4, CANPASS is a Nexus-Air affiliate border-crossing program designed to speed “pre-approved, low-risk air travelers” across the border. Meant to showcase the efficiency of replacing subjective humans with objective machines, the demonstration did not go as planned: “McLellan stared into the scanning machine... but twice a computerized voice declared: ‘Iris scan unsuccessful'” (“Canada’s Edmonton Airport Implements Iris-Recognition Screener at Immigration” 2011).

As the Edmonton airport failure reveals, new technologies designed to ease identification do not always function in the straightforward way that industry discourse would have us believe. News of biometric failures
circulated shortly after their introduction, as test results indicating their poor efficacy quickly made their way into the media. Simultaneously indications of the ease with which they could be “spoofed” (fooled into malfunctioning) proliferated. Before turning to the science on which biometric technologies rely, it is useful to examine the cracks in the façade of biometric success. That is, it is helpful to look at reported biometric failures before investigating why these errors might occur.

**Surveys, Spoofs, and Hacks**

One of the earliest documented failures of a biometric identification system involves facial recognition technology used in Ybor City, Florida. Given the significant costs and possibilities for surveillance provided by the system, and given its use within a predominantly Latino neighborhood, the system attracted significant media attention from its inception. In 2003 the American Civil Liberties Union documented that, after its first year, the system worked so poorly that the police were unable to identify a single criminal using a biometric facial recognition system that included thirty-five cameras. Although the system was renewed for a second year, it proved so difficult, expensive, and time-consuming for the police to use, while yielding only mismatches and failing to recognize known subjects, that it was ultimately abandoned (Gates 2004).

Other reports of biometric failures soon followed. The *ACLU* (2003) obtained documentation concerning a pilot project testing facial recognition technology at Logan Airport in Boston in which the photographs of forty employee volunteers were scanned into a database. The employees then tried to pass through two security checkpoints equipped with biometric cameras. The volunteers could not be identified 96 times out of 249 over a period of three months, a 39 percent failure rate. Key to these failures were lighting distinctions between the original photograph and the image captured on the biometric cameras. A security expert, Bruce Schneier (2001), suggested that technological dependence on good lighting conditions might be problematic, given that it is unlikely that terrorists will stop to pose for well-lit photographs. More recently the Face Recognition Vendor Test (*FRVT*), conducted in 2006 and partially sponsored by the Department of Homeland Security and the *FBI*, concluded that the error rate for facial recognition technology has decreased since 2002, partly because the technology is better able to identify faces across different lighting environments. The ideal was set as a false rejection rate
and a false acceptance rate of 1/1000. In 2002 one out of five people was not accurately identified; by 2006 one out of a hundred was not accurately identified. However, an error rate of 1/100 is still very high. Given that the International Civil Aviation Organization standard requires that all passports eventually contain facial biometric information, and given the volume of traffic that passes through airport security, this represents a significant number of people who will encounter difficulty (P. J. Phillips et al. 2007:5). At Logan International Airport, which handles 27 million passengers a year, 739 people would not be correctly biometrically identified on an average day.

Even those biometric technologies that did not fail were only as strong as the privacy measures in place to protect individual biometric information. There have already been a significant number of security breaches. At a convention intended to showcase new biometric technologies, the fingerprint and retinal information of thirty-six people trying out vendor products accidentally was sent by email to everyone attending the conference (Williams 2008).

The number of reports about the ease with which high-tech biometric technologies are hacked also calls their security into question. Researchers at Yokohama National University found that biometric fingerprint readers are easy to deceive using artificial gelatin fingers onto which a real print was dusted (Matsumoto, Matsumoto, Yamada, and Hoshino 2002). In Germany the magazine c't published extensive results on ways to successfully spoof biometric technologies (Thalheim, Krissler, and Ziegler 2002). Their methods included using high-quality digital printouts of irises to deceive iris scanners, using a little water on a biometric fingerprint scanner in order to reactivate the previous person’s latent image, and moving one’s head slightly from side to side to outwit facial recognition technology scanners. Marie Sandström (2004), a scientist, reproduced c't’s success in deceiving biometric fingerprinting; she tested nine different biometric fingerprint recognition systems and found that each was fooled by an artificial gelatin imprint.

As I noted in the introduction, one kind of biometric fraud causes particular anxiety. The possibility that a biometric scanner can be deceived by a severed body part garnered a good deal of attention, as was apparent by the multiple references to this possibility in mainstream news reports and media representations (Geoghegan 2005; Richtel 1999; Carney 2007; Mullins 2007). Moreover ongoing scientific research on the best
method to prevent a biometric scanner from recognizing the body part of a corpse (Abhyankar and Schuckers 2006; Parthasaradhi et al. 2005; Antonelli et al. 2006) gives credence to contemporary anxieties about the ramifications of biometrics for bodily security.

High-Tech Racism

Biometric technological failures do not occur equally across the board. The growth of biometrics occurred in a climate of increased anxieties about the “inscrutability” of racialized bodies. Given this cultural context, it is unsurprising that reports that biometric technologies did not function in the objective ways claimed for them began to proliferate. For example, a business brief about the possibilities of using biometrics for secure transactions reported that some “Asian women . . . had skin so fine it couldn’t reliably be used to record or verify a fingerprint” (Sturgeon 2005). Advocates of multimodal biometrics, in which more than one technology is used, took as their starting point that biometrics had difficulty recording the image of the bodies of people of color. Multimodal biometrics claimed to be able to enroll more othered bodies than could a unimodal technology: “At first glance, a Multi Modal biometric system offers certain advantages for your business, when contrasted to a Uni Modal security system: A Multi Modal system can capture the unique, biometric characteristics of a much larger and more varied target population. For example, it has been known that certain ethnic races have more difficulty in enrolling and verifying than other ethnic races. A Multi Modal system can help alleviate this problem over time” (Das 2007). Similarly the U.S. Transportation Security Administration (tsa) claimed they used a biometric iris system instead of one dependent on biometric fingerprinting because an iris scanner “allow[s] broader participation,” whereas “gender, ethnicity and age affect the qualities of fingerprints” (Fletcher 2006:20).

Despite tsa’s claim about the objectivity of iris scanning, reports circulated about iris scanners that functioned differentially on racialized bodies. Media reporting on biometric trials in the U.K. claimed that iris scanners disproportionately were unable to read the irises of people of color (Saeb 2005). Other news reports suggested that racism was being technologized in the form of the biometric iris scanner. It seemed that the darker a person’s skin, the greater the technological failure: “Answering a question on whether it regarded the rates as satisfactory, the Home Office replied: ‘It is true to say that at times in the past some difficulties have
been experienced in successfully recording the iris images of people with very dark skin (on some iris systems). The difficulty lay in the ability of the system to successfully locate irises against a darker skin tone" (Kablenet 2006). This response fails to explain why skin color would make a difference, as the irises of all people are surrounded by the white of the eye.

Such examples point to the problematic failures of biometric technologies. Activists fighting the implementation of biometric ID cards raised alarms about biometric plans, saying, "Little did we know that the government's own computers would actually be favoring blue eyes" (Saeb 2005). The ways that biometric technologies best imaged bodies racialized as white is reminiscent of Richard Dyer's (1997) work on how film was developed in order to be able to visualize whiteness. Evidence suggests that both government and industry representatives promoting biometrics were well aware of the differential success of biometric identification technologies in the accurate recognition of racialized persons, as news reports of biometric trials in the U.K. revealed that the technologies were tested on different racial and ethnic communities. These tests suggested that the government expected that different groups would yield different results: “Volunteers [will] be recruited from different ethnic groups to help . . . analyze the results [and] to examine any differences in results by demographics” (Kablenet 2006). Testing biometric technologies on different communities in this fashion poses an interesting contradiction. It undermines earlier industry assertions that biometric technologies are race-neutral while simultaneously recognizing the material effects of racial categories.

The technological fallibility of biometrics did not end with racialized bodies. News reports that biometric technologies consistently could not identify those deviating from the “norm” of the young, able-bodied male suggested that, in general, “one size fits all” biometric technologies failed to work. Here we see the perils of what Haraway (1997:142) terms “corporeal fetishism,” as biometric science is imagined to be able to condense complex relationships and situated knowledges into a single digital map of the body, one free from the “failures” of culture and understood to be outside troping or representational strategies. In the process of corporeal fetishism, particular bodies are rendered legible to new technologies and then packaged into a commodified form able to be circulated in the transnational networks of global capital as part of what Simone Browne (2009) calls the “identity-industrial complex.” Here we have the failure of bio-
metric science to recognize bodily complexity. These types of biometric failures result in part from what Haraway (1997:137) would call the error of mistaking complex and "worldly bodies-in-the-making" for fixed and reified things. A news article posted on Black Information Link, a community website by and for people of color living in the U.K., suggested that biometric facial recognition technology worked very poorly with elderly persons and failed more than half the time in identifying those in the study who have disabilities (Saeb 2005). Other news articles suggested that biometric iris scanners were particularly bad at identifying those with visual impairments and those who are wheelchair users, due to difficulties in getting the angle between the eye and the iris scanner within the parameters required for the scanner to work or because people could not see the red light in the scanner itself directing them where to look (Gomm 2005). Class also was a factor, as hard physical labor erases fingerprints. The U.K. Biometrics Working Group (2002) found that accurately fingerprinting those with "clerical, manual, [and] maintenance" occupations was more difficult than fingerprinting those in other occupations. Biometric iris scanners additionally failed disproportionately with very tall persons (Gomm 2005), and biometric fingerprint scanners couldn't identify 20 percent of those with nonnormative fingers: "One out of five people failed the fingerprint test because the scanner was 'too small to scan a sufficient area of fingerprint from participants with large fingers'" (Saeb 2005). In short, any kind of bodily deviance could give rise to biometric failure, begging the question as to exactly what type of body would not yield errors. "Worn down or sticky fingertips for fingerprints, medicine intake in iris identification (atropine), hoarseness in voice recognition, [and] a broken arm for signature" all gave rise to temporary biometric failures; "well-known permanent failures are, for example, cataracts, which makes retina identification impossible or rare skin diseases, which permanently destroy a fingerprint" (Bioidentification 2007). In a blatant acknowledgment that their biometric scanners failed to work for people with a number of disabilities, the Clear program in the U.S., which uses biometric iris and fingerprint information to speed travelers through security, posted the following warning:

Our verification kiosk currently includes a scanning device that requires that you walk into and stand on the kiosk. Therefore, the kiosk may not be able to serve all our members.
If you have any of the following conditions, please inform the Clear [program] attendants BEFORE entering the kiosk: artificial limbs, bone or joint replacements, metal implants, plates, rods, pins or screws, shrapnel, surgical staples or wires, pacemaker or other life-sustaining medical device(s).

Clear is committed to working with TSA and our technology partners to develop and deploy a registered traveler solution that serves the broadest possible population. (Clear Program Guidelines 2007)

Despite its token attempt to suggest that it works with a broad population, Clear is one among many examples of biometric programs that are unable to serve customers with disabilities. The Clear program helps to reveal which bodies can be rendered as commodities and which cannot, suggesting that disabled bodies cannot be rendered as financially profitable objects. This is also true of the biometric iris scanners used to speed travelers across the U.S.-Canada border: you must be able to stand and you must have relatively normative vision to use the Nexus-Air biometric scanners; thus wheelchair users and those with visual disabilities may not participate in this program. Here we are reminded of the ways that corporeal fetishism is used to transform bodies into objects—ascribing a value to every body—as some are deemed to have more economic value than others.

Assertions regarding the inability of biometrics to identify othered bodies also could be found in biometric textbooks (Murray 2007; Pugliese 2005). In their primer, Biometrics: Identity Verification in a Networked World, Nanavati, Thieme, and Nanavati (2002:60) explain one of the weaknesses of finger scans: “Certain ethnic and demographic groups have lower-quality fingerprints and are more difficult to enroll than others. IBG’s Comparative Biometric Testing has shown that elderly populations, manual laborers, and some Asian populations are more likely to be unable to enroll in some finger-scan systems.” They describe similar difficulties with iris-scanning technology for people with disabilities: “Users with poor eyesight and those incapable of lining up their eyes with the technology’s guidance components have difficulty using the technology” (85). Given the long list of reasons why a biometric scanner might fail, it seems that these technologies work best for blue-eyed males with good eyesight and no disabilities, neither too young nor too old, a Goldilocks subject who is “just right.” The group that can be reliably identified is a
relatively small percentage of the population, though perhaps a somewhat more significant proportion of business travelers and other users of voluntary biometric programs.

Although technological utopianism and biometric technologies as a panacea for social problems are a key part of the fabric of the discourse on these new surveillance technologies, we see that, rather than reciting a narrative of seamless technological functionality, the biometric failures I have detailed, including their disproportionate failure on othered bodies, suggest that these technologies do not operate with the mechanical objectivity claimed for them.

Scientific Representations of Biometrics

Everyone always wants the latest and coolest stuff, and this holds true for the computer industry. Many firms eagerly jump into the next big technology so they can say they were there first. This is referred to as being on the leading edge. In recent times, many have believed that biometrics were not on the leading edge, but on the bleeding edge. The bleeding edge is where a technology gets debunked. Biometrics have spent more time than any other technology in recent memory on the bleeding edge.

PAUL REID, BIOMETRICS FOR NETWORK SECURITY

Most vendor statements on accuracy bear little relevance to real-world performance of biometric systems.

SAMIR NANAVATI, MICHAEL THIEME, AND RAJ NANAVATI, BIOMETRICS: IDENTITY VERIFICATION IN A NETWORKED WORLD

The number of reported failures in biometric technologies demonstrates the fallibility of any technology that takes as its starting assumption the consistency of bodily identity. As we saw, the biometric industry regularly asserts that any difficulty with these technologies can be solved with sufficient research, money, and time. Although billions of dollars have been injected into state-funded biometric programs—from the prison system to the welfare system to border security—persistent failures remain. Like the polygraph, a technology whose perfection we continue to be assured is just around the corner (Littlefield 2005), it remains far from clear that biometrics will ever work reliably, no matter how long we leave them to gestate in the publicly subsidized private labs of biometric companies. It is necessary to investigate those instances when biometric technologies
fail and to ask what their failures tell us. The moments in which they fail are useful to identify the assumptions upon which they rely and the cultural context that they encode.

I turn now to an investigation of scientific studies on biometric technologies designed to improve their ability to classify individuals based on bodily identity. Biometric scientists rely upon the computerized recognition of gender and race to help with the development of significantly faster biometric identification—one of the vaunted goals of the industry. In general these studies argue that it is useful to reduce the size of the database against which a particular individual is matched, especially when performing a one-to-many (1:N) search, and they rely upon gender, racial, and other categories of identity to reduce the population size (the N) against which the individual is screened. If the person being identified is already classified as male and thus need only be checked against a database of other males, the argument is that this will cut computer processing time in half (Childers et al. 1988:603). As well, using so-called soft biometric traits like gender, race, and age in order to classify subjects is hypothesized to enhance the overall accuracy of biometric recognition (Buderi 2005; Jain, Dass, and Nandakumar 2004b). Soft biometrics “are nondistinctive, limitedly permanent human traits such as gender, age, hair color, weight and height” (Jain, Dass, and Nandakumar 2004a).

Much of the research on biometric recognition is based on a foundational article titled “SexNet: A Neural Network Identifies Sex from Human Faces” (Golomb, Lawrence, and Sejnowski 1991). A research team led by the biologist and medical doctor Beatrice Golomb combined developments in computing and informatics with rudimentary biology in order to develop a computerized network able to identify sex from frontal facial photographs. Giving their network the somewhat obvious name “SexNet,” the team concluded that their machine could classify human faces by sex more reliably than people could. They postulated that the computer network’s average error rate was 8.1 percent, in contrast to 11.6 percent for human error. However, SexNet’s overall error rates remained high. One in ten faces was incorrectly identified. The researchers found some faces especially problematic for both humans and computers. One male face was mis-sexed by both, suggesting perhaps that human difficulties in identifying biological sex from faces were being technologized. As stated by Golomb, Lawrence, and Sejnowski, “Similar errors seemed to affect the net and humans. One male face gave particular trouble to SexNet, being
mis-sexed when a test face, and taking long to train when a training face. This same face was (erroneously) judged ‘female,’ ‘sure’ by all 5 human observers” (575). In order to address this difficulty, the researchers suggested creating a “special category for the individual” and others like him (575). In this way one would avoid needlessly amending the male and female categories in order to be able to correctly classify what was referred to as one “fluke” face (575). This would additionally permit sex “outliers to be correctly identified without adverse consequences to generalization” (576). Thus individuals whose biological sex was not immediately apparent to either people or computers, a sample imagined by Golomb, Lawrence, and Sejnowski to be a tiny fraction of the human population, would not interrupt SexNet’s ability to classify the vast majority of faces.

In the event that readers of the study should think that these sex “outliers” indicated that SexNet functioned poorly, Golomb, Lawrence, and Sejnowski cited the following example of the network’s superior ability to identify sex as proof that their system worked. During the labeling of the sex of each photograph, one female face was accidentally assigned a male value. This human error was detected by SexNet, as described in the results section of their paper: “SexNet proved right: The face was a clear female whose sex value had been mistranscribed” (1991:575). This example was given as evidence that the network “had evidently done a fine job of abstracting what distinguishes the sexes” (575) and was able to eliminate problematic human intervention in the pure practice of classification. A number of future applications for SexNet were outlined in the study’s conclusion, including the suggestion that this network could help to indicate whether sex could be extrapolated from the face of other mammals in addition to humans, for example, an experiment investigating whether the faces of rhesus monkeys differed by sex. Golomb and her collaborators suggested that a second, more “frivolous” application for systems like SexNet would be to “scientifically test the tenets of anthroposcopy (physiognomy), according to which personality traits can be divined from features of the face and head” (576). In this way the development of biometric systems of classification attempted to reopen discussions about the scientific worth of formerly discredited branches of scientific inquiry such as physiognomy. This type of biometric research also marks the return to contemporary biological understandings of gender and race, a debate that is once again on the rise.

Though these technologies may fail to work in the ways claimed for
them, the case studies in this book show how biometric technologies work to exclude particular communities, including prison inmates, welfare recipients, and immigrants and refugees. Applications for this type of biometric research are abundantly clear. No longer restricted to an underfunded future sorting rhesus monkeys, biometric technologies were rolled out as an essential part of the security-industrial complex.

Moving from the biological to the computational sciences, studies on ways to refine SexNet proliferated. In their study of how to classify facial images by gender, Jain and Huang (2004) suggested using two algorithms to extract geometric features and classify human faces. In “An Experimental Study on Automatic Face Gender Classification,” Yang, Li, and Haizhou (2006) attempted to use a “normalization” process to classify frontal facial images by gender. Running photos of faces through a number of statistical procedures before generating their digital template, they compared three algorithms in order to see which better classified their database of normalized faces. The database consisted of “11,500 Chinese snapshot images, including 7000 male and 4500 female . . . whose faces are always upright and neutral without beard[s] or strange hair style[s]” (3).

In this study, Yang, Li, and Haizhou concluded that subjecting the photos to statistical normalization helped the computer to learn to classify the faces correctly. It appears from figures 2.1 and 2.2 that smiling is a telling indicator of femaleness, in keeping with other studies that conclude that showing emotion in the face is a key indicator of female identity. Also, the face with long hair is identified as female, whereas the face with short hair is identified as male. One of the normalization procedures Yang, Li, and Haizhou followed was to run all of the photos through a statistical method of triangulation warping, in which the shape of the individual face is discarded in favor of a mean face shape. What Golomb, Lawrence, and Sejnowski (1991) called “sex outliers” were shed in the move from biology to computer science. In keeping with homophobic ideologies that assert that God made Adam and Eve, not Adam and Steve, these later studies (Jain and Huang 2004; Ueki et al. 2004; Givens et al. 2004; Yang, Li, and Haizhou 2006) rejected Golomb’s “sex outlier” category altogether. Rather than outliers, these studies concluded that faces that could not be recognized by the machine were evidence that the technology needed further fine-tuning.

Some sex classification systems attempted to use biometric indicators other than the face in order to categorize their subjects. One early study
used voice biometrics to classify individuals by sex. Childers et al. (1988) claimed to be able to identify the sex of their subject based on the number of voiced fricatives, a sound produced by pushing air through a restriction in the vocal tract, such as occurs when producing the sounds “f” and “s.” They concluded that women uttered fricatives more commonly and in this way could be differentiated from men (603). Other studies used skin color biometrics in order to improve recognition. In these cases the color of the skin of one individual was superimposed on a different photograph of the same individual, with the idea that this would make the individual more identifiable over time (Yin, Jia, and Morrissey 2004; Li, Goshtasby, and Garcia 2000). In their study on biometric classification by gender, Ueki et al. (2004) attempted to demonstrate the importance of sartorial markers to consistent bodily identity. They tried to show the importance of “neckties and décolletés (clothes with [a] low-cut neckline)” to “differentiate gender” (see figs. 3 and 4).

In addition to clothing cues, Ueki et al. attempted to integrate the subject’s hairstyle into the process of biometric classification, asserting
FIGURE 3 The biometric template of the necktie is created from the raw biometric data (Ueki et al. 2004). The Laplacian is a scalar operator that can transform an image into an image more easily analyzed.

FIGURE 4 The biometric template of the neckline is created from the raw biometric data (Ueki et al. 2004). The skin image is meant to demonstrate whether the neckline is revealing (female) or discreet (male).

that "hairstyle is considered to be one of the effective features in gender classification" (fig. 5). Postulating that long hair helps to demonstrate that the unknown subject is a woman, whereas short hair indicates masculinity, Ueki et al. concluded that neckties, hairstyles, and whether or not the individual is wearing a revealing top all improve the system's ability to classify individuals by gender. As a quick glance could accomplish the same task for a lot less money than would be required to refine and
implement this biometric system, we need to keep in mind the profit motives driving the development of these technologies.

The methods used for gender classification were next adapted to attempts to use biometrics to categorize subjects by race. One example is found in "A Real Time Race Classification System" (Ou et al. 2005). The researchers set out to design a cataloguing system that reliably could use biometric facial recognition technology to divide the scanned faces into two categories, Asian and non-Asian. First, they proposed to turn the raw biometric data extracted from the face into a digital template using an algorithmic process they called principal component analysis (PCA). Using this method they located each face’s eigenvectors, defined as “mathematical properties that describe the unique geometry of a particular face” (P. Reid 2004:99). Ou et al. (2005: 379) then used a supervised form of PCA to isolate the eigenvectors that contained key information about race. Using a technique called independent component analysis (ICA) they extracted the features most useful to classifying each face. They argued that this method would help to isolate the facial features with the best “race information” (380). Once they had refined their PCA and ICA processes to select and extract the features that contain the key information about the test subject’s race, they then classified their facial images into two categories: Asian and non-Asian. Using a statistical technique called Support Vector Machines, they flattened each face to reduce the three-dimensional model to a two-dimensional model (380). Ou et al. then input a large database of faces into their computer and manually labeled the race of
each face. Having "taught" the computer which faces represented which race, Ou et al. tested the computer on a new series of faces. They found their total error rate to be 17.5 percent.

The method followed in their paper is standard. Their major contribution is the PCA and ICA methods they used to generate the digital template of the face. The authors also proposed a new algorithm to improve their chances of selecting features that contain good race information and to reduce the chance that they will choose features that contain bad race information (Ou et al. 2005:381). Other than the digital template contributions, the authors follow a well-defined path to the binary classification of bodies into racial categories.

Other biometric studies attempted to analyze the impact that a particular race's "feature characteristics" might have on the ability of these individuals to be recognized by a given biometric technology. In a paper titled "Rapid Pose Estimation of Mongolian Faces Using Projective Geometry," Hua-Ming, Zhou, and Geng (2004) used anthropometry as the foundation of their study. Anthropometry arose out of physical anthropology and is the technique of reading human characteristics (including intelligence) off the body. It is a largely discredited branch of science, famously debunked by the Harvard biologist Stephen Jay Gould (1996). In 1996 the American Association of Physical Anthropologists issued a statement denying any biological theory of race. Yet, as we see in the paper by Hua-Ming, Zhou, and Geng, anthropometry as a field of study is being revived by biometric scientists, including Golomb, Lawrence, and Sejnowski (1991) in their suggestions of possible future applications for their sex classification system. The resurgence of interest in reified understandings of race and gender reflects the debates that continue to rage over whether race is biological, despite the wealth of scientific evidence to the contrary.

Hua-Ming, Zhou, and Geng (2004) begin their study of "Mongolian" faces by asserting, "The difference of Race is obvious, and it is the central field of the research of anthropology. Anthropometry is a key technique to find out this difference." They declare, "[As] the Mongolian race is regarded as the main race of China, the statistical information of its feature[s] has very important scientific meaning to our research in the field such as facial pose estimate and face recognition." These scientists predictably define the Mongolian race's distinctive features as the "width of the eye feature" and the "length of the nose," characteristics that they
argue are uncontaminated by facial expression, which may make facial recognition more difficult (fig. 6). In developing this model, the authors concluded that they would be able to improve computer facial recognition by accounting for what they term "the Mongolian race's feature characteristic." That is, in refining biometric technologies to identify Mongolian faces, Hua-ming, Zhou, and Geng would help facial recognition technology work well in China.

Many of the studies attempting the biometric classification of bodies aim to categorize individuals by both gender and race. For example, in their study Givens et al. (2004) conducted a comparison test of the efficacy of three algorithms at identifying faces based on their features. They included gender and race as facial features, alongside "glasses use, facial hair, bangs, mouth state, skin complexion, state of eyes, makeup use, and facial expression." In indicating how to classify each individual, Givens et al. give the following explanation of their categories:

Race [White*, African American, Asian, Other.] The "Other" category was used for Arab, Indian, Hispanic, mixed race, and any subject that did not fit into the other three categories.

Gender [Male*, Female.] Self-explanatory

The asterisk indicates the factor that was designated as the baseline; that is, it was assumed as the default category. While the scientists conducting
this study do acknowledge that it is possible for the rating of each facial feature to have a subjective component, they stress that it is not statistically significant. They conclude, “Gender, skin, glasses and bangs were easy for our viewer to judge, [while] race, facial hair, expression, mouth and eyes were somewhat harder, although the viewer was still confident in his judgments.” When the judge could not decide, the default values of white and male were selected automatically.

Givens et al. ultimately found that, regardless of the algorithm used, “old [elderly] subjects and non-Caucasian subjects are easier to recognize.” For one of the algorithms, women are harder to identify, whereas for the other two there is no significant difference. Although the authors asserted that most of the work on gender classification finds that men are easier to recognize they cite no sources. Givens et al. attributed the improvement of their study on other attempts at biometrically recognizing women to the fact that they also controlled for factors such as facial hair and makeup.

Givens et al.’s classification of faces based on features is just one study among many that attempt to group subjects according to both their gender and race identities. Invariably these categorization processes are done sequentially rather than simultaneously. For example, in their study “Gender and Ethnic Classification of Face Images” Gutta, Wechsler, and Phillips (1998:194) developed two classification tasks, one for gender and one for race. This type of sequential ordering is repeated in “Mixture of Experts for Classification of Gender, Ethnic Origin and Pose of Human Faces” (Gutta et al. 2000) and “Classifying Facial Attributes Using a 2-D Gabor Wavelet Representation and Discriminant Analysis” (Lyons et al. 2000). In all of these studies “hybrid” subjects (for example, women of color) would need to be classified first by gender and then by race, though no instructions for how to classify these subjects are provided. This is especially ironic given that the new racial categories used in the U.S. census of 2000 showed increasing numbers of “hybrid” individuals selecting two or more racial categories. One might ask about the difficulties that individuals like President Barack Obama would face under this biometric regime.

These experiments represent only a few of the many biometric studies that classify individuals based on bodily identity, each using slightly different methods or a different data set. The initial labeling of the images by gender or race in order to train the computer system must be done man-
ually by the scientists themselves. The following statement is standard, demonstrating that so-called physiognomic differences are key: “The ground truth label for gender and ethnic origin were determined by visual inspection after the images were collected” (Gutta et al. 2000:198). That is, scientists themselves decide on the gender and race of an individual before using algorithms to train their computer to do the same. While the biometric classification method in these studies remained constant, the categories themselves varied. Individuals may be labeled Asian or non-Asian (Ou et al. 2005), Mongolian or non-Mongolian (Hua-Ming, Zhou, and Geng 2004), East Asian or non-East Asian (Lyons et al. 2000), Japanese or non-Japanese (Tanaka et al. 2004), Caucasian, Asian, Oriental, African, South Asian, or East Asian (Gutta, Wechsler, and Phillips 1998; Gutta et al. 2000). The ways that biometric technologies identify racialized and gendered bodies differently is known to scientists. From comparisons of the impact of biometric scanners that could identify some “races” better than others (Tanaka et al. 2004) to attempts to teach biometric systems to classify gender (Ueki et al. 2004), these studies help to explain biometric failures and their connection to race and gender identities. The papers just reviewed rely on racist research that is long debunked, while ignoring the host of empirical work in the past century on the complexity of bodily identity.

Significance: Historical Work on the Human Body

The scientific papers I have discussed rely predominantly on the fields of computer processing and recognition and largely ignore the rich field of empirical research that arose from studying human expression, emotion, and movement. Studies on the complex nature of the human face date back to 1806, with the publication of “Essay on the Anatomy of Expression in Painting” (C. Bell). More recent research includes the work of Ray Birdwhistell, one of the founding fathers of kinesiology, who spent much of his career attempting to develop a classification system for nonverbal communication. Other work in this area includes the research of Paul Ekman, whose book *Emotion in the Human Face* (Ekman, Friesen, and Ellsworth 1972) provides a detailed examination of the relationships between emotion, gender, age, and facial expression, and upon whom the tv show *Lie to Me* claims to be based. In the introduction to his book Ekman demonstrates the complex nature of human facial expression with his assertion that “man’s facial muscles are sufficiently complex to allow
more than a thousand different facial appearances; and the action of these muscles is so rapid, that these could all be shown in less than a few hours' time" (1). The rich literature on acting also gives detailed descriptions of the complexity of the human body and how to portray a great variety of human expressions, calling into question any notion of an essential or immutable bodily identity. Given this literature on the complexity of the human body, it seems strange that biometric scientists rely upon long-discredited assumptions about the biological nature of identity while refusing to engage with a field of research that dates back more than a hundred years. Certainly the omission of even a cursory review of this vast field of research seems egregious. Biometric discourse clearly functions as a form of corporeal fetishism in which complex human bodies are represented by ones and zeroes without discussion of the bodily processes that these strands of binary code hide from view or the implications of this particular representational strategy.

Biological Understandings of Race and Gender

The studies I analyzed earlier reveal some of the reasons that biometric technologies regularly fail, and why race and gender identities are so often connected to these failures. We saw that many biometric technologies are founded upon erroneous understandings of race and gender as reified phenotypes. In this way biometrics remind us of earlier technologies that attempted to read deviance off the body, including craniology, phrenology, and anthropometry. Biological categories of race have long been debunked by scientists (Tishkoff and Kidd 2004; Wells 2002; Kaufman 2008), social scientists (Sternberg 2007; Fish 2000; Duster 2005; American Association of Physical Anthropologists 1996), and cultural theorists (Gould 1996; Hammonds 2006). Similarly the biological nature of gender is problematized by a wide range of fields, from biology to philosophy to women's studies (Kessler 1990; Haraway 1997; Fausto-Sterling 2000; Butler 1990). Many of the biometric papers I cited refer to much earlier work that attempted and failed to definitively measure race and gender.

Consider the following quotation from an atlas of electroencephalography (the neurophysiologic measurement of the electrical activity of the brain, or the measurement of brain waves), written in 1941: "It is possible to tell an Eskimo from an Indian by the mathematical relationship between certain body measurements at a glance. . . . It would be wrong, however, to disparage the use of indices and objective measurements;
they are useful and should be employed wherever possible" (Gibbs and Gibbs 1941:n.p.). The study of racial classification and the use of biometrics by Ou et al. (2004:379) is more than slightly evocative of that earlier study: "We consider that every [facial] feature encodes different information in a certain scale such as gender, race, identity, etc. . . . By analyzing the distribution of the project $2n$ points, we can roughly select the eigenvectors which have more race information." Similarly, the study by Gutta, Wechsler, and Phillips (1998:195) on the use of facial geometrics to classify subjects by race reminds us of the 1941 study. Although Gutta, Wechsler, and Phillips use computers, the narrative bears more than passing similarity to the earlier study:

Face processing first detects a pattern as a face and then will box the face. It proceeds to normalize the face image to account for geometrical and illumination changes using information about the box surrounding the face and/or eyes location, and finally it identifies the face using appropriate image representation and classification algorithms. The result reported later on assumes that the patterns corresponding to face images have been detected and normalized. The specific task considered herein is that of gender and ethnic classification, i.e., discrimination of human faces as belonging to either a female or male category and Caucasian, Asian, Oriental or to African categories respectively.

In contending that particular races have associated characteristics or in suggesting that some body parts contain more race information than others, long debunked biological theories of race again take on the authority of objective scientific assertions. This ignorance of basic contemporary concepts—for example, that race is not biological even if systemic racism means that race as a category has material significance—gives rise to a host of difficulties. One ramification is that mixed-race individuals, in addition to the overwhelming number of people who do not meet the rigid racial types defined by these experiments, are ignored altogether by biometric classification systems as they do not easily fit defined categories, including those mixed-race individuals who get classified within groups. As a result of biometric science, entire communities become what Leigh Star and Geoff Bowker have called "boundary objects," Donna Haraway has called "monsters," and Kal Alston has called "unicorns"—uncategorizable objects that do not fit into any classification system, objects at once "mythical and unknowable, straddling multiple worlds"
(Bowker and Star 1999:306). Although systemic forms of discrimination give race and gender material significance, this does not imply that race and gender are stable qualities that can be reliably read off the body.

Nor do mixed-race individuals present the only problem with premising biometrics on biological understandings of race, as racist ideologies are necessarily at the core of any assertion that race can be reliably measured or classified. This helps to explain why biometric studies consistently feature whiteness and maleness as normative. For example, in using white and male as the default categories for biometric selection (Givens et al. 2004), or in attempting to determine whether biometric scanners will be able to identify the “distinctive” faces of the “Mongolian race” (Hua-Ming, Zhou, and Geng 2004), researchers are suggesting that white faces may easily be recognized, whereas nonnormative racialized or female faces pose problems for biometric recognition. In his book White Richard Dyer (1997) shows that using technologies to privilege whiteness has a long history. Using biometric technologies to measure race, ethnicity, and gender, new technologies serve as disturbing reminders of older technologies underpinning racist policies. Moreover biometric scientists turn to essentialist understandings of race and gender at precisely the time that the debate on whether race is indeed biological again rises to prominence. In 2006 the Social Science Research Council launched a forum titled “Is Race Real?” in order to problematize the causal connections being drawn between race and genomics. Assertions about the biological nature of race are not the province of low-profile science or scientists. The Nobel prize–winning molecular biologist James Watson asserted in 2007 that injections of melanin would increase sex drive, and claimed that black people did not have the same capacity to reason as white people (Milmo 2007).

Biometric systems of categorization have the potential to exclude both those who don’t belong to the privileged category and those whose body is illegible. If you cannot obtain a passport unless your fingerprints can be collected—a proposal currently under consideration in Canada and the United States—then those without legible fingerprints cannot travel. Here we see the possibility for rendering othered bodies illegible to the biometric scanner in ways that may have serious implications for people’s freedom and mobility. Thus in addition to lengthier and more intrusive forms of surveillance, biometric technologies may also deprive certain communities of their human right to mobility.
In her groundbreaking book on AIDS, the feminist science studies theorist Paula Treichler (1999:162) notes that the majority of researchers doing cultural studies research on the AIDS epidemic “have at least a rudimentary theoretical grasp of virology and immunology. The same cannot be said of most scientists’ grasp of social and cultural theory.” This holds true for biometric scientists; their ignorance of even the most fundamental tenets of theories of race and racism is deeply problematic, and is made evident in their claims that biometrics might usefully help scientists to reexamine the credibility of physiognomy (Golomb, Lawrence, and Sejnowski 1991) or the suggestion that anthropometry is the basis of modern anthropology (Hua-ming, Zhou, and Geng 2004). This lack of familiarity with contemporary knowledge regarding the socially constructed nature of identity raises questions regarding the knowledge base upon which these scientific practices depend. Clearly the impact of locational differences on biometric functioning, such as Japanese scanners that have trouble recognizing non-Japanese faces, tells us that these technologies are not created in a laboratory environment free of cultural influence. As these scientists label the images according to their understandings of their own biological race and gender identities, preconceptions about gender and race are codified into the biometric scanners from the beginning. Thus assumptions that women are more likely to have long hair and men are more likely to wear ties or that the “Mongolian race” has a certain type of eyelid are reified and then programmed into what David Lyon (2003) calls a “technology of social sorting.” Biometric scientists base their studies on dangerous, racist understandings of identity from the 1930s and earlier and ignore the past thirty years of research that has definitively disproved any biological theory of race.

Racial Profiling

The terrorist has a different look, a different face. . . . If I see someone (who) comes in that’s got a diaper on his head and a fan belt wrapped around the diaper on his head, that guy needs to be pulled over.

CONGRESSMAN JOHN COOKSEY OF LOUISIANA, CITED IN REEM BAHDI, “NO EXIT: RACIAL PROFILING AND CANADA’S WAR AGAINST TERRORISM”

Biometric technologies have had an interesting role to play in concerns about racial profiling after 9/11. In his article analyzing the increase in racial profiling following Canada’s war on terrorism, the legal theorist
Reem Badhi (2003) notes that the racial profiling of Arabs and Muslims was promoted as being in the interest of national security. Certainly the epidemic of racist incidents targeting individuals who are imagined by various security, immigration, and other institutional personnel to bear the signifiers of Arab and Muslim identities have made it clear that racial profiling is an integral part of the national security strategy of both Canada and the United States, revealing the discursive shift from “Is racial profiling occurring?” to “Should it continue to be condemned?” One example of this is the roundtable facilitated by the editors of the New York Times in which they posed the question “Will profiling make a difference?” to a wide range of security experts, engineers, policymakers, and FBI agents (2010). One might ask if this question has already been answered given explicit decisions in the United States to racially profile its citizens. For example, the National Security Entry-Exit Registration System requires men (both visitors and immigrants) from a list of countries born on or before November 15, 1986, to undergo special registration procedures, including the collection of their biometric information. The countries on this list include Afghanistan, Algeria, Bahrain, Bangladesh, Egypt, Eritrea, Indonesia, Iran, Iraq, Jordan, Kuwait, Lebanon, Libya, Morocco, North Korea, Oman, Pakistan, Qatar, Saudi Arabia, Somalia, Sudan, Syria, Tunisia, the United Arab Emirates, and Yemen. Over forty local, national, and community organizations in the U.S., from human rights groups to faith-based coalitions and immigrant advocacy groups, called for an audit of this program in 2009 because it has increased the intimidation and harassment of Arab and Muslim communities.

It is no accident that biometrics play a significant role in racial profiling after 9/11. Held up by industry and government proponents as objective and free from the forms of systemic discrimination that plague real life, biometric technologies are represented as particularly useful because they will help to eliminate racial profiling. Biometric technologies, which claim to eliminate racial profiling through mechanical objectivity, simultaneously are explicitly based upon assumptions that categorize individuals into groups based on phenotypical markers of racialization and used in the implementation of programs specifically aimed at racial profiling. Moreover biometric technologies result in new forms of technologized racial profiling as people may not be allowed to travel as a result of how the scanners work. Clearly biometrics allow the state to both implicitly
and explicitly engage in racial profiling while using the rhetoric of technological neutrality and mechanical objectivity to obscure this fact.

**Queer Renderings of the Body**

In the studies described earlier old assumptions about the ways that sex may be read off the body, from hair length to clothing, are assertions about the absolute nature of the divide between men and women. Those bodies that do not fit the inflexible criteria defined for men and women regularly are discounted, as we saw in the Yang, Li, and Haizhou (2006) study, which deemed any face that had a “strange” hairstyle to be unclassifiable. These studies are reminiscent of earlier research attempts to read sexual variance and sexual deviance off the body, as in the case of the medical doctors who attempted to identify lesbianism by measuring vulva size and nipple length (Terry 1990). With respect to biometrics, we might imagine discounted bodies to regularly include those of butch women and femme men as well as transgendered persons, as the photos of those who failed to be correctly identified by Yang et al.’s system suggest. Although Golomb, Lawrence, and Sejnowski (1991) make a reference to “sex outliers” in their foundational study of computerized sex classification, this remains a deeply problematic category. In general people who cannot easily be categorized as either men or women are interpreted as biometric system failures. Showing a naive belief in the assumption that low-cut blouses and long hair can be used to distinguish women from men with beards and ties, the scientists conducting these studies rely on narrow definitions of sex and gender in which both are collapsed, and in which those who do not easily fit these categories are erased altogether. As Paula Treichler commented, these scientists appear to be immune to even the most basic tenets of fashion; even one season of *Project Runway* might make a world of difference to their attempts at classification.

Although biological understandings of race and gender have long been analyzed by cultural theorists and scientists, their findings have largely failed to make it into the labs of scientists designing biometric systems. Biometrically producing reified racialized and gendered identities can have severe material ramifications. Most at risk from having their race, sex, and gender identities biometrically codified are those who refuse neat categorizations as well as those whose bodies the state believes to be a threat.

What are the implications of biometric techniques of verification for
vulnerable bodies? What happens when biometrics fail? Given that the studies I've discussed assume neat bifurcations of gender into the mutually exclusive categories of male and female, the transsexual and transgendered community in particular faces significant risks from biometric forms of identification. For example, the U.S. Real ID Act of 2005 calls for the development of a national database of information and the creation of national identification cards equipped with chips that would carry both biometric data and information about biological sex. The Act poses grave risks for transgendered people living in the United States and was identified as one of the most pressing issues facing transgendered people today by Mara Keisling (2007), the executive director of the National Center for Transgender Equality. Any form of identification that contains biometric information could easily endanger trans folks if it was used to link them to a history of name changes or spotlight discrepancies in legal names and gender markers. In particular it could publicly identify people by making visible connections to outdated gender designations. In this way the representation of biometrics as able to stain identity onto the body—especially given the essentialized notions of gender upon which they are based—makes this community vulnerable to the prying eyes of the state. Mobilization also is occurring in the U.K. to address difficulties created by British plans for biometric IDs and for a national identification card. It remains unclear whether British ID cards will compare a person's biometric profile with his or her "birth gender" or "chosen gender" (Oates 2006).

Summary

Scientific studies that rely upon biological understandings of gender and race represent some of the most egregious failures of biometric technologies. Any technology that takes as its premise the assumption that bodies are stable entities that can be reliably quantified is problematic. Relying upon erroneous biological understandings of race and gender in the development of biometric technologies has a number of ramifications, from the marginalization of transgendered bodies to facilitating forms of mechanized racial profiling. Like other identification technologies before them, biometric technologies are deployed in ways that remind us of other racist regimes premised on similar strategies of racialized and gendered classification.

Using technology to tell us "truths" about the body never reveals the
stable narratives we are hoping for. Biometric technologies cannot be counted on effectively and definitively to identify any bodies. However, as these technologies are specifically deployed to identify suspect bodies, the impact of technological failure manifests itself most consistently in othered communities. Representing these new identification technologies as able to circumvent cultural assumptions and subjective human judgment does not make it so. Rather biometric technologies are always already inflected by the cultural context in which they were produced. Biometrics are marketed as able to eliminate systemic forms of discrimination at the same time as they are produced in a context marked by the persistence of problematic assumptions about difference. That is, the rhetoric of scientific neutrality masks their racist, sexist, homophobic, ableist, and classist practices. Given the context for which they were developed, it is unsurprising that biometric technologies are imagined as able definitively to identify suspect bodies. Nor is it surprising, given cultural assumptions about othered bodies, that these assumptions are both explicitly and implicitly coded into the technologies. Biometrics fail precisely at the task which they have been set: to read the body perfectly, and in doing so tattoo permanent identities onto deviant bodies. Thus biometrics fail most often and most spectacularly at the very objective they are marketed as able to accomplish. Race and gender identities are not nearly as invisible to new identification technologies as is claimed. The technological fallibility of biometrics manifests itself practically in their disproportionate failure at the intersection of racialized, queered, gendered, classed, and disabled bodies, as they represent the latest attempt to definitively tie identity to the body. Rather than telling stories of mechanical objectivity, race neutrality, and the guaranteed detection of formerly invisible bodies, biometric technologies continue to tell stories heavily inflected by the intersection of bodily identities.
Biometrics and policing are not strangers to each other.

ANN CAVOUKIAN, PRIVACY COMMISSIONER OF ONTARIO, BIOMETRICS AND POLICING:
COMMENTS FROM A PRIVACY PERSPECTIVE

The demonstration of the new iris scanner was identical to technical demos staged at biometric industry conferences aimed at proving how efficiently their products work. For Charles Coney, however, there was a significant difference: he could not refuse to be tested. Coney is a prisoner at Iowa's Story County Jail. He is one of those compelled to use this new technology, bankrolled by the government and rolled out across the United States.

As with any origin story, the history of biometric technologies does not have a tidy timeline. The biometric industry began as a series of fragmented endeavors loosely organized around a generalized interest in access control. Although biometrics made their debut in a number of different spaces, from banks to the workplace, the prison industrial complex is the first program to broadly adopt these new identification technologies.¹ Previous research helpfully grounds the growth of the biometric industry in the financial sector (Gates 2004; van der Ploeg 2005). In this chapter I build on this research and additionally track the beginnings of biometrics to the first major government-funded program to use biometric identification technologies. I am particularly interested in the rise of the prison industrial complex as a site of surveillance that disproportionately targets and criminalizes particular communities in ways that are tied to their gender, race, class, and sexual identities.
Biometric companies capitalized on rising rates of incarceration in order to create a profitable market for their products. Using narratives of corporeal fetishism to represent prisoners' bodies as strands of code capable of yielding their own product inventory numbers in ways imagined to facilitate the management of prison life, state projects use these new identification technologies to create new forms of knowledge about othered bodies. Use and exchange values are wrested from prisoners, whose criminalized bodies are treated as the raw material of capitalism, the fuel necessary to feed the ever-expanding prison economy. Biometric science organizes bodies—bodies imprisoned according to gender, race, disability, class, and sexual identities—in the service of capitalism. Moreover biometric technologies are key to what are broadly termed systems of "knowledge engineering" (Lynch and Rodgers n.d.), processes meant to replace human decision makers with computers. As a result the inclusion of biometric technologies in the prison industrial complex has significant implications for prisoners, including the removal of human witnesses to their suffering and the increased surveillance of prison life. I begin by describing the history of the invention and development of biometric technologies, the disparate companies working independently on these new identification technologies, and some of the early vocabulary developed to describe the science of identification. I then show that early industry focus was most successful for those companies interested in marketing their products to the prison system. I examine the growth of biometric technologies against the backdrop of the expansion of the prison industrial complex. Analyzing the ways that the intersection of poor people, people of color, and women were produced as the primary targets of biometric identification, I show that biometrics were used to police an increasingly broad range of criminalized individuals, from those warehoused in the U.S. penal system to newcomers to the country. I end this chapter by examining some of the implications of adding biometric technologies to the prison system, including the ramification of using prisoners as a test bed for new technologies as well as the consequences of codifying flawed science.

The History of Biometric Technologies

From bertillonage to portrait painting to ink fingerprinting, analog biometric technologies that measure the body for the purposes of identification have a long-standing history (C. M. Robertson 2004; Gates 2004;
Lalvani 1996; Gould 1996). However, my primary concern is the invention of digital biometric technologies, including the new possibilities that networking digital technologies provide for information sharing. As companies with no obvious customers floundered in their attempts to develop a product that could appeal to mass markets, a number of different technologies were researched and tested separately.

Although early biometric research focused primarily on digital fingerprinting, one of the first biometric technologies on the market was a hand geometry reader developed during the 1960s. The company Identimation initially sold biometric hand scanners to a Wall Street investment firm to be used as time clocks for the firm's employees (Sidlauskas and Tamer 2008). Hundreds of these technologies were sold in the late 1970s, and the Identimat remained available until 1987 (Sidlauskas and Tamer 2008). In 1979 Wackenhut bought Identimation. Wackenhut is the largest private security company in the United States and a key player in the privatization of prisons both in the United States and worldwide (Sidlauskas and Tamer 2008). Biometric retinal scanning began shortly after hand geometry, making its debut in the 1970s. In 1975 Robert "Buzz" Hill founded the company EyeDentify. Hill's technology was patented in 1978, and the first working prototype became available in 1981 (Hill 1999).

Early retinal scanners were expensive, costing up to $60,000; by 1988 EyeDentify's scanner sold for approximately $7,000 (M. Browne 1988). Although biometric retinal scanners were first used for access control in high-security buildings such as the Pentagon, once they had come down in price prisons bought them for the purposes of prisoner identification (Lichanska n.d.). Not to be confused with biometric retinal scanning, some of the earliest biometric research concentrated on iris scanning. Frank Burch, an ophthalmologist, proposed the idea of using iris patterns for personal ID in 1932 (National Center for State Courts 2002). However, the idea did not take off until the intervention of John Daugman, a scientist who created algorithms for iris recognition which he patented in 1994, the year that biometric iris scanners were first used in the prison system. Daugman's algorithms are the basis for all current iris recognition systems (National Science and Technology Council Subcommittee on Biometrics 2006).

Early biometric developments centered on generalized attempts at access control. That is, in attempting to pitch their products to a broad market, access control was one of the key ways of speaking about the
utility of biometric technologies. For example, early retinal scanners were used to control employees coming into work (Reuters 1986). Biometric prototypes also were used for access control in banks and other secured spaces, such as U.S. Navy facilities (Johnson 1984). Interestingly the term access control itself grew out of postwar telecommunications. It was listed in a glossary of telecommunications terms in 1949. Given that developments in security and computing technologies generated new language and, as a result, new markets in access control, prisons seemed a natural fit for an industry preoccupied with securing spaces. Obviously the prison is a site understood to require significant access control. In addition prisoners themselves represented “acres of skin” to a biometric industry in its infancy, and one requiring a broad population upon which to test its products. Fingerprinting remains the technology most closely associated with law enforcement and the prison system, and thus biometric fingerprinting was a primary focus of the early industry.

Biometric Fingerprinting and the Prison Industrial Complex

During the 1950s the FBI began using punch cards to store information about fingerprints; thus the origins of biometric fingerprinting date back to the early days of computing (S. A. Cole 2004). It is notable that the FBI’s search-and-retrieve fingerprint system relied upon information about identity from the outset: “By assigning a punch card encoded with information such as the individual’s gender, age, [and] race . . . to each fingerprint card, operators could then do a card sort searching for certain parameters, and operators could then retrieve the matching fingerprint cards” (17). Here we see that assumptions about the fixed nature of race and gender identities were central to the classification and surveillance of individuals involved in the prison industrial complex from the beginning.

In the 1960s the FBI sponsored research at the National Bureau of Standards on the potential of further automating fingerprint identification and searches. A major research paper on the possibility of this project was published in Nature by Mitchell Trauring in 1963. Trauring’s paper had a significant impact on the development of early biometric technologies, and is an important and heavily referenced part of biometric history. His article provided the basis for the continued development of biometric fingerprinting and is one of the first papers published in the field of automated biometric identification (Wayman 2004). The first patent awarded for biometric fingerprinting technology was issued to IBM, awk-
wardly titled “Personal Security System Having Personally Carried Card with Fingerprint Identification” (Wayman 2004). Attempts were made in the late 1960s to use holographic imaging for digital fingerprinting, but the technology proved too expensive (S. A. Cole 2004). New techniques facilitating the enhancement of images developed for NASA during the late 1960s and early 1970s significantly improved the process of digitizing fingerprinting (Cherry and Inwinkelried 2006). The first biometric fingerprinting system was tested in 1970 by what became the National Institute of Standards and Technology, then known as the U.S. National Bureau of Standards (Wegstein 1970). Automated fingerprint identification systems (AFIS) also were central to biometric fingerprinting development. This technique was debuted in 1972 by the FBI (S. A. Cole 2004). In the mid-1970s a number of biometric companies—including Fingerprintmatrix (1999) in the United States, which has been in business since 1976, NEC (Japan), and Morpho (France)—began marketing different versions of AFIS digital fingerprinting technologies to law enforcement agencies (S. A. Cole 2001:253–54). Both NEC and Morpho had made successful inroads into U.S. markets by 1985 (S. A. Cole 2001). Although the FBI began using automated search techniques for fingerprints in 1979, these did not become standard until 1983 (S. A. Cole 2004). The prison systems’ growing state-backed budgets provided an ideal location for biometric beginnings, as “procurement of an AFIS was ... in the range of $2 million to $10 million, and the conversion of the database—scanning fingerprint cards into digital form—could cost hundreds of thousands of dollars” (S. A. Cole 2001:253). In 1983 the FBI reported that it had digitized its entire fingerprint file, right back to 1928 (S. A. Cole 2001). By 1986 police bureaus had embraced digital AFIS, giving rise to “a frenzy of Request for Procurements” (253).

Given that AFIS shifted the standards for fingerprinting identification in addition to dramatically increasing search capabilities and the speed with which searches could be conducted, the fingerprinting historian Simon Cole notes that AFIS has justly been placed alongside DNA typing as “one of the two most important advances in forensic science in the 20th century” (2004:19). Biometric fingerprinting technologies made it “technically feasible to routinely check the fingerprints of everyone who comes into contact with the police,” profoundly shifting identification practices in the United States (S. A. Cole 2001:257). Thus biometric technologies are part of a larger scientific trend toward corporeal fetishism; that is,
these new technologies are used to codify bodies in ways that claim individual identities to be both knowable and searchable, without reference to the ways that biometric codifications of the body are themselves troping devices that draw on existing cultural assumptions that individuals can be broken down into their component parts and sold as commodities. In representing complex, relational bodily identities as discrete, reified things, biometric science eased the passage of individual identities to market in the prison industrial complex.

One of the significant expansions in biometric fingerprinting systems occurred in 1989, when Congress provided initial funding to what was then Immigration and Naturalization Services (INS) to develop an automated biometric fingerprint system for newcomers to the United States (U.S. Department of Justice 2001). The original goal of this program was to identify individuals who were repeatedly apprehended attempting to enter the United States without being inspected as well as those individuals who previously had been deported, were suspected of criminalized activity, or had outstanding warrants for their arrest (U.S. Department of Justice 2001). The expansion of biometric fingerprinting to newcomers to the U.S. fits in more broadly with an agenda aimed at the increasing criminalization of immigration, one that furthers xenophobic policies while generating corporate profits by expanding the prison industrial complex through building new immigration and refugee detention centers. Between 1991 and 1993 INS piloted its first AFIS system at the U.S. border with Mexico in the San Diego Border Patrol Center (U.S. Department of Justice 2004). Fearing delays for applicants to INS as well as coordination issues with the FBI, INS initially abandoned this pilot project and instead continued with its own IDENT system rather than the FBI's AFIS system (U.S. Department of Justice 2001). IDENT made its debut in 1994. Congress then mandated that the FBI's AFIS fingerprint system be integrated with the IDENT immigrant identification system before they would give the INS any additional funding to develop IDENT (U.S. Department of Justice 2000). In the coordination between INS and the FBI, biometric technologies were part of the increase in state systems of surveillance, rendering immigrant and refugee bodies suspect and extending technologies formerly limited to law enforcement to immigration in a move sometimes termed “crimmigration” (T. Barry 2010).

In addition to technological challenges for the INS and the FBI, standards between law enforcement agencies were incompatible. Although
few law enforcement agencies were without a repository of AFIS fingerprints by the 1990s, in 1992 a survey found that twenty-nine local law enforcement agencies used Printtrak in their storage of fingerprints, twenty-six used the NEC system, and seven used the Morpho system. FBI prints were stored in another manner altogether, in a computerized system known as FINDER (S. A. Cole 2001:253-54). Because the various AFIS databases were not linked, agencies were unable to share information or conduct national searches for a particular set of fingerprints. In 1994 the FBI sponsored a competition for a technological solution that would allow AFIS repositories to be connected to form a giant fingerprint database, linking hundreds of AFIS databases, making it a searchable, national fingerprint database. The FBI awarded Lockheed Martin the contract to build the IAFIS database (National Science and Technology Council Subcommittee on Biometrics 2006). IAFIS’s homepage describes the system as a national fingerprint and criminal history system maintained by the Federal Bureau of Investigation (FBI), Criminal Justice Information Services (CJIS) Division. The IAFIS provides automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses, 24 hours a day, 365 days a year. As a result of submitting fingerprints electronically, agencies receive electronic responses to criminal ten-print fingerprint submissions within two hours and within 24 hours for civil fingerprint submissions. (IAFIS 2008).

IAFIS is now undergoing expansion into a system called, in true Star Trek fashion, Next Generation Identification (NGI). In 2008 Lockheed Martin won a $1 billion, ten-year contract to expand IAFIS into NGI for the U.S. government. NGI is “the world’s largest biometric database” (Lipowicz and Bain 2008). Although “fingerprints will still be the big player” (Lipowicz and Bain 2008), the Next Generation program will also include biometric iris information, palm print information, and tattoo mapping, and is expected to include a greater range of biometric information down the line.

The 1990s also mark the expansion of biometric technologies to other programs, mirroring the growth of state surveillance systems, including their application to the U.S. welfare system. But the history of biometrics is not a neat chronology; the 1990s also is when biometric technologies began to expand from strictly access control and law enforcement appli-
cations to their introduction in prisons themselves. Although the first prison to include biometric retinal scanners to identify prisoners opened in Utah in 1988 (M. Browne 1988), prison use of biometric identification technologies occurred largely after 1990. In that year the Cook County Prison adopted biometric retinal scanning in order to track its prisoners. By 1995 it claimed to have identified 350,000 prisoners using retinal scanning technology (Ritter 1995). In 1994 Pennsylvania’s Lancaster County Prison became the first to use biometric iris scanners for prisoner identification (QuestBiometrics 2005). In the late 1990s adding biometric technologies to prisons became a booming business. Identix biometric technologies were increasingly adopted in California’s prison system between 1997 and 1999 (Beiser 1999). Between 1999 and 2002 biometric systems were installed at prisons in Florida and Massachusetts, expanding to include facial recognition technologies (“State Lines: Digital Prison Stripes” 2004). In 2000 the National Institute of Justice (the research arm of the Department of Justice) and the Department of Defense embarked on a research study comparing the use of different biometric technologies in prisons (Miles and Cohn 2006). In 2005 the International Biometric Group was awarded two grants totaling $900,000 from the National Institute of Justice to study prison applications of biometrics (International Biometric Group n.d.). Following 9/11 the biometric industry turned to bigger fish, including the multibillion-dollar contracts being offered by the newly formed Department of Homeland Security.

The Expansion of the Prison Industrial Complex

Biometric technologies were developed for the prison system at a time when the system itself was undergoing tremendous expansion. The massive growth in prisons of the surveillance, policing, and criminalization of marginalized communities is well documented (A. Y. Davis 1981, 1998, 2003, 2005; Garland 2001a, 2001b; Sudbury 2004; Gilmore 2007). With a dramatic shift from rehabilitation to punishment in the 1970s (Gilmore 2007) and in part as a result of “three strikes” laws, truth in sentencing initiatives, the war on drugs (Cole and Mobley 2005; D. E. Roberts 2001), the shift from a welfare state to a neoliberal state, resulting in dramatic cutbacks to social programs (Wacquant 2009; A. Y. Davis 2003), and the surveillance and criminalization of immigration, the number of people in prison has exploded in the past thirty years. Prison populations have risen by a factor of ten, from 200,000 in the late 1960s to more than 2 mil-

58 CHAPTER TWO
lion by 2000 (A. Y. Davis 2003). Today the United States has more people behind bars than any other country (Hartney 2006), an astonishing 25 percent of the world’s prisoners, although the country has only 5 percent of the world’s population (Critical Resistance 2000). The role of the prison industrial complex as an engine of inequality through the disproportionate incarceration of both poor people and people of color is widely noted; for example, 1 million African Americans are behind bars (Sudbury 2004), and despite studies finding little difference between drug use among people of color and white people (J. Webb 2009), over two-thirds of those in prison or jail for drugs are people of color (S. A. Cole 2007).

Nor can we disregard gender in theorizing inequality in the prison system. In keeping with worldwide trends in which poor racialized women and men with mental health disabilities are the fastest growing groups to be incarcerated (CAEFS 2004), African American women are now the fastest growing prison population, having outpaced African American men (A. Y. Davis 2003). The incarceration of poor women (and poor people generally) must be placed alongside the dismantling of the welfare state. The elimination of welfare programs like Aid to Families with Dependent Children causes women to seek out criminalized forms of employment so that they can afford food and housing. Sexual, emotional, and physical violence also propel women into the prison system (CAEFS 2004). As women flee abusive situations, the lack of a social safety net means they must turn to criminalized forms of labor such as sex work and the drug trade in order to meet their subsistence needs (Sudbury 2005; A. Y. Davis 2003). (It is important to note that, in addition to the fact that a huge proportion of women who end up in prison are survivors of sexual violence, the prison itself is a source of sexual violence, both through the rape of prisoners by guards and the state-sponsored sexual assault of the strip search; Sudbury 2005; A. Y. Davis 2003).

Homophobia, transphobia, and heterosexism and their intersection with sexism and racism render LGBTQ people vulnerable to the prison industrial complex. As Beth Richie’s (2005) study of young black lesbians shows, the relationship between homophobia and sexual harassment places queer women at increased risk of violence, sometimes leading to their engagement in illegal activities. Queer people have historically been and continue to be disproportionately caught up in the prison system, as queered sexualities are criminalized by the state (Kunzel 2008). Homophobia also continues to play a significant role in sentencing and in the
space of the prison. Queers are subject to disproportionate violence while incarcerated. For both queer men and queer women who were kept in separate prison wings, these spaces often resulted in worse treatment, including no programming and continual confinement with fewer activities than other prisoners (Kunzel 2008; Goldstein 2001). The role of homophobia in sentencing is understudied, but preliminary research indicates the ways that queer identities can result in more severe punishment. For example, it is well documented that homophobic judges and juries regularly assume that same-sex prisons are utopias for queer men and women and thus have no difficulty sentencing them to confinement (Kunzel 2008; Goldstein 2001). And research indicates that homophobia may have an impact on inciting judges and juries to condemn queer individuals to death (Goldstein 2001). For example, in the case of Wanda Jean Allen, a black lesbian accused of murdering her partner, part of the evidence that appears to have fueled the jury's decision to execute Allen was that she was a butch woman who "wore the pants in the family" and preferred the male spelling of her middle name (Gene). Evidence of Allen's butchness was used to question any suggestion that she and her partner were both abusive to each other, and instead was used to prove that she had used her masculine power to overwhelm her partner, evidence that played a role in the jury's decision to execute her, the first woman to be put to death in the state of Oklahoma. It is additionally notable that Allen did not have any funds to hire a lawyer, and the lawyer assigned to her case was paid only $800 (Goldstein 2001).

Disability also makes people more vulnerable to criminalization: "The U.S. Department of Justice estimates that 16% of the adult inmates in American prisons and jails—which means more than 350,000 of those locked up—suffer from mental illness, and the percentage in juvenile custody is even higher. Our correctional institutions are also heavily populated by the 'criminally ill,' including inmates who suffer from HIV/AIDS, tuberculosis, and hepatitis" (J. Webb 2009). Women with disabilities are one of the fastest growing groups to be incarcerated. As the prison system replaces state-funded efforts to address mental and physical health, people living with disabilities are increasingly caught up in the prison industrial complex.

The expansion of the prison industrial complex must be situated against the rise of global capitalism and the profits made from increased surveillance. As the U.S. spearheads an international turn toward neo-
liberal policies, the welfare state is being dismantled (Wacquant 2009), and prison building has risen to take its place (Sudbury 2005; A. Y. Davis 2003; Gilmore 2007; J. James 2007). Prison populations have risen alongside the decline of New Deal programs, including those supporting education, health, and welfare, meaning that members of many communities of color—including Native Americans, Latinos, and African Americans—have a greater chance of going to prison than of getting an education (Wacquant 2009; A. Y. Davis 2003). This has led some prison scholars to assert that "short of major wars, mass incarceration has been the most thoroughly implemented government social program of our time" (Currie 1998:10). As Dorothy Roberts (2001:91) explains, "The prison became our employment policy, our drug policy, our mental health policy, in the vacuum left by the absence of more constructive efforts."

The prison economy is big business. Warehousing 2 million people behind bars has provided companies like the Corrections Corporation of America and Wackenhut with unprecedented opportunities for profit (Myser 2007). Having one in every thirty-one adults in the U.S. caught up in the prison industrial complex—whether incarcerated or under surveillance following or in place of literal confinement—is extremely costly to taxpayers (J. Webb 2009). Local, state, and federal spending on corrections adds up to about $68 billion a year in the U.S. alone (J. Webb 2009). The drive for profits has led to many instances of abuse. Guards working for the Corrections Corporation of America complained "that they were encouraged to write up inmates for the most minor infractions and place them in segregation, which takes away points they've established for good behavior. It also adds a full 30 days to their sentences, which can help make about $1,000 for the prison in pure profit" (Frank 2009). One prison run by Corrections Corporation of America was described as a "hotel that's always 100% occupancy . . . and booked to the end of the century" (Welch and Turner 2007). In 2009 two judges pleaded guilty to charges that they took millions of dollars in kickbacks from a private prison company in return for sending juveniles to the company's privately run juvenile detention facilities (Urbina 2009; Freed 2009). The judges were discovered partly as a result of their exceedingly harsh approach to juvenile punishment:

Mr. Conahan's alleged partner in the scheme, Judge Mark Ciavarella Jr., reportedly sent kids to the private detention centers when probation officers didn't think it was a good idea; he sent kids there when their
crimes were nonviolent; he sent kids there when their crimes were insignificant. It was as though he was determined to keep those private prisons filled with children at all times. According to news stories, offenses as small as swiping a jar of nutmeg or throwing a piece of steak at an adult were enough to merit a trip to the hoosegow.

Over the years Mr. Ciavarella racked up a truly awesome score: He sent kids to detention instead of other options at twice the state average, according to the New York Times. He tried a prodigious number of cases in which the accused child had no lawyer—here, says the Times, the judge’s numbers were fully 10 times the state average. And he did it fast, sometimes rendering a verdict “in the neighborhood of a minute-and-a-half to three minutes,” according to the judge tasked with reconsidering Mr. Ciavarella’s work. (Frank 2009)

Making money by sending children to jail is just one of the terrible consequences of running prisons for profit.

Biometric companies too profited tremendously from the expansion of the prison system. Biometric technologies are enormously expensive. In the early 1990s Los Angeles law enforcement spent $15 million on mobile biometric fingerprint scanners (Adelson 1992). State police departments across the United States spent hundreds of millions of dollars installing live-scan fingerprint readers for local agencies. Valued at more than $30 million dollars each, live-scan readers and matching computers were installed in thirty-six states by 1992, costing a total of $1.1 billion (Adelson 1992). High-tech companies hoping to develop their technological products for the prison industry have valued sales of new technology at $1.4 billion (Business Editors and Technology Writers 2001). Clearly the addition of biometric technologies to the prison system must be located within the growth and privatization of the prison industrial complex itself.

Implications of Adding Biometrics to the Prison Industrial Complex

Given the astronomical start-up costs of biometrics, the industry had to find significant funding to get its technologies launched. In applying its technologies to the prison system, the industry found the necessary research and development funds from a combination of government subsidies, grants, and private-public partnerships. It is the billions of dollars of funding for systems like AFIS, IDENT, and other fledgling biometric surveillance systems that enabled this technology to get off the ground.
PRISONERS AS TEST BEDS FOR BIOMETRIC TECHNOLOGIES

The prison industrial complex offered another resource to a fledgling industry testing out a new product: prisoners' bodies are valuable commodities to biometric companies, providing the industry with a captive test population for assessing the efficacy of these new identification technologies. While the banking industry might be cautious about introducing biometric technologies to their clients for fear of scaring off potential customers, prisons do not have the same restrictions. In this way biometric technologies are key to the intensification of particular forms of monitoring, as they provide a way for companies selling surveillance technologies to try out products that would be rejected by the general public. As Calum Bunney, editor of the magazine *Biometric Technology Today*, based in the U.K., asserted:

In the outside world, having your retina or iris scanned can be an inconvenience. Not so in the coercive environment of the clink, where biometric technology is used to great effect. A bank will obviously not want to put its customers off by falsely rejecting them when they want to access their account via a biometric ATM. . . . A prison, on the other hand, has a captive audience, and can make the user of a biometric device perform the actions required for passing as many times as it likes until it is satisfied. Who cares if the customer doesn't like it? (Glave 1997)

The biometric industry used the prison industrial complex as a giant laboratory where they could refine their technologies without fear of reprisal. The rights of prisoners to refuse biometric technologies were considered negligible:

Larry Cothran is pretty frank about the degree to which civil rights and privacy issues figure in his work. They don't. "When you come on to a state property, you give up most of your rights," Cothran says.\(^\text{11}\) As executive officer of the Technology Transfer Program with the California Department of Corrections, Cothran evaluates and recommends systems that are expressly designed to watch, detect, secure, and contain some 155,500 inmates in 32 prisons across California. (Glave 1997)

Testing biometric technologies in places where they can't be refused has a number of implications. For example, biometric retinal scanning is
not in widespread use, partly because retinal scans are very difficult and
time-consuming to take, and people dislike having their eyes so close to
the scanner. Another reason is that biometric retinal scans can reveal
significant amounts of health information, including pregnancy, HIV sta-
tus, diabetes, and other information that might have a significant impact
on the person's health privacy (Shaikh and Dimitriadis 2008; Kiruba
2005). Although this presents an obstacle for their development for other
applications, because prisoners cannot decline to be scanned means these
technologies can continue to be refined and find a market in the prison
system.¹²

PRISONERS AS HUMAN INVENTORY

"In risk society, policing is not just a matter of repressive, punitive, deter-
rent measures to control those who are morally wrong. It is also a matter
of surveillance, of producing knowledge of populations that is useful for
administering them" (Ericson and Haggerty 1997:41). Biometric technol-
ogies are used to produce new forms of knowledge about prison popula-
tions. Producing every incarcerated body as a strand of binary code paves
the way for understanding prisoners as human inventory. It is a form of
corporeal fetishism that reduces complex human bodies to products used
to generate value for the prison industrial complex. Connections between
merchandise and prisoners are often made explicit:

In a small-town grocery store, a routine inventory is under way. Clerks
move quickly among the shelves of canned goods and boxes of pasta,
holding scanners in their hands, passing them over bar codes and
flashing information back to the store's central database.

Down the road, in the state correctional facility, officers move among
inmates "counting heads"—not just once, but several times during the
course of the day. Another type of routine "inventory" is being con-
ducted, but this one consumes much more time and resources. Soon,
however, correctional officers may have access to improved technology
that makes counting inmates go as quickly, smoothly and accurately as
other inventory counts. (Lewis 2003)

There are implications to using biometric technologies to count heads
in ways that reduce the bodies of criminalized individuals to biometric in-
ventory. For example, counting heads provides an opportunity for guards
to determine if a prisoner is ill, injured, or otherwise in distress. It also
provides inmates with a set of eyes to bear witness, including to forms of prisoner resistance or protest. How effective would a hunger strike be if a biometric scanner were the only bystander? The addition of biometric technologies to prisons also has consequences for prisoners’ health and well-being, as well as for the means of protest available to them. Biometric representations of the body as a simple series of ones and zeroes reinforce existing ideologies in which prisoners are reduced to numbers that need to be counted instead of being understood as human beings to whom we need to attend.

BIOMETRIC TECHNOLOGIES AND KNOWLEDGE ENGINEERING

In a short paper detailing the benefits of adding biometrics to law enforcement, Clive Reedman (n.d.), a biometrics industry representative, describes one of the central advantages of these new identification technologies as “automation.” Reedman explains that, if compelled to identify a large population for hours on end, he “will become tired, bored, or distracted: I will need to take a break and eventually sleep. My concentration will fail and I will make mistakes.” Unlike humans, biometric scanners never get tired, are never lazy, nor do they commit errors. As biometric technologies regularly are represented as able to improve upon human failings, they are easily incorporated into what are broadly termed systems of “knowledge engineering,” processes that are meant to replace human decision makers with computers: “Knowledge engineering is an iterative process that allows the expert and knowledge engineer to continue to refine the rules and facts embedded in the expert system until it functions at the level of the expert. Unlike conventional computer programs, expert systems are designed to be readily modifiable to incorporate new, conflicting, or incomplete information” (Lynch and Rodgers n.d.). In this way biometric technologies are imagined to be able to improve upon subjective human experts by providing mechanical objectivity, eliminating the need for human intervention. This rhetoric hides how these new identification technologies both codify and intensify existing cultural assumptions and inequalities.

LABOR, BIOMETRICS, AND SURVEILLANCE

Questions of labor are central to understanding the growth of the prison industrial complex. One of the reasons that privatization can be marketed as cost-effective is because it paves the way for reductions in pay. Rather
than being compelled to hire highly trained, unionized prison workers, privatization allows companies to hire personnel and give them little to no training, keep them permanently on part-time work, and thus reduce their wages. As Pat Cannan, a representative with Wackenhut, says:

“We don’t pay a lot of overtime, and maintain a part-time work force.” Stock options in the company are given rather than cash, if for no other reason than that it’s usually cheaper for these businesses to do so; in 1996, annual earnings for unionized prison staff was about $33,330, while the non-union boys, even with the stock options the companies love to talk about, only made about $24,000—or a whole third less in total income. (Montgomery 2001)

Paying workers less is only one part of the prison industry’s strategy for cutting down on expensive labor costs. Another strategy is to replace human personnel with machines. Biometric technologies are central to this strategy. As industry experts reported, biometric technologies eliminate the need for human screening, helping to cut costs.

Before they discovered Schlage Recognition Systems HandKey, Northern Ireland Prison Services monitored all comings and goings at its prisons by posting guards at all access sites and supplying them with keys. This was an expensive policy, given the guards’ high salaries. . . .”We were able to install a pair of HandKeys for a one-time payment of less than one-fourth of what we paid each guard annually,” said Michael Pepper, Director of Activities and Services at Maghaberry Prison. “And costs were not the only consideration. HandKeys are not subject to intimidation, for example, nor do they tire easily.” (Schlage 2006)

Identifying prisoners biometrically also allows for intensified forms of surveillance, including of prisoner labor. For example, biometric checks can be used to monitor prisoners while they are at work, including ensuring that inmates have their pay docked if they take too many bathroom breaks:

“Inmates are always playing games,” Donlin [corrections program manager at the National Institute of Justice’s National Law Enforcement and Corrections Technology Center] says. “They get paid, say, 40 cents a day to work in the work center and they report to work. But then
they say they have to go to the doctor, they have to go to the psycholo-
gist, they spend the whole day running around, then claim they were
there the whole time. Using this system for portal control would track
their movements and show that they shouldn’t be paid for that day.”
(Lewis 2003)

Given the consequences for prisoners’ health, privacy, labor rights, and
well-being, the effect of adding biometrics to the prison system goes far
beyond technological efficiency.

Summary
The rise of biometric identification technologies was accompanied by
industry and governmental assertions that biometric identification pro-
duces the truth of identity, a truth that can be neither distorted nor con-
cealed. Yet given the fraught conditions under which biometric identities
are wrested from prisoners’ bodies, the integration of these technologies
in the prison can hardly be regarded as a success. Although parallel de-
velopments occurred in welfare as well as in the financial, military, and
health sectors, the driving logic behind the expansion of biometric identi-
fication is the control and management of marginalized communities.
The development of biometric technologies resulted in the intensification
of existing processes of criminalization while increasing corporate profits
—calling into question industry claims that biometric technologies func-
tion with mechanical objectivity. However, although biometrics fail to
function in the neutral ways that industry claims, these technologies
succeed even where they fail. Making captive populations productive by
using biometric technologies to transform bodies into binary code allows
vulnerable bodies to be spun into gold.

With the decline of the welfare state and the intensification of state sur-
veillance, the prison industrial complex has stepped in to fill the gap for-
erly occupied by the educational system and a more expansive social
safety net. Biometric companies with a vested interest in expanding their
profits and state legislators with conservative agendas represent these new
technologies as the panacea for fixing what is broken in the prison system.
Thus technological solutions are offered up to solve social problems, and
the same vulnerable communities—poor people, queers, women, and
people of color—serve as the raw materials upon which to test new tech-
nologies. Besides marking a return to nineteenth-century claims about
the possibility of reading criminality right off the body, biometrics have ramifications for the state's most vulnerable populations in ways that reinforce existing forms of systemic inequality, including sexism, racism, classism, and homophobia.

Despite the significant human and economic costs of these technologies, technological solutions to the problems of poverty are on the rise. With their eyes firmly fixed on the potential for profits to be made in the prison system, new high-tech companies are attempting to get themselves a piece of the pie by positing ever more draconian technological solutions to social problems. Most recently injecting prisoners with chips containing biometric information is being offered as the ideal solution to the problem of violent offenders, a problem that comes with a $1.4 billion price tag for the company in question (Business Editors and Technology Writers 2001). And the biometric industry continues to seek other clients for its markets.
Teaching a Critical Digital Literacy of Wearables: A Feminist Surveillance as Care Pedagogy

Les Hutchinson, Maria Novotny

Abstract

This article critically responds to the collection of data drawn from the body and the surveillance of everyday experiences via the use of wearable technologies. Bringing together feminist methodologies in rhetoric and writing with feminist conversations in surveillance studies, Hutchinson and Novotny argue that a feminist surveillance as care pedagogy teaches professional writing students a user-centered design practice that supports consent and user agency, and resists ubiquitous, non-consensual surveillance of user’s bodies. Their pedagogy centers on acquisition of critical digital literacies as necessary for teaching students to engage with emerging technological issues, specifically ones raised when considering the ethical implications with surveillance and privacy. The two courses outlined in this article approach wearable technologies through the lens of rhetorics of health and medicine, enabling the kind of critical digital literacies needed to interrogate privacy and surveillance concerns that impact students—a demographic most often targeted as users of these technologies.

© 2018 Elsevier Inc. All rights reserved.

Keywords: Surveillance studies; Feminist research methodologies; Feminist pedagogies; Critical digital literacy; Professional & digital writing

Strategically hidden inside our computers are files that track our movements on the web. Inside the files are long strings of alphanumeric codes that do not reveal, on the surface, the kinds of personal information they contain. Concealed inside the code, such personal data includes housing type, age, sex, income, spending habits, hobbies and interests, items bought, items you’re interested in buying, if you’re traveling soon, and other data that may be fairly revealing. ~Estee Beck, The Invisible Digital Identity

1. Introduction

On June 19, 2017 privacy researchers exposed the secret relationship between AcurianHealth and Walgreens (Hill & Mattu, 2017). Researchers Hill and Mattu found that AcurianHealth had been paying Walgreens to gain access to all their customer’s pharmacy records, and that Walgreens had authorized this use of its customer’s health information in its privacy policy. AcurianHealth used this information to target Walgreens customers with advertising promotions

* Corresponding author.

E-mail addresses: hutch220@msu.edu (L. Hutchinson), novotnym@uwosh.edu (M. Novotny).

https://doi.org/10.1016/j.compcom.2018.07.006

8755-4615/© 2018 Elsevier Inc. All rights reserved.
about new pharmaceutical drugs for health-related diseases and illnesses. Often, this targeted advertising was for health issues Walgreens customers did not currently have, but were based upon searches done in their browser history. Hill and Matt’s article points to the depth of health privacy issues within a society that is growing ever-increasingly connected to the Internet. Wearable technologies that sync the body to health applications should sit at the forefront of any conversations about data collection and safety because of the lack of privacy regulations such as the Health Insurance Portability & Accountability Act (HIPAA) overseeing them. The tech-health industry normalizes its practice of unethically sharing private customer health information with unknown third parties through its Terms of Service/Use contracts and Privacy Policies (ToS/C and PP). Therefore, we propose this article as a pedagogical response to the lack of conversation regarding these privacy concerns as they relate to the growing digital and mobile infrastructure in health communication.

Teaching critical digital literacies of health and wearables within professional writing programs introduces privacy issues to students who, arguably, are both being marketed for wearables and may become future designers of these technologies within industry-related fields after graduation. Stuart Blythe, Claire Lauer, and Paul Curran’s (2014) study on the workplace writing practices of professional writing alumni make clear that “the availability of digital and mobile technologies has blurred the lines between the personal and professional purposes” (p. 282). As instructors of professional writing, we believe it imperative as Stephanie Vie (2017) writes “to equip our students for the kinds of communication they are likely to do post-graduation” (p. 354). This means that our professional writing curriculums and courses reimagine the scenes of professional writing – as they apply to more mobile, and thereby wearable, technologies. Such serves as our exigence for this article and our attention to the intersections of surveillance and wearables in the professional writing classroom.

We open then with the Walgreens/AcurianHealth incident as one professional writing case where everyday surveillance practices establish the collection of data from the body, potentially causing immediate and lasting affects for people (see, too, Shane Wood’s article in this issue for further discussion of the affective experiences with wearables that impact our mental and emotional states). Private health information is protected by privacy laws such as HIPAA. However, HIPAA does not protect health data provided within wearable technologies, thus such private bodily information becomes forms of data products that can be legally shared within a consumerist, corporate system without users’ knowledge. Research in surveillance studies (Abu-Laban, 2015; Lyon, 2002) shows that privacy criticism is often theoretical and rarely takes up affect, particularly when it comes to bodies. We see professional writing courses needing to address how privacy concerns within technological systems implicate the body in real, material ways. In their article “Beyond Students as Users” (forthcoming), Dawn Opel and Jacqueline Rhodes critique industry’s influence on composition studies because of how they see the rhetoric of expediency, efficiency, and engagement defining users as merely consumers, thus limiting technological choices and participation in civic life (“Beyond student as user”). Informed by their critique, we model a pedagogy that addresses embodied, material privacy health concerns within professional writing courses. Such a model encourages students to develop a critical digital literacy (Beck, 2015; Vie, 2008) regarding the collection of personal data as well as surveillance’s affective consequences. Our careful scaffolding of readings and assignments guides students into a material understanding of how their own (as well as their loved ones’) information is commodified and circulated. By the end of the course, students gain a critical digital literacy about how data is not just an artificially constructed artifact, but, rather, how data is a visual and virtual representation of the physical body. Students leave the course with a knowledge of the real risks posed to the body when personal data is not secure (Figs. 1 and 2).

This article responds to the call for this special issue urging scholars in rhetoric and composition to consider the various literacies required to navigate concerns that arise with the collection of personal data via wearable technologies and their mobile health apps. This response – a feminist surveillance as care pedagogy – offers a student-centric, relational model, which centers on the development of critical digital and health literacies; both we see as necessary.

---


2 We situate professional writing within the discipline of rhetoric and composition. As such, in this article, we focus on professional writing courses but understand our proposed pedagogy examining wearables could be adopted to other courses in the discipline of rhetoric and composition and throughout the discipline.

3 Jason Tham and Ann Hill Duin’s chapter in Writing in the Digital Age details how Oral Roberts University mandated that all college freshman wear Fitbits and follow a rigorous ideological code of conduct in order to succeed at that university.

4 This article is slated to come out in Computers and Composition prior to this special issue.
to rhetorically analyze, critique, and respond to the increasing investment and dependence on wearables. We refer to Opel and Rhodes’s critique, but also look back to Kristin Arola’s (2010) worry that “the loss of design production in Web 2.0 might lead to a less critical consciousness not only about the meaning design conveys but also the ways in which that meaning is enmeshed in the world around us” (7–8). Arola worried about an uncritical approach to design due to the shift to Web 2.0 technologies, which is relevant to our work in that we, too, worry that this loss of critical consciousness meant a lack of awareness regarding digital privacy as well—especially as this loss relates to ubiquitous data collection enabled through the design of wearable technologies.

Our article focuses primarily on issues regarding digital privacy and online health information because of the lack of attention these conversations have had in the greater rhetoric and composition discipline. In 2016, Estee Beck and Les Hutchinson put a call out for an edited collection entitled Writing in a digital age: Surveillance, privacy, & writing infrastructures in an attempt to amend this lack. They acknowledged the last twenty years of rhet/comp scholarship covering surveillance and privacy issues regarding course management systems, plagiarism detection software, social media use in and outside the classroom, and gaming technologies, but also recognized a need for “scholarship that analyzes surveillance and privacy from more culturally-situated and community-oriented

<table>
<thead>
<tr>
<th>Enacting a Feminist Surveillance as Care Pedagogy</th>
<th>A Scaffolding of Les’s Course: “Technical Writing”</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weeks</td>
<td>Readings</td>
</tr>
<tr>
<td>-------</td>
<td>----------</td>
</tr>
<tr>
<td>1</td>
<td>- &quot;Work Patterns&quot; (Hart-Davidson)</td>
</tr>
<tr>
<td></td>
<td>- &quot;What do technical communicators need to know about information design&quot; (Schröer)</td>
</tr>
<tr>
<td></td>
<td>- &quot;How can technical communicators evaluate the usability of artifacts?&quot; (Mirel)</td>
</tr>
<tr>
<td>2</td>
<td>&quot;Making New Media Make Sense&quot; from Nancy K. Baym’s Personal Connections in the Digital Age</td>
</tr>
<tr>
<td>4</td>
<td>Laura Gurak’s Persuasion and privacy in cyberspace</td>
</tr>
</tbody>
</table>
Fig. 1. Les’s “Technical Writing” Course Scaffolding.

<table>
<thead>
<tr>
<th>3</th>
<th>Data Detox Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>“The Invisible Digital Identity” (Beck)</td>
</tr>
<tr>
<td>7</td>
<td>“Video Games and Surveillance” (Vie &amp; deWinter) and “Digging into Data: Professional Writers as Data Users” (Gonzales &amp; DeVoss)</td>
</tr>
<tr>
<td>10 - 12</td>
<td><em>Students chose one day from the Data Detox Guide and wrote a reflection on the steps they enabled to adopt that day’s privacy task and then an analysis of how accessible the directions were presented from a technical writing perspective.</em></td>
</tr>
<tr>
<td>6 - 9</td>
<td><em>Students read Beck’s article, then wrote a response describing their experience with downloading Ghostery, using it, and what they learned about their browsing behaviors.</em></td>
</tr>
<tr>
<td>10 - 16</td>
<td><em>Students wrote a response on the two readings and what they contributed to the course thus far. We determined that the Gonzales and DeVoss article was not written for professional writing students, and was thus somewhat discursively inaccessible.</em></td>
</tr>
<tr>
<td>3</td>
<td><em>Students only wrote one response at the end of the text that expressed their stance on the ethics of obfuscation in regard to privacy and protest.</em></td>
</tr>
<tr>
<td>6 - 9</td>
<td><em>Critique, analysis, and response</em></td>
</tr>
<tr>
<td>6 - 9</td>
<td><em>Critique and analysis</em></td>
</tr>
<tr>
<td>10 - 16</td>
<td><em>Analysis</em></td>
</tr>
<tr>
<td>6 - 9</td>
<td><em>Analysis and response</em></td>
</tr>
</tbody>
</table>

**Big Project Proposal:**
After meeting with our REHS partners, students separated into groups based on theme and drafted a project proposal that stipulated how they would execute the creation of technical documents to fulfill their theme’s focus in the Safer Internet Guide. REHS reviewed proposals and offered feedback twice during the semester.

**The Big Project:**
Students spent the remainder of the course researching, drafting, and finalizing their groups’ portion of the Safer Internet Guide for REHS. They presented nearly finished final drafts of their groups’ project as a class to REHS during week 16, then revised them for final submission during finals week.
perspectives” (Beck & Hutchinson, 2016). Therefore, we seek to further respond to such loss of consciousness by merging conversations around surveillance, privacy and technologies to health and medicine, and ponder how these scholarly interests may translate and hold relevance in the rhetoric and composition classroom. We see wearables and the mobile health apps often used in wearable technologies that collect and survey private health information as a useful source of rhetorical inquiry. The professional writing classroom (and its interdisciplinary curricular) is an ample and needed site for our the methodologies guiding our research to be translated into critical pedagogical practice. Incidentally, it is not enough to simply research these conversations about surveillance, data, and privacy as they implicate the body. As the editors to this special issue note, mobile health wearables ground the body into an immersive surveillance experience, which makes the material risk of data collection tangibly real and affective. We view it our task to influence and pedagogically design moments of immersion, interruption, and interrogation for our professional writing students – the future designers of these technologies – to facilitate real and effective change in the collection and consent of personal health data.

The perception we often have of surveillance falls under quick, catch-all metaphors such as Big Brother, the panopticon, and a harkening to Orwell’s 1984. However, we use the classroom to trouble this kind of universalizing of surveillance as singly, solely negative. Our Western society’s reliance and enthusiasm for technologies will not halt anytime in the near future; data is being collected whether we want to participate in it or not. It is for that reason that we theorize a feminist approach to surveillance: to resist universalizing surveillance as negative and to rethink

<table>
<thead>
<tr>
<th>Enacting a Feminist Surveillance as Care Pedagogy</th>
<th>Maria’s Course “Digital Rhetoric in Health &amp; Medicine”</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enacting a Feminist Surveillance as Care Pedagogy</strong></td>
<td><strong>Maria’s Course “Digital Rhetoric in Health &amp; Medicine”</strong></td>
</tr>
<tr>
<td><strong>Foundational Theories</strong></td>
<td><strong>Weeks 1-3</strong></td>
</tr>
</tbody>
</table>
|  |  | • “Identifying New Topics in TC Curricula: Preparing Students for Success in a Changing World” (Spyridakis) | • Module 1a: Digital Rhetoric Manifesto
  • Objective: Draw on foundational texts & experiences to articulate what digital rhetoric means to you. |
|  |  | • Because Digital Writing Matters (DeVoss, Eidman-Aadahl & Hicks) | • Module 2: Mini Digital Research Project
  • Objective: Develop digital literacy research skills and critical awareness of how online personal information may put individuals at risk. |
|  |  | • Digital Rhetoric: Theory, Method, Practice (Eyman) |  |
|  |  | • “Personal Connections in the Digital Age” (Baym) |  |
|  |  | • “User Data on the Social Web” (Reyman) |  |
| **Analysis**  | **Weeks 4-6** | **Key Readings** | **Assignments** |
|  |  | • Persuasion and privacy in cyberspace: The online protests over lotus marketplace and the clipper chip (Gurak) | • Module 3: Mini Digital Analysis Project
  • Objective: Practice rhetorical analysis of a digital health technology, such as a wearable and connect analysis to a theoretical lens (such as feminism), which may expose potential risk danger or related questions to the use of the technology. |
|  |  | • “The invisible Digital Identity” (Beck) |  |
|  |  | • Selections of Race in Cyberspace (Nakamura) |  |
|  |  | • Optional watching of film “Snowden” |  |
|  |  | • “Using a fitness app taught me the scary truth about why privacy settings are a feminist issue” (Quartz) |  |
|  |  | • “How a Company You’ve Never Heard |  |
Fig. 2. Maria’s “Digital Rhetoric in Health & Medicine” Course Scaffolding.

data collection from within a feminist ethical framework. Our feminist surveillance as care pedagogy considers the role professional writers have in the design of technical documents like ToS/C and PP to promote agency and care among technology users. We ask students to engage in three rhetorical acts (analysis, critique, and response) as they design documents, and even the health applications themselves, to reposition users as agents over their own data and their health. Students study health wearables and their associated technical documents, engaging in coursework that combines rhetorics of surveillance and privacy and rhetorics of health and medicine (RHM). This pedagogy allows critical digital literacies of health wearables (Chinn, 2011) to emerge within carefully scaffolded coursework and models a feminist approach to considering the needs of bodies in relationship to data.

We offer this pedagogical model with supplemental course materials from professional writing classes we have taught to show examples of how a critical digital literacy of privacy and health, when coupled with a feminist surveillance as care framework, can be enacted in a multitude of professional writing courses by focusing on wearable technologies. We share two course designs in this article. Both designs expand conceptions of topics traditionally taught in rhetoric and composition. Specifically, this article brings together topics from across the fields of surveillance studies, service learning/community-engagement, and feminist ethics to address the new interfaces professional writers now encounter. 

Jan Spyridakis (2015) argues that when developing technical communication curriculum focusing on rhetoric, writing, editing, and design, teacher-scholars should consider “who is using and interacting with the products that technical communicators create, and what those artefacts are” (p. 35) as topics of inquiry in courses. While speaking to the
field of technical communication, we apply Spyridakis’ recommendation to the teaching of wearables in rhetoric and composition, suggesting that their design and their related technical documents (such as PPs and TOS/Cs) are indeed texts in need of rhetorical inquiry given their increasing use and dependence. That is, we see rhetorical inquiry around wearable technologies as an opening into conversations of designing for user agency and consent, specifically examining this in the context of privatized health information.

2. A Need for Surveillance Studies and Feminist Ethics in Rhetorical Wearable Inquiry

In their 2012 article “Surveillance studies and the violence against women,” Corinne Mason and Shoshana Magnet establish that “conversations about violence against women are rarely referenced in the increasingly ubiquitous discussions about the decline of consumer privacy” (p. 106). Mason and Magnet trace surveillance’s historical relationship to inequality, and in their research, learned that “while inequalities have been paid serious attention in the field, axioms of oppression are rarely analyzed simultaneously” (p. 107). They identify a lack of scholarship focusing on how surveillance is used to perpetuate violence against women, and call for surveillance studies scholars to investigate the relationship between surveillance technologies and gender-based violence (such as stalking). They offer their theoretical framework to not only initiate this research, but to also consider “how some technologies may help women find safety from abusers” (p. 107). Mason and Magnet also cite what was at the time an upcoming volume titled Feminist Surveillance Studies (Magnet & Dubrofsky, 2015). This volume, Mason and Magnet find, continues the focus of scholarship they state is needed in the field.

Dubrofsky and Magnet’s (2015) edited collection further establishes feminist-focused scholarship in surveillance studies. They assert that this volume presents additional frames for thinking about surveillance because it demonstrates the importance of thinking beyond contemporary developments in new technologies and the intensification of surveillance since the 1980s, tracing the history of surveillance back to organized forms of state control such as slavery, the management of women’s reproductive autonomy, the regulation of sexuality, and the institutionalized scrutiny of those living in poverty. Rather than rehashing arguments as to whether or not surveillance keeps the United States safe, we instead take an intersectional critical feminist approach to illuminate what constitutes surveillance, who is scrutinized, why, and at what cost. (p. 15)

Dubrofsky and Magnet see the historical tracing of surveillance back to its systemic discrimination of socially-marginalized peoples. Their volume continues research in the historical processes that have enabled these technologies to be created in the service of technological forms of discrimination. Dubrofsky and Magnet’s edited collection shows the need for even more scholarship to scrutinize surveillance’s affects and material realities for non-dominant bodies, particularly women.

In addition to Dubrofsky and Magnet’s collection, surveillance studies scholar Yasmeen Abu-Laban’s work is the most recent scholarship in the field to approach surveillance from an explicitly feminist perspective. Her article “Gendering Surveillance Studies” critiques surveillance studies for having surprisingly few analyses of how surveillance can be thought through acts of compassion and care. She refers to these frames, compassion and care, as the other face of surveillance—their counterpart being control and violence (very masculine acts). She asks what we felt to be an intriguing question: “Are we fully recognizing emotive complexities around issues of surveillance?” (p. 44). This question, she hopes, will prompt researchers to look at how surveillance can be used as a tool of care and support when people are able to have technological means in which to look out for one another and themselves. Like Mason and Magnet believed that technologies can be used to help protect women from abuse, Abu-Laban urges scholars to reconsider surveillance as strictly negative. Seeing surveillance as enabling people to act with compassion and care continues to challenge a one-sided perception of data collection.

Rhetoric and composition scholars have attended to issues of surveillance and privacy with regard to how these impact the scholarship in our discipline. Estee Beck’s (2014, 2015, 2016a, 2016b, 2017) and Estee Beck et al. (2016), work, for instance, has provided us with multiple critiques of algorithms and data collection. Stephanie Vie’s (2008, 2013, 2014, 2015a, 2015b, 2016), deWinter Jennifer and Vie Stephanie (2016) and Beck et al. (2016) work, too, has analyzed the impact of surveillance on games and students through grading technologies such as Turnitin.com. Tim Amidon and Jessica Reymans’s (2014) chapter in Cultures of Copyright explicates how social media companies retain the rights to collect, use, and control the information contributed by their users—in other words: hidden ownership policies that are made valid through TOS/Cs and PPs. With an attention to the growing trend and impetus for scrutinizing
surveillance practices, Beck and Hutchinson (forthcoming) noted the need for more sustained critique of surveillance practices and looks specifically to how surveillance impacts the field writing studies.

Despite the growing repository of robust scholarship on these topics, there has yet to be any focused attention on how surveillance and privacy intersect with RHM. Jennifer Malkowski, Blake Scott, and Lisa Keränen’s (2016) “Rhetorical Approaches to Health and Medicine” cite what Lisa Meloncon and Erin Frost (2015) call “a capaciousness to rhetoric” inviting a variety of perspectives into RHM including feminist theory. They argue such capaciousness indicates new need to examine the role of emerging technologies in health and medicine as well its use of big data. Catherine Gouge’s and John Jones’ special issue “The Communication Design of Wearable Technologies in Health and Medicine” in Communication Design Quarterly begins to open up the field of RHM to intersections of wearables as inquiry. We join these conversations by proposing a feminist surveillance as care framework. This framework argues the necessity to analyze the data collection performed by a wearable technology and its corresponding ToS and PP, looking at how that collection affects user agency and consent.

Feminism and surveillance studies meet RHM in connecting Erin Frost’s (2013, 2014) rhetorical critique of efficiency and Abu-Laban’s (2015) proposal of surveillance as care. Frost’s critique of efficiency, informed from her apparent feminist methodology, is feminist as it examines how efficiency has been valued as an apparent and pragmatic model of labor within corporate systems. Her work exposes how valuing efficiency often fails to fully address the cultural feminist means of marginalized bodies. For us, tending to the work of efficiency is vital when interrogating the purpose of wearable technologies. Frost’s critique of efficiency asks: for whom is this product made efficient? Important is this question given the continuous marketing of wearables as a self-empowering device, most notably, because of how efficiently wearables gather, analyze and report data to the user. It is in this context of empowerment that we may view surveillance as caring. Yet, when we look further into the ownership of users’ data, this appeal to self-empowerment given the device’s efficiency is troubling. Such a critique allows us to see the double-edged sword of wearables as efficient and empowering devices. We bridge Frost’s critique with Abu-Laban’s feminist understanding that surveillance can translate to care as an empowering practice in how women use self- and co-monitoring sharing practices within technological systems. Abu-Laban states that “just as ‘care’ blurs into control, it may be equally relevant to consider the ways in which ‘control’ may blur into care” (p. 53). Reorienting control as an extension of care “may alert us to emotive and expressive components of surveillance in ways that sharpen our collective understanding” (Abu-Laban, 2015, p. 55). Care, as a practice, repositions affect differently as it works in tandem with surveillance—a practice that analyzes and critiques monitoring processes from a more feminist perspective.

3. Feminist Surveillance as Care: A Pedagogical Framework for Engaging with Wearables

We share the origin of how framework emerged as it illuminates our embodied feminist methodological approach (Johnson, Levy, Manthey, & Novotny, 2015) to the study of surveillance and wearable data. As such, we set the stage for how interest and investment in examining this issue came to be. Our friendship started during the 2014 Computers and Writing conference. There, Les, an incoming PhD student, met up with Maria who was starting her second year, both in the Rhetoric and Writing program at Michigan State University. Over dinner one night at the conference, our conversation shifted from school to concerns about the healthcare system and need for more feminist approaches to medicine. Maria explained her experiences with the fertility and urology industry, and Les described her time working in emergency rooms and a fertility clinic. We shared our aggravation for how medicine as an institution has always prioritized the care and treatment of able-bodied cis men. Joking about the possibility of opening a hospital that operated with specific attention to women, gender queer, and transgender people’s needs, this playful, yet serious conversation initiated scholarly collaboration bringing together Maria’s and Les’s main fields of study: feminism, health, medicine, and privacy.

Fast-forward a few years and we are sitting on Les’s couch one evening and talking about our research. Maria shared how friends of hers within the infertility community were raving about the fertility mobile application, GLOW. Interested in what the buzz was about, Maria told Les that she began initial research about the application. Maria’s interest in GLOW emerged as she learned about the app from those in the infertility community. Many in the community shared with Maria how they were excited that the app provided reassurance that if pregnancy did not result after usage of the app, then their money would be reallocated towards fertility treatment. This promise enticed many who struggled to conceive, as many insurances fail to provide comprehensive fertility coverage. The marketing of the app thus lured many in the community to consider using it. Realizing the interest and potential value such an app could provide to the
infertility community, Maria shared with Les the need to rhetorically investigate GLOW’s term of service and privacy policies, especially given the numerous amounts of intimate, private data the app collects.

On the surface, the application appeared intriguing as it guaranteed those unsuccessfully conceived after 10-months of use a “payout” to support fertility treatment at preselected clinics. Given the fact that fertility treatment is frequently not covered by most insurances, Maria shared with Les how GLOW was uniquely and strategically marketing itself as not only a mobile health application empowering women to better understand their reproductive cycles, but offering assistance with the potential cost of fertility treatment. Maria and Les began to map how GLOW appears to provide users with the ability to control and have agency over their reproductive health and finances. Maria was curious about the relationships GLOW had with fertility clinics as the app offered pre-selected treatment locations. Les became concerned with how GLOW may be treating private user data. We quickly realized that there seemed to be both privacy implications and a lack of transparency in its marketing campaign.

Here, we bring together Frost, as a feminist RHM perspective to critique the efficiency of gendered wearables, with Abu-Laban, whose proposal that surveillance can mean care offers people a more compassionate connection with technology. Connecting these two theoretical positions enables us to assess how applications like GLOW have attempted to claim care as an outcome of application use, but fail users in their “efficient” design, which we argue disempowers the user. GLOW’s current model of data collection includes unilaterally collecting of user data without consent, selling that data to unidentified third parties, and retaining ownership rights to all user data indefinitely without giving users any legal rights to amend these surveillance practices. A feminist design would adopt adjustable terms and conditions that would allow users to decide what data is collected from them, how long it is stored by GLOW, to whom it is sold, and have the legal rights to retain ownership over their digital intellectual property. Therefore, we introduce a surveillance as care framework that offers a three-step pedagogical process for engaging in methodological feminist intervention in health wearables. First, this framework rhetorically analyzes the collection of bodily data by wearable technologies. Second, it critiques how these technologies fail to design transparent technical documents such as ToS/C contracts and PP that impact user consent in regard to understanding how their bodily data is collected, interpreted, and co-opted for biocapitalist5 uses. We frame this as critiquing the “apparent” efficiency of those technical documents when such proclamations raise the issue of for whom are these documents efficient. Third, it engages in a feminist response to identify areas of critique by modeling critical digital health literacies for users of wearables.

This framework offers an explicitly feminist approach to addressing the current collection of bodily data in wearable health technologies. Often, these technologies are touted and marketed with a technologically determinist inflection that they will bring users freedom, control, and self-empowerment over their health. The critique portion of the framework actively interrogates the rhetorical interplay between what a mobile health app hosted on a wearable technology promises and what it does when it collects information off the body. Then, a reflective feminist response is offered as a call for either an ethical redesign of the wearable app and its related technical documents or deliverables that promote a critical digital health consciousness.

3.1. Enacting a Feminist Surveillance as Care Pedagogy

We see our framework, intervening in the design and technical documents of wearables, as not isolated from the classroom, but wholly inspired by our pedagogical learning goals, which foremost value feminist ethics and user advocacy. Given this, we propose a feminist surveillance as care pedagogy to address the very real, embodied, and material privacy health concerns in wearable health technologies by situating them as the main focus in professional writing courses. We apply this framework to professional writing as we view it as a curriculum that trains students not only how to engage with the discourse and practices of professional writing but interrogate and redesign notions of professionalism6. Hence, a pedagogy focused around the rhetorical principles of analysis, critique and response (or re-invention). A feminist surveillance as care pedagogy focuses a professional writing course on three distinct rhetorical actions, each reflective of the framework we outline above:

5 We situate biocapitalist uses within the emergence of biocapitalism, which Pierce (2011) defines as a “model that arose from the complex set of relations existing between technoscientific research and neo-liberal practices of economic development” (p. 2.).
6 See Danielle DeVoss’ conference paper, Feminist/Citizen/Activist Designer, presented at the 11th Biennial Feminisms and Rhetorics Conference at The University of Dayton.
1. **Analysis:** The first rhetorical action uses texts and small assignments that teach students initial practices to guide them towards acquiring a critical digital literacy of surveillance, privacy, and health information. Theories of gender, sexuality and race are integrated to further student literacy of technologies. Through analysis, students learn to read data rhetorically where wearables and their technical documents serve as source texts in the course.

2. **Critique:** The second rhetorical action of students’ critical digital education involves critiquing the ideological systems and discourses that shape the design of technological interfaces. Students engage critically—skeptically—with the composition of wearables through a series of assignments that ask them to consider how data gathered from their bodies and other users’ bodies implicates them within a biocapitalist economy.

3. **Response:** The last rhetorical action of the class focuses on service learning as an embodied rhetorical practice. Students partner with a university organization on a specific project in the development of technical documents or deliverables that educate others about privacy issues that are relevant to the entire university community. The instructor serves in a kind of managerial role in the facilitation of this project while students work in groups to propose, develop, and present their groups’ portion of the project through a series of project proposals and revision stages.

These three rhetorical actions support a feminist approach to a rhetoric and composition curriculum that can be adapted within professional writing courses. Drawing on Jacqueline Jones Royster and Gesa E. Kirsch’s (2012) feminist rhetorical practices, we critically reimagine the scenes and texts for rhetorical inquiry to include wearables. Royster and Kirsch felt compelled “to reconfigure the nature and scope of rhetorical enterprises, to decenter [their] biases, and to broaden [their] sense of accountability by connecting local and global analyses” (p. 78). To do that work, they propose critical imagination as a rhetorical practice that reorients researchers to consider looking at people, research sites, texts, and genres that have been, up until now, historically underrepresented in scholarship.

Given our concern to enact a pedagogy supportive of feminist intervention, we critically reimagine the foci of professional writing courses to incorporate the frequent use of wearables as a needed topic of rhetorical inquiry in the classroom. We thus build our learning goals to support this reimagination, arguing that students will:

- acquire a critical digital literacy of surveillance and privacy, especially in regard to health and technology;
- learn to engage in feminist rhetorical intervention of privacy health concerns;
- understand that feminist intervention requires an ethical stance that situates user advocacy and agency as central outcomes;
- practice and refine professional writing skills in a real-world setting;
- negotiate rhetorical and discursive expectations with a university partner through a service learning project.

4. **Two Courses Engaging in A Feminist Surveillance as Care Pedagogy**

In this section, we present two professional writing courses as examples of how our feminist surveillance as care pedagogy has developed in light of our growing concern regarding privacy and wearable health applications. Both courses we present here incorporate readings and assignments that encourage the acquisition of critical digital literacies in regard to their particular course foci. Les’s class focused on Internet safety and Maria’s focused on digital health safety. By adding service learning as another facet to these courses, each provided students with the additional outcome of learning how to use rhetorical action in the service of advocacy and activism.

We feel it important to add that both of these courses were taught at different institutions with different identities of professional writing. Les’s course was taught within an R1 and well-known professional writing major, where pushing the boundaries of “what is professionalism” and incorporating more critical, theoretical and cultural approaches to professional writing are encouraged (if not expected). Maria, while trained as a graduate student in the institution where Les was teaching, developed a course for a new liberal arts institution and within an English Department where professional writing is becoming embraced yet whose identity is not well-established nor necessarily understood by faculty or students. We disclose this information as it informs the context and implications of such a course. Mainly, that the course we envision is relevant and applicable across professional writing programs, given our two course’s shared emphasis on the rhetorical foundations that inform student understanding of data, privacy and surveillance as it shifts across digital infrastructures (in Les’ case the internet and in Maria’s digital health technologies, like wearables).
Because our surveillance as care pedagogy requires analysis, critique, and response, students are positioned to extend this work into local public contexts that thus speak into and on behalf of the university. Les details how the initial application of this pedagogy developed from a theoretical inquiry she began in her doctoral coursework and exams. Maria explains how, through conversation with Les about her course design, she adapted Les’s theoretical model into a pedagogy that teaches digital health literacy applied to wearables. Both provide overviews of their course and description of the scaffolding of readings and assignments in separate graphs. We provide these courses as examples of how to incorporate our feminist pedagogical model into a multitude of rhetoric and composition courses.

4.1. Les’ Course: A Critical Digital Literacy of Surveillance and Privacy in a Technical Writing Class

In the spring semester of 2017, Les was assigned to teach WRA 320: Technical Writing at Michigan State University (MSU). This was her second time teaching the course after teaching it online as a six-week summer class the year before. One of her dissertation committee advisors and the Director of Undergraduate Programs in her department, Stuart Blythe, assigned her this course as a way to put into practice my theoretical research that incorporated surveillance and privacy into a professional writing curriculum.

Prior to the semester beginning, she and Blythe worked together in the forming of a partnership between her Technical Writing course and MSU’s Residential Education and Housing Services (REHS) program. The purpose of the partnership was to create a “Safer Internet Use” guide for REHS’s 2017–2018 Safety and Awareness campaign that sought to reach all the students living on campus. During initial meetings with REHS representatives, they decided on five areas of focus for the guide: general online safety, identifying what is real vs. fake online (fake news, phishing, email scams, etc), online safety for four social media platforms (Facebook, Snapchat, Twitter, and Linkedin), simple ways for students to protect themselves, and safer online professional development. The hope was that by the end of the semester, students would have worked together to create the guide in the form of print and digital content that REHS could then use to promote to students throughout the entirety of the next academic year.

Les includes the chart below to show how her course design incorporated the three rhetorical actions this pedagogy offers. The purpose of her class was to develop students’ critical digital literacies of surveillance and privacy, so readings were scaffolded in such a way to build upon technical writing practices and critical theories of technology before having students assess technological systems. Les’s goal was to first give them the critical language and analytical means (rhetoric) that would enable engaged, material responses to Internet safety implications. Most readings and small assignments took place during the first half of the semester. During midterms week, students submitted their groups’ proposals to REHS and spent the remainder of the class designing their portion of the course’s Internet Safety Guide. Considering that this course was designed prior to her and Maria’s theorizing of the feminist surveillance as care pedagogy, Les’s chart lists critique, analysis, and response across different weeks and, often, in tandem with one another. Her chart shows how her students enacted the three rhetorical actions throughout the duration of the course as they acquired the kind of critical digital literacy required of them to complete the service-learning project.

4.2. Maria’s Course: Digital Rhetoric in Health & Medicine

As Les and Maria continued to discuss the mobile application GLOW, Les shared with Maria how she had structured her professional writing course to address issues of privacy, surveillance, and safety. At this time, Maria discovered that she was assigned to teach Digital Rhetoric as new faculty. Interested in connecting her research in RHM to professional writing curriculum, Maria used Les’s class as inspiration in her design of consulted with Les digital rhetorics class with a more explicit RHM focus. Maria titled this course “Digital Rhetoric in Health and Medicine,” which situated wearables and their health applications as texts bridging critical digital literacies of surveillance and privacy and critical health literacies.

This course focused upon two guiding questions: (1) what is digital rhetoric? and (2) why does digital rhetoric matter to health and medicine? The chart (below) details how Maria designed the course around her and Les’s then evolving feminist surveillance as care framework. Students were assigned modules asking them to practice analysis, critique, and formulate a collaborative response as a process to develop critical digital health literacies. Maria scaffolded her course to first engage in definitions, theories and methods of digital rhetoric and later made the transition to incorporate digital concerns related to health and medicine, focusing on wearables as a text for inquiry. This move was imperative as she learned that none of her students had taken a rhetoric course in the past. As English majors, they had practice engaging
in “close readings” of literary texts. As such, Maria spent many of the first few weeks in the course defining *rhetoric*: its application to digital technologies and infrastructures, and gaining comfortability in doing rhetorical analysis of digital texts. This was an unpredictable moment of this course and underlines an unforeseen takeaway of this pedagogical model. Mainly, that at the foundation of this pedagogy are rhetorical theories and practices that allow students to connect moments of praxis to their everyday interactions with digital technologies, and, in the case of Maria’s digital health technology and wearable apps.

5. Reflective Takeaways from a Feminist Surveillance as Care Pedagogy

Since a necessary part of this pedagogy emphasizes reflection, Les and Maria each reflect below on key moments in their courses where they witnessed students acquiring critical digital literacies.

5.1. Les’s Reflection

At the start of week six of Les’s WRA 320 course, she asked her students during group discussion if they found themselves more concerned with issues of privacy and online safety now that the class had been underway. Only one student had raised their hand when she asked on the first day of class, and Les was curious if that number had changed any since then. About half of the class raised their hand the second time. Some spoke about being completely invested in the topic; others mentioned being more cautious with the information they post, but remained skeptical. Les reiterated the spiel that she had given them on the first day when she had explained that her purpose was not to convert them to become privacy fanatics, but that they had been enlisted to educate a large group of people who may or may not have reasons to need a greater awareness of Internet safety practices.

Les, then, shifted the conversation to a group activity that began by pulling familytreenow.com up on the viewscreen in class. She proceeded to look up her father in the search bar and explained how a simple search of his name and date-of-birth quickly led her to a full profile on him that detailed all of his previous residences, his family contacts (aside from her because she had deleted her own profile weeks earlier), his phone number, and known acquaintances however quaint. Les explained to the class that they would probably have a profile with the same information posted publicly and asked them to search. Her suspicion was correct: most of them did. The ones who did not seemed pleased, so Les urged them to look up their parents and grandparents. After that, her students realized that everyone in the class had someone they knew closely listed on this website.

They spent the rest of the class deleting their family members’ profiles, writing emails to the website to express their concern with the kind of information it made public, and they discussed the possible privacy and security issues that arise from the personal information freely given on this site. The greatest concern Les’s students had is still a salient one: what if they were to get into a disagreement with someone online, say politically, and they were to find out where we lived and also had information on all of their family members? How might that put them and their families in danger?

All of Les’s students remarked in their end-of-semester evaluations that this was the turning moment in their awareness and investment in online privacy and security. Every single one.

5.2. Maria’s Reflection

Teaching for the first time at a new institution with a population of students who were English majors and confessed to having never studied digital rhetoric, nor rhetoric in general, Maria admits that when the course began she feared the scope was a bit ambitious. Students did, indeed, express confusion and feelings of being overwhelmed. Many of these feelings centered around a lack of exposure to what is meant by “rhetoric”.

Yet, as the semester continued on and trust was established, a similar finding noted in Les’ reflection emerged in my class; students in both classes found personal stake in the topics presented. They began to connect the theories to real-world practices. For example, when students were assigned the Digital Rhetoric Analysis Project, many came into the class ecstatic to share their findings. While this project asked them to investigate their own presence on FamilyTreeNow.com and TruthFinder.com, they were also expected to work with family and friends to investigate how their personal data was shared and circulated on the web. What was most shocking to my students was the general apathy their peers had to the presence of personal online data. students noted in the presentation of their findings
that when they offered to act as digital rhetoric advocates, helping them opt out of the collection of data, most of their peers simply said “why bother, it will all be leaked anyways.” This differed greatly when working with with their parents or grandparents, many of whom were appalled at how their personal data was available for general access.

Maria shares a summary of this conversation as it continued to reappear in her course, especially as students began their collaborative projects with the Women’s Center and the Student Health Center. As students worked to create digital deliverables for these campus centers, they discussed how to engage their intended audience: students themselves. How do we make issues of online privacy and digital tracking apparent and matter to their peers? User-testing, or the bringing in of their peer’s bodies, allowed for greater, embodied response and revision to the deliverables that were created. Such an outcome was not predicted prior to designing this course. Yet, it stresses how the teaching of surveillance as it relates to the risk posed in the collection of bodily data must be constructed through embodied experiences.

5.3. Wearable Health Privacy Literacy Starts from Embodied Experience

We share these reflections as they highlight digital privacy as an affective, embodied, and material experience. Such experiences necessitate rhetorical practices. As Opel and Rhodes (2018) profess, “A key part of our approach is the foregrounding of rhetoric as an embodied, relational, and ethical negotiation of semiotic systems, a negotiation that forms the very bones of any textual interaction” (forthcoming). Les learned in this pedagogical moment that to teach a critical digital literacy of privacy and surveillance required students to feel how their privacy became implicated in a specific technological system (much in the way that Erin Schaefer, in this issue, describes a person’s immersive experience when emotionally attached to a certain narrative). We reflect upon what this experience teaches both of us, and we realized that wearables function as the kind of rhetorical text that—by design—forces the body into a technological infrastructure. The body becomes data. As such, issues of surveillance, privacy, health, and safety immediately arise. Wearables are the apparatus that perform this body as data-text mutation.

Beck’s (2015) concept of the invisible digital identity further supports wearables mutating the body as data-text by explaining:

   - code spreads and interacts with other code thereby suggesting an object-to-object relationship independent of human interaction. This also leads us to question how algorithms and tracking technologies output data that plot decisions upon virtual and physical bodies. The pulse of online engagement influences user interaction in virtual environments—shaped by the very code nabbing bits of user data for a fluid web experience. (p. 127)

Beck’s scholarship reinforces the need for frameworks to examine wearables in the context of human interaction, always implicating the body in rhetorical inquiry. Further, our anecdotal experiences with our classes serve as added evidence for a pedagogical model that purposefully scaffolds assignments and readings connecting the body to digital technologies. To teach critical digital literacies requires the critical inquiry between user/body and technology.

We see then a need for teaching critical digital literacies prior when analyzing wearables as texts for rhetorical inquiry. In 2008, Stephanie Vie argued that “students possess technological know-how and access to computers but lack critical technological literacy skills” (p. 10). She proposed the teaching of critical technological literacies in composition courses to help students identify issues of intellectual property and privacy on their own. Looking back at this text as a foundational source of scholarship on surveillance and privacy, Vie’s argument still demands attention. Giving critical digital literacies the emphasis in our courses provides students with the means to interrogate and use technologies in safer, more critical ways while also understanding how these technologies implicate and affect their lives. However, acquiring this literacy also provides them with the opportunity to engage others—especially when such composition courses adapt a service learning project as part of the course’s curriculum. Students, then, are trained as digitally literate advocates who serve on behalf of a given community.

Adding wearables as the focus of analysis connects literacy, privacy, and health together. Wearables shift the scenes of analysis from the hospital and doctor’s offices to data collection, online health management systems, and everyday applications. Critical digital literacies of surveillance and privacy fuse with critical health literacies. What is at stake in acquiring this fused literacy is an understanding of how our private health information becomes transferrable data that moves invisibly from the wearable interface worn on the body through technological infrastructures and onto the screens of unidentified third party affiliations. Wearables, then, are not read as some technological “fad,” but serve to broaden understanding about our bodily data’s tangible, material connection with current and future privacy
consequences. Our task as teacher-scholars in rhetoric and composition must be to not only teach how to rhetorically analyze and critique such affective technological consequences but prepare students to respond as user-advocates who practice a critical digital literacy of health technologies.

6. Conclusion: Care and Advocacy as Critical Digital Health Literacy Outcomes

We take a turn, now, to re-emphasize what we mean by surveillance as care and situate care as a practice that allows for students to take on roles as advocates for health and data privacy within professional writing courses. Our definition of care comes from feminist education philosopher Nel Noddings. Theorizing care as a practice most teachers aim to engage in, Nel Noddings (2005) troubles the notion of practicing care, stating “even for the majority [of teachers] who do care, in the virtue sense – that is, they profess to care and work hard at their teaching – there are many who do not adopt the relational sense of caring” (p. 1). Rather, a more responsible and affective model of care for teachers enacts a sense of relationality in which “caring forces us [the teacher] to look at the relation” (p. 1). This suggestion reorients the concept of care from a hierarchical position in which teacher cares for student, and instead, creates a sense of reciprocity where teacher and student care for each other. We expand upon Noddings’ definition of care to suggest that this model of reciprocal care can also support a sense of student civic advocacy, especially in courses that have service learning components. Here, students who are engaged in practices of care in the classroom make the shift to care for others outside of the classroom.

Care as more than a concept, but as praxis, enhances students’ acquiring of critical digital literacies taught in these courses because learning moments occur when students feel their privacy implicated without their consent. An awareness of surveillance often stems from one’s body feeling vulnerable and/or at risk. As Les’s anecdote qualifies, a material and embodied understanding of the affects of data collection shows students how important and relevant privacy is in regard to their safety. Realizing this, Maria’s course waited to incorporate critical health literacy themes until after Module 2, when students assessed how their privacy information is at risk. Tending to moments of risk reinforces attention to vulnerability. To then be advocates for more critical approaches to wearables, first, students must feel how their bodies are implicated in digital spaces. They must understand surveillance’s affects before they can understand the effects of data collection.

Once they understand their own affective relationship with technologies as embodied data-texts, then surveillance becomes a digital literacy they can engage with critically. Dubrofsky and Magnet argue that education and research around surveillance “open[s] up avenues for the examination of mediascapes that increasingly blur the lines between what have conventionally been understood as public and private spheres, and the concomitant implications of the use by private citizens of personal technologies to create publicly available and widely circulating images and bits of data” (p. 16). We strongly believe in the importance of addressing surveillance implications in professional writing courses through service learning projects for how the deliverables made in these assignments facilitate a response to how invisible the blurred lines between private and public have become. Wearables work as an ideal source text to make clear these blurred lines.

Through teaching care as a needed perspective on surveillance, wearables are situated not just as a text of inquiry, but in a public context as a mechanism that affects how health technologies write themselves onto our bodies, as well. We want wearables to be self-empowering; therefore, we use care as a model for students to think about how wearables can help us show care for our bodies and one another’s bodies. In Les’s class, care came in the form of creating a guide for all MSU students to acquire critical digital knowledge about safer Internet use. Maria’s course modeled care when students acted as carers for the greater community teaching to their peers surveillance as care through a series of co-created deliverables, including digital health safety workshops and web content. A course that focuses primarily on wearables would, in effect, adopt both Les’s and Maria’s pedagogical emphases on care. The deliverables would prioritize care as a response that informs university stakeholders about privacy health concerns.

Since wearable technologies draw data from the body without oversight of protective health legislation (i.e. HIPAA), we feel compelled to not just educate our students about concerns that certainly affect them, but to provide them the means of educating others in the act of service learning. Our service learning projects enable students to act as advocates for the health of the university community by engaging in care as a practice. We teach a feminist surveillance as care pedagogy to our students and our students take the critical digital literacies they learn and reciprocally teach them to others. In their essay “Decolonization as Care,” anthropologist Uzma Z. Rizvi (2016) mentions that “Our ability to understand ourselves in relation to everything else is predicated upon the ability to understand and contextualize the
real, tangible, sensory aspect of moving through the world as compared to conceptual, abstract notions of thinking of our bodies in the world” (SavageMinds, n.p.). Like the editors note in the special introduction, we, too, “see a growing need for focus on embodiment and embodied cognition” (p. 9). Our hope is that this article, along with our supplemental teaching documents, assist others in designing similar courses that interrogate that everyday risks and realities posed by interacting with wearables.

Further, the future of this work we believe requires applying a critical cultural approach to how such data implicates particular bodies and their cultural histories. In citing Scott, Longo, and Wills (2007), Angela Haas (2012) points out that “The intellectual work of these scholars makes evident that cultural studies approaches to technical communication research, practice, and pedagogy can guide and support us in creating more culturally responsive and responsible texts that accommodate their users” (p. 280–1). Approaching surveillance through the practice of care as pedagogical design starts from a place of culturally responsive accommodation where our bodies are not only addressed as sites of study, but active in the composing of texts that materially implicate our lives. When teacher-scholars teach a feminist surveillance as care pedagogy, care about health and data privacy becomes a reciprocal, relational, and culturally responsive outcome. Wearables are, then, the site for feminist action. We see this pedagogy preparing students, who are users of wearables, with the resources for better determining how their technologies implicate and affect their lives, inciting a consensual and supportive relationship with wearable technologies.

Les Hutchinson is a PhD candidate in the Writing, Rhetoric, and American Cultures department at Michigan State University. Her research brings together cultural and digital rhetorics, particularly at the intersection of intellectual property and surveillance. She has published scholarship on doxing, anonymity, whistleblowing, and student authorship. Her dissertation, Privacy, property, and sovereignty, looks at how Chicanx and Indigenous women use social media platforms as forms of resistance and cultural expression despite how those platforms appropriate the data collected from them. She can easily be reached on Twitter (@techairos) where she curates a frequent presence and enjoys a good gif/meme.

Maria Novotny is an assistant professor of English at the University of Wisconsin Oshkosh where she teaches a variety of professional and digital writing courses. Her research engages in community advocacy by facilitating a variety of public pedagogy projects focused on reproduction. She is committed to working in communities with student advocates to develop greater critical awareness on intersectional issues of reproductive rights, digital privacy, user consent in health devices and their applications. She has been published in Communication Design Quarterly, Peitho, and Enculturation.

References


Vie, Stephanie. (2014). You are how you play: Privacy policies and data mining in social networking games. In Jennifer deWinter, & Ryan Moeller (Eds.), *Computer games and technical communication: Critical methods and applications at the intersection* (pp. 171–187). Ashgate.


It was a hot August afternoon in 1946. Lou Boudreau, the player-manager of the Cleveland Indians, was having a miserable day. In the first game of a doubleheader, Ted Williams had almost single-handedly annihilated his team. Williams, perhaps the game's greatest hitter at the time, had smashed three home runs and driven home eight. The Indians ended up losing 11 to 10.

Boudreau had to take action. So when Williams came up for the first time in the second game, players on the Indians' side started moving around. Boudreau, the shortstop, jogged over to where the second baseman would usually stand, and the second baseman backed into short right field. The third baseman moved
to his left, into the shortstop’s hole. It was clear that Boudreau, perhaps out of desperation, was shifting the entire orientation of his defense in an attempt to turn Ted Williams’s hits into outs.

In other words, he was thinking like a data scientist. He had analyzed crude data, most of it observational: Ted Williams usually hit the ball to right field. Then he adjusted. And it worked. Fielders caught more of Williams’s blistering line drives than before (though they could do nothing about the home runs sailing over their heads).

If you go to a major league baseball game today, you’ll see that defenses now treat nearly every player like Ted Williams. While Boudreau merely observed where Williams usually hit the ball, managers now know precisely where every player has hit every ball over the last week, over the last month, throughout his career, against left-handers, when he has two strikes, and so on. Using this historical data, they analyze their current situation and calculate the positioning that is associated with the highest probability of success. And that sometimes involves moving players far across the field.

Shifting defenses is only one piece of a much larger question: What steps can baseball teams take to maximize the probability that they’ll win? In their hunt for answers, baseball statisticians have scrutinized every variable they can quantify and attached it to a value. How much more is a double worth than a single? When, if ever, is it worth it to bunt a runner from first to second base?

The answers to all of these questions are blended and combined into mathematical models of their sport. These are parallel universes of the baseball world, each a complex tapestry of probabilities. They include every measurable relationship among every one of the sport’s components, from walks to home runs to the players themselves. The purpose of the model is to run different
scenarios at every juncture, looking for the optimal combinations. If the Yankees bring in a right-handed pitcher to face Angels slugger Mike Trout, as compared to leaving in the current pitcher, how much more likely are they to get him out? And how will that affect their overall odds of winning?

Baseball is an ideal home for predictive mathematical modeling. As Michael Lewis wrote in his 2003 bestseller, *Moneyball*, the sport has attracted data nerds throughout its history. In decades past, fans would pore over the stats on the back of baseball cards, analyzing Carl Yastrzemski’s home run patterns or comparing Roger Clemens’s and Dwight Gooden’s strikeout totals. But starting in the 1980s, serious statisticians started to investigate what these figures, along with an avalanche of new ones, really meant: how they translated into wins, and how executives could maximize success with a minimum of dollars.

“Moneyball” is now shorthand for any statistical approach in domains long ruled by the gut. But baseball represents a healthy case study—and it serves as a useful contrast to the toxic models, or WMDs, that are popping up in so many areas of our lives. Baseball models are fair, in part, because they’re transparent. Everyone has access to the stats and can understand more or less how they’re interpreted. Yes, one team’s model might give more value to home run hitters, while another might discount them a bit, because sluggers tend to strike out a lot. But in either case, the numbers of home runs and strikeouts are there for everyone to see.

Baseball also has statistical rigor. Its gurus have an immense data set at hand, almost all of it directly related to the performance of players in the game. Moreover, their data is highly relevant to the outcomes they are trying to predict. This may sound obvious, but as we’ll see throughout this book, the folks building WMDs routinely lack data for the behaviors they’re most interested in. So they substitute stand-in data, or proxies. They draw statistical
correlations between a person's zip code or language patterns and her potential to pay back a loan or handle a job. These correlations are discriminatory, and some of them are illegal. Baseball models, for the most part, don't use proxies because they use pertinent inputs like balls, strikes, and hits.

Most crucially, that data is constantly pouring in, with new statistics from an average of twelve or thirteen games arriving daily from April to October. Statisticians can compare the results of these games to the predictions of their models, and they can see where they were wrong. Maybe they predicted that a left-handed reliever would give up lots of hits to right-handed batters—and yet he mowed them down. If so, the stats team has to tweak their model and also carry out research on why they got it wrong. Did the pitcher's new screwball affect his statistics? Does he pitch better at night? Whatever they learn, they can feed back into the model, refining it. That's how trustworthy models operate. They maintain a constant back-and-forth with whatever in the world they're trying to understand or predict. Conditions change, and so must the model.

Now, you may look at the baseball model, with its thousands of changing variables, and wonder how we could even be comparing it to the model used to evaluate teachers in Washington, D.C., schools. In one of them, an entire sport is modeled in fastidious detail and updated continuously. The other, while cloaked in mystery, appears to lean heavily on a handful of test results from one year to the next. Is that really a model?

The answer is yes. A model, after all, is nothing more than an abstract representation of some process, be it a baseball game, an oil company's supply chain, a foreign government's actions, or a movie theater's attendance. Whether it's running in a computer program or in our head, the model takes what we know and uses it to predict responses in various situations. All of us carry thousands
of models in our heads. They tell us what to expect, and they
guide our decisions.

Here's an informal model I use every day. As a mother of three,
I cook the meals at home—my husband, bless his heart, cannot
remember to put salt in pasta water. Each night when I begin
to cook a family meal, I internally and intuitively model every-
one's appetite. I know that one of my sons loves chicken (but hates
hamburgers), while another will eat only the pasta (with extra
grated parmesan cheese). But I also have to take into account that
people's appetites vary from day to day, so a change can catch
my model by surprise. There's some unavoidable uncertainty
involved.

The input to my internal cooking model is the information I
have about my family, the ingredients I have on hand or I know
are available, and my own energy, time, and ambition. The out-
put is how and what I decide to cook. I evaluate the success of a
meal by how satisfied my family seems at the end of it, how much
they've eaten, and how healthy the food was. Seeing how well it
is received and how much of it is enjoyed allows me to update
my model for the next time I cook. The updates and adjustments
make it what statisticians call a “dynamic model.”

Over the years I've gotten pretty good at making meals for my
family, I'm proud to say. But what if my husband and I go away for
a week, and I want to explain my system to my mom so she can fill
in for me? Or what if my friend who has kids wants to know my
methods? That's when I'd start to formalize my model, making it
much more systematic and, in some sense, mathematical. And if
I were feeling ambitious, I might put it into a computer program.

Ideally, the program would include all of the available food
options, their nutritional value and cost, and a complete data-
base of my family's tastes: each individual's preferences and aver-
sions. It would be hard, though, to sit down and summon all that
information off the top of my head. I've got loads of memories of people grabbing seconds of asparagus or avoiding the string beans. But they're all mixed up and hard to formalize in a comprehensive list.

The better solution would be to train the model over time, entering data every day on what I'd bought and cooked and noting the responses of each family member. I would also include parameters, or constraints. I might limit the fruits and vegetables to what's in season and dole out a certain amount of Pop-Tarts, but only enough to forestall an open rebellion. I also would add a number of rules. This one likes meat, this one likes bread and pasta, this one drinks lots of milk and insists on spreading Nutella on everything in sight.

If I made this work a major priority, over many months I might come up with a very good model. I would have turned the food management I keep in my head, my informal internal model, into a formal external one. In creating my model, I'd be extending my power and influence in the world. I'd be building an automated me that others can implement, even when I'm not around.

There would always be mistakes, however, because models are, by their very nature, simplifications. No model can include all of the real world's complexity or the nuance of human communication. Inevitably, some important information gets left out. I might have neglected to inform my model that junk-food rules are relaxed on birthdays, or that raw carrots are more popular than the cooked variety.

To create a model, then, we make choices about what's important enough to include, simplifying the world into a toy version that can be easily understood and from which we can infer important facts and actions. We expect it to handle only one job and accept that it will occasionally act like a clueless machine, one with enormous blind spots.
Sometimes these blind spots don’t matter. When we ask Google Maps for directions, it models the world as a series of roads, tunnels, and bridges. It ignores the buildings, because they aren’t relevant to the task. When avionics software guides an airplane, it models the wind, the speed of the plane, and the landing strip below, but not the streets, tunnels, buildings, and people.

A model’s blind spots reflect the judgments and priorities of its creators. While the choices in Google Maps and avionics software appear cut and dried, others are far more problematic. The value-added model in Washington, D.C., schools, to return to that example, evaluates teachers largely on the basis of students’ test scores, while ignoring how much the teachers engage the students, work on specific skills, deal with classroom management, or help students with personal and family problems. It’s overly simple, sacrificing accuracy and insight for efficiency. Yet from the administrators’ perspective it provides an effective tool to ferret out hundreds of apparently underperforming teachers, even at the risk of misreading some of them.

Here we see that models, despite their reputation for impartiality, reflect goals and ideology. When I removed the possibility of eating Pop-Tarts at every meal, I was imposing my ideology on the meals model. It’s something we do without a second thought. Our own values and desires influence our choices, from the data we choose to collect to the questions we ask. Models are opinions embedded in mathematics.

Whether or not a model works is also a matter of opinion. After all, a key component of every model, whether formal or informal, is its definition of success. This is an important point that we’ll return to as we explore the dark world of WMDs. In each case, we must ask not only who designed the model but also what that person or company is trying to accomplish. If the North Korean government built a model for my family’s meals, for example, it
might be optimized to keep us above the threshold of starvation at the lowest cost, based on the food stock available. Preferences would count for little or nothing. By contrast, if my kids were creating the model, success might feature ice cream at every meal. My own model attempts to blend a bit of the North Koreans’ resource management with the happiness of my kids, along with my own priorities of health, convenience, diversity of experience, and sustainability. As a result, it’s much more complex. But it still reflects my own personal reality. And a model built for today will work a bit worse tomorrow. It will grow stale if it’s not constantly updated. Prices change, as do people’s preferences. A model built for a six-year-old won’t work for a teenager.

This is true of internal models as well. You can often see troubles when grandparents visit a grandchild they haven’t seen for a while. On their previous visit, they gathered data on what the child knows, what makes her laugh, and what TV show she likes and (unconsciously) created a model for relating to this particular four-year-old. Upon meeting her a year later, they can suffer a few awkward hours because their models are out of date. Thomas the Tank Engine, it turns out, is no longer cool. It takes some time to gather new data about the child and adjust their models.

This is not to say that good models cannot be primitive. Some very effective ones hinge on a single variable. The most common model for detecting fires in a home or office weighs only one strongly correlated variable, the presence of smoke. That’s usually enough. But modelers run into problems—or subject us to problems—when they focus models as simple as a smoke alarm on their fellow humans.

Racism, at the individual level, can be seen as a predictive model whirring away in billions of human minds around the world. It is built from faulty, incomplete, or generalized data. Whether it comes from experience or hearsay, the data indicates
that certain types of people have behaved badly. That generates a binary prediction that all people of that race will behave that same way.

Needless to say, racists don’t spend a lot of time hunting down reliable data to train their twisted models. And once their model morphs into a belief, it becomes hardwired. It generates poisonous assumptions, yet rarely tests them, settling instead for data that seems to confirm and fortify them. Consequently, racism is the most slovenly of predictive models. It is powered by haphazard data gathering and spurious correlations, reinforced by institutional inequities, and polluted by confirmation bias. In this way, oddly enough, racism operates like many of the WMDs I’ll be describing in this book.

In 1997, a convicted murderer, an African American man named Duane Buck, stood before a jury in Harris County, Texas. Buck had killed two people, and the jury had to decide whether he would be sentenced to death or to life in prison with the chance of parole. The prosecutor pushed for the death penalty, arguing that if Buck were let free he might kill again.

Buck’s defense attorney brought forth an expert witness, a psychologist named Walter Quijano, who didn’t help his client’s case one bit. Quijano, who had studied recidivism rates in the Texas prison system, made a reference to Buck’s race, and during cross-examination the prosecutor jumped on it.

“You have determined that the . . . the race factor, black, increases the future dangerousness for various complicated reasons. Is that correct?” the prosecutor asked.

“Yes,” Quijano answered. The prosecutor stressed that testimony in her summation, and the jury sentenced Buck to death.

Three years later, Texas attorney general John Cornyn found
that the psychologist had given similar race-based testimony in six other capital cases, most of them while he worked for the prosecution. Cornyn, who would be elected in 2002 to the US Senate, ordered new race-blind hearings for the seven inmates. In a press release, he declared: "It is inappropriate to allow race to be considered as a factor in our criminal justice system. . . . The people of Texas want and deserve a system that affords the same fairness to everyone."

Six of the prisoners got new hearings but were again sentenced to death. Quijano's prejudicial testimony, the court ruled, had not been decisive. Buck never got a new hearing, perhaps because it was his own witness who had brought up race. He is still on death row.

Regardless of whether the issue of race comes up explicitly at trial, it has long been a major factor in sentencing. A University of Maryland study showed that in Harris County, which includes Houston, prosecutors were three times more likely to seek the death penalty for African Americans, and four times more likely for Hispanics, than for whites convicted of the same charges. That pattern isn't unique to Texas. According to the American Civil Liberties Union, sentences imposed on black men in the federal system are nearly 20 percent longer than those for whites convicted of similar crimes. And though they make up only 13 percent of the population, blacks fill up 40 percent of America's prison cells.

So you might think that computerized risk models fed by data would reduce the role of prejudice in sentencing and contribute to more even-handed treatment. With that hope, courts in twenty-four states have turned to so-called recidivism models. These help judges assess the danger posed by each convict. And by many measures they're an improvement. They keep sentences more consistent and less likely to be swayed by the moods and bi-
ases of judges. They also save money by nudging down the length of the average sentence. (It costs an average of $31,000 a year to house an inmate, and double that in expensive states like Connecticut and New York.)

The question, however, is whether we’ve eliminated human bias or simply camouflaged it with technology. The new recidivism models are complicated and mathematical. But embedded within these models are a host of assumptions, some of them prejudicial. And while Walter Quijano’s words were transcribed for the record, which could later be read and challenged in court, the workings of a recidivism model are tucked away in algorithms, intelligible only to a tiny elite.

One of the more popular models, known as LSI–R, or Level of Service Inventory–Revised, includes a lengthy questionnaire for the prisoner to fill out. One of the questions—“How many prior convictions have you had?”—is highly relevant to the risk of recidivism. Others are also clearly related: “What part did others play in the offense? What part did drugs and alcohol play?”

But as the questions continue, delving deeper into the person’s life, it’s easy to imagine how inmates from a privileged background would answer one way and those from tough inner-city streets another. Ask a criminal who grew up in comfortable suburbs about “the first time you were ever involved with the police,” and he might not have a single incident to report other than the one that brought him to prison. Young black males, by contrast, are likely to have been stopped by police dozens of times, even when they’ve done nothing wrong. A 2013 study by the New York Civil Liberties Union found that while black and Latino males between the ages of fourteen and twenty-four made up only 4.7 percent of the city’s population, they accounted for 40.6 percent of the stop-and-frisk checks by police. More than 90 percent of those stopped were innocent. Some of the others might have been drinking underage
or carrying a joint. And unlike most rich kids, they got in trouble for it. So if early “involvement” with the police signals recidivism, poor people and racial minorities look far riskier.

The questions hardly stop there. Prisoners are also asked about whether their friends and relatives have criminal records. Again, ask that question to a convicted criminal raised in a middle-class neighborhood, and the chances are much greater that the answer will be no. The questionnaire does avoid asking about race, which is illegal. But with the wealth of detail each prisoner provides, that single illegal question is almost superfluous.

The LSI–R questionnaire has been given to thousands of inmates since its invention in 1995. Statisticians have used those results to devise a system in which answers highly correlated to recidivism weigh more heavily and count for more points. After answering the questionnaire, convicts are categorized as high, medium, and low risk on the basis of the number of points they accumulate. In some states, such as Rhode Island, these tests are used only to target those with high-risk scores for antirecidivism programs while incarcerated. But in others, including Idaho and Colorado, judges use the scores to guide their sentencing.

This is unjust. The questionnaire includes circumstances of a criminal’s birth and upbringing, including his or her family, neighborhood, and friends. These details should not be relevant to a criminal case or to the sentencing. Indeed, if a prosecutor attempted to tar a defendant by mentioning his brother's criminal record or the high crime rate in his neighborhood, a decent defense attorney would roar, “Objection, Your Honor!” And a serious judge would sustain it. This is the basis of our legal system. We are judged by what we do, not by who we are. And although we don’t know the exact weights that are attached to these parts of the test, any weight above zero is unreasonable.

Many would point out that statistical systems like the LSI–R
are effective in gauging recidivism risk—or at least more accurate than a judge’s random guess. But even if we put aside, ever so briefly, the crucial issue of fairness, we find ourselves descending into a pernicious WMD feedback loop. A person who scores as “high risk” is likely to be unemployed and to come from a neighborhood where many of his friends and family have had run-ins with the law. Thanks in part to the resulting high score on the evaluation, he gets a longer sentence, locking him away for more years in a prison where he’s surrounded by fellow criminals—which raises the likelihood that he’ll return to prison. He is finally released into the same poor neighborhood, this time with a criminal record, which makes it that much harder to find a job. If he commits another crime, the recidivism model can claim another success. But in fact the model itself contributes to a toxic cycle and helps to sustain it. That’s a signature quality of a WMD.

... 

In this chapter, we’ve looked at three kinds of models. The baseball models, for the most part, are healthy. They are transparent and continuously updated, with both the assumptions and the conclusions clear for all to see. The models feed on statistics from the game in question, not from proxies. And the people being modeled understand the process and share the model’s objective: winning the World Series. (Which isn’t to say that many players, come contract time, won’t quibble with a model’s valuations: “Sure I struck out two hundred times, but look at my home runs . . .”)

From my vantage point, there’s certainly nothing wrong with the second model we discussed, the hypothetical family meal model. If my kids were to question the assumptions that underlie it, whether economic or dietary, I’d be all too happy to provide them. And even though they sometimes grouse when facing
something green, they'd likely admit, if pressed, that they share the goals of convenience, economy, health, and good taste—
though they might give them different weights in their own mod-
els. (And they'll be free to create them when they start buying
their own food.)

I should add that my model is highly unlikely to scale. I don't see Walmart or the US Agriculture Department or any other
titan embracing my app and imposing it on hundreds of millions
of people, like some of the WMDs we'll be discussing. No, my
model is benign, especially since it's unlikely ever to leave my
head and be formalized into code.

The recidivism example at the end of the chapter, however, is a
different story entirely. It gives off a familiar and noxious odor. So
let's do a quick exercise in WMD taxonomy and see where it fits.

The first question: Even if the participant is aware of being
modeled, or what the model is used for, is the model opaque, or
even invisible? Well, most of the prisoners filling out mandatory
questionnaires aren't stupid. They at least have reason to suspect
that information they provide will be used against them to control
them while in prison and perhaps lock them up for longer. They
know the game. But prison officials know it, too. And they keep
quiet about the purpose of the LSI–R questionnaire. Otherwise,
they know, many prisoners will attempt to game it, providing an-
wers to make them look like model citizens the day they leave the
joint. So the prisoners are kept in the dark as much as possible and
do not learn their risk scores.

In this, they're hardly alone. Opaque and invisible models are
the rule, and clear ones very much the exception. We're modeled
as shoppers and couch potatoes, as patients and loan applicants,
and very little of this do we see—even in applications we happily
sign up for. Even when such models behave themselves, opacity
can lead to a feeling of unfairness. If you were told by an usher,
upon entering an open-air concert, that you couldn’t sit in the first ten rows of seats, you might find it unreasonable. But if it were explained to you that the first ten rows were being reserved for people in wheelchairs, then it might well make a difference. Transparency matters.

And yet many companies go out of their way to hide the results of their models or even their existence. One common justification is that the algorithm constitutes a “secret sauce” crucial to their business. It’s intellectual property, and it must be defended, if need be, with legions of lawyers and lobbyists. In the case of web giants like Google, Amazon, and Facebook, these precisely tailored algorithms alone are worth hundreds of billions of dollars. WMDs are, by design, inscrutable black boxes. That makes it extra hard to definitively answer the second question: Does the model work against the subject’s interest? In short, is it unfair? Does it damage or destroy lives?

Here, the LSI–R again easily qualifies as a WMD. The people putting it together in the 1990s no doubt saw it as a tool to bring evenhandedness and efficiency to the criminal justice system. It could also help nonthreatening criminals land lighter sentences. This would translate into more years of freedom for them and enormous savings for American taxpayers, who are footing a $70 billion annual prison bill. However, because the questionnaire judges the prisoner by details that would not be admissible in court, it is unfair. While many may benefit from it, it leads to suffering for others.

A key component of this suffering is the pernicious feedback loop. As we’ve seen, sentencing models that profile a person by his or her circumstances help to create the environment that justifies their assumptions. This destructive loop goes round and round, and in the process the model becomes more and more unfair.

The third question is whether a model has the capacity to grow
exponentially. As a statistician would put it, can it scale? This might sound like the nerdy quibble of a mathematician. But scale is what turns WMDs from local nuisances into tsunami forces, ones that define and delimit our lives. As we’ll see, the developing WMDs in human resources, health, and banking, just to name a few, are quickly establishing broad norms that exert upon us something very close to the power of law. If a bank’s model of a high-risk borrower, for example, is applied to you, the world will treat you as just that, a deadbeat—even if you’re horribly misunderstood. And when that model scales, as the credit model has, it affects your whole life—whether you can get an apartment or a job or a car to get from one to the other.

When it comes to scaling, the potential for recidivism modeling continues to grow. It’s already used in the majority of states, and the LSI–R is the most common tool, used in at least twenty-four of them. Beyond LSI–R, prisons host a lively and crowded market for data scientists. The penal system is teeming with data, especially since convicts enjoy even fewer privacy rights than the rest of us. What’s more, the system is so miserable, overcrowded, inefficient, expensive, and inhumane that it’s crying out for improvements. Who wouldn’t want a cheap solution like this?

Penal reform is a rarity in today’s polarized political world, an issue on which liberals and conservatives are finding common ground. In early 2015, the conservative Koch brothers, Charles and David, teamed up with a liberal think tank, the Center for American Progress, to push for prison reform and drive down the incarcerated population. But my suspicion is this: their bipartisan effort to reform prisons, along with legions of others, is almost certain to lead to the efficiency and perceived fairness of a data-fed solution. That’s the age we live in. Even if other tools supplant LSI–R as its leading WMD, the prison system is likely to be a powerful incubator for WMDs on a grand scale.
So to sum up, these are the three elements of a WMD: Opacity, Scale, and Damage. All of them will be present, to one degree or another, in the examples we’ll be covering. Yes, there will be room for quibbles. You could argue, for example, that the recidivism scores are not totally opaque, since they spit out scores that prisoners, in some cases, can see. Yet they’re brimming with mystery, since the prisoners cannot see how their answers produce their score. The scoring algorithm is hidden. A couple of the other WMDs might not seem to satisfy the prerequisite for scale. They’re not huge, at least not yet. But they represent dangerous species that are primed to grow, perhaps exponentially. So I count them. And finally, you might note that not all of these WMDs are universally damaging. After all, they send some people to Harvard, line others up for cheap loans or good jobs, and reduce jail sentences for certain lucky felons. But the point is not whether some people benefit. It’s that so many suffer. These models, powered by algorithms, slam doors in the face of millions of people, often for the flimsiest of reasons, and offer no appeal. They’re unfair.

And here’s one more thing about algorithms: they can leap from one field to the next, and they often do. Research in epidemiology can hold insights for box office predictions; spam filters are being retooled to identify the AIDS virus. This is true of WMDs as well. So if mathematical models in prisons appear to succeed at their job—which really boils down to efficient management of people—they could spread into the rest of the economy along with the other WMDs, leaving us as collateral damage.

That’s my point. This menace is rising. And the world of finance provides a cautionary tale.
WEAPONS OF MATH DESTRUCTION

HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY

CATHY O’NEIL

CROWN NEW YORK
“A Society, Searching,” pp. 35-63

Excerpt from *Algorithms of Oppression* by Safiya Umoja Noble
just over $203 billion. At the time of the hearings, Google’s latest income statement, for December 2011, showed gross profit at $24.7 billion. It had $43.3 billion cash on hand and just $6.21 billion in debt. Google held 66.2% of the search engine market industry in 2012. Google Search’s profits have only continued to grow, and its holdings have become so significant that the larger company has renamed itself Alphabet, with Google Search as but one of many holdings. By the final writing of this book in August 2017, Alphabet was trading at $936.38 on NASDAQ, with a market capitalization of $649.49 billion.

The public is aware of the role of search in everyday life, and people’s opinions on search are alarming. Recent data from tracking surveys and consumer-behavior trends by the comScore Media Metrix consumer panel conducted by the Pew Internet and American Life Project show that search engines are as important to Internet users as email is. Over sixty million Americans engage in search, and for the most part, people report that they are satisfied with the results they find in search engines. The 2005 and 2012 Pew reports on “search engine use” reveal that 73% of all Americans have used a search engine, and 59% report using a search engine every day. In 2012, 83% of search engine users used Google. But Google Search prioritizes its own interests, and this is something far less visible to the public. Most people surveyed could not tell the difference between paid advertising and “genuine” results.

If search is so trusted, then why is a study such as this one needed? The exploration beyond that first simple search is the substance of this book. Throughout the discussion of these and other results, I want to emphasize the main point: there is a missing social context in commercial digital media platforms, and it matters, particularly for marginalized groups that are problematically represented in stereotypical or pornographic ways, for those who are bullied, and for those who are consistently targeted. I use only a handful of illustrative searches to underscore the point and to raise awareness—and hopefully intervention—of how important what we find on the web through commercial search engines is to society.

Search Results as Power

Search results reflect the values and norms of the search company’s commercial partners and advertisers and often reflect our lowest and
most demeaning beliefs, because these ideas circulate so freely and so often that they are normalized and extremely profitable. Search results are more than simply what is popular. The dominant notion of search results as being both “objective” and “popular” makes it seem as if misogynist or racist search results are a simple mirror of the collective. Not only do problematic search results seem “normal,” but they seem completely unavoidable as well, even though these ideas have been thoroughly debunked by scholars. Unfortunately, users of Google give consent to the algorithms’ results through their continued use of the product, which is largely unavoidable as schools, universities, and libraries integrate Google products into our educational experiences.  

Google’s monopoly status, coupled with its algorithmic practices of biasing information toward the interests of the neoliberal capital and social elites in the United States, has resulted in a provision of information that purports to be credible but is actually a reflection of advertising interests. Stated another way, it can be argued that Google functions in the interests of its most influential paid advertisers or through an intersection of popular and commercial interests. Yet Google’s users think of it as a public resource, generally free from commercial interest. Further complicating the ability to contextualize Google’s results is the power of its social hegemony. Google benefits directly and materially from what can be called the “labortainment” of users, when users consent to freely give away their labor and personal data for the use of Google and its products, resulting in incredible profit for the company.

There are many cases that could be made to show how overreliance on commercial search by the public, including librarians, information professionals, and knowledge managers—all of whom are susceptible to overuse of or even replacement by search engines—is something that we must pay closer attention to right now. Under the current algorithmic constraints or limitations, commercial search does not provide appropriate social, historical, and contextual meaning to already overracialized and hypersexualized people who materially suffer along multiple axes. In the research presented in this study, the reader will find a more meaningful understanding of the kind of harm that such limitations can cause for users reliant on the web as an artifact of both formal and informal culture. In sum, search results play a powerful role in providing fact and authority to those who see them, and as such, they must
be examined carefully. Google has become a central object of study for digital media scholars, due to recognition on these scholars’ parts of the power and impact wielded by the necessity to begin most engagements with social media via a search process and the near universality with which Google has been adopted and embedded into all aspects of the digital media landscape to respond to that need. This work is addressing a gap in scholarship on how search works and what it biases, public trust in search, the relationship of search to information studies, and the ways in which African Americans, among others, are mediated and commodified in Google.

To start revealing some of the processes involved, it is important to think about how results appear. Although one might believe that a query to a search engine will produce the most relevant and therefore useful information, it is actually predicated on a matrix of ways in which pages are hyperlinked and indexed on the web. Rendering web content (pages) findable via search engines is an expressly social, economic, and human project, which several scholars have detailed. These renderings are delivered to users through a set of steps (algorithms) implemented by programming code and then naturalized as “objective.” One of the reasons this is seen as a neutral process is because algorithmic, scientific, and mathematical solutions are evaluated through procedural and mechanistic practices, which in this case includes tracing hyperlinks among pages. This process is defined by Google’s founders, Sergey Brin and Larry Page, as “voting,” which is the term they use to describe how search results move up or down in a ranked list of websites. For the most part, many of these processes have been automated, or they happen through graphical user interfaces (GUIs) that allow people who are not programmers (i.e., not working at the level of code) to engage in sharing links to and from websites.

Research shows that users typically use very few search terms when seeking information in a search engine and rarely use advanced search queries, as most queries are different from traditional offline information-seeking behavior. This front-end behavior of users appears to be simplistic; however, the information retrieval systems are complex, and the formulation of users’ queries involves cognitive and emotional processes that are not necessarily reflected in the system design. In essence, while users use the simplest queries they can in a
search box because of the way interfaces are designed, this does not always reflect how search terms are mapped against more complex thought patterns and concepts that users have about a topic. This disjunction between, on the one hand, users’ queries and their real questions and, on the other, information retrieval systems makes understanding the complex linkages between the content of the results that appear in a search and their import as expressions of power and social relations of critical importance.

The public generally trusts information found in search engines. Yet much of the content surfaced in a web search in a commercial search engine is linked to paid advertising, which in part helps drive it to the top of the page rank, and searchers are not typically clear about the distinctions between “real” information and advertising. Given that advertising is a fundamental part of commercial search, using content analysis to make sense of what actually is served up in search is appropriate and consistent with the articulation of feminist critiques of the images of women in print advertising.34 These scholars have shown the problematic ways that women have been represented—as sex objects, incompetent, dependent on men, or underrepresented in the workforce35—and the content and representation of women and girls in search engines is consistent with the kinds of problematic and biased ideas that live in other advertising channels. Of course, this makes sense, because Google Search is in fact an advertising platform, not intended to solely serve as a public information resource in the way that, say, a library might. Google creates advertising algorithms, not information algorithms.

To understand search in the context of this book, it is important to look at the description of the development of Google outlined by the former Stanford computer science graduate students and cofounders of the company, Sergey Brin and Larry Page, in “The Anatomy of a Large-Scale Hypertextual Web Search Engine.” Their paper, written in graduate school, serves as the architectural framework for Google’s PageRank. In addition, it is crucial to also look at the way that citation analysis, the foundational notion behind Brin and Page’s idea, works as a bibliometric project that has been extensively developed by library and information science scholars. Both of these dynamics are often misunderstood because they do not account for the complexities of human intervention involved in vetting of information, nor do they pay attention
to the relative weight or importance of certain types of information. For example, in the process of citing work in a publication, all citations are given equal weight in the bibliography, although their relative importance to the development of thought may not be equal at all. Additionally, no relative weight is given to whether a reference is validated, rejected, employed, or engaged—complicating the ability to know what a citation actually means in a document. Authors who have become so mainstream as not to be cited, such as not attributing modern discussions of class or power dynamics to Karl Marx or the notion of “the individual” to the scholar of the Italian Renaissance Jacob Burckhardt, mean that these intellectual contributions may undergird the framework of an argument but move through works without being cited any longer. Concepts that may be widely understood and accepted ways of knowing are rarely cited in mainstream scholarship, an important dynamic that...
Linda Smith, former president of the Association for Information Science and Technology (ASIS&T) and associate dean of the Information School at the University of Illinois at Urbana-Champaign, argues is part of the flawed system of citation analysis that deserves greater attention if bibliometrics are to serve as a legitimating force for valuing knowledge production.

Brin and Page saw the value in using works that others cite as a model for thinking about determining what is legitimate on the web, or at least to indicate what is popular based on many people acknowledging particular types of content. In terms of outright co-optation of the citation, vis-à-vis the hyperlink, Brin and Page were aware of some of the challenges I have described. They were clearly aware from the beginning of the potential for “gaming” the system by advertising companies or commercial interests, a legitimated process now known as “search engine optimization,” to drive ads or sites to the top of a results list for a query, since clicks on web links can be profitable, as are purchases gained by being vetted as “the best” by virtue of placement on the first page of PageRank. This is a process used for web results, not paid advertising, which is often highlighted in yellow (see figure 1.6). Results that appear not to be advertising are in fact influenced by the advertising algorithm. In contrast to scientific or scholarly citations, which once in print are persistent and static, hyperlinking is a dynamic process that can change from moment to moment. As a result, the stability of results in Google ranking shifts and is prone to being affected by a number of processes that I will cover, primarily search engine optimization and advertising. This means that results shift over time. The results of what is most hyperlinked using Google’s algorithm today will be different at a later date or from the time that Google’s web-indexing crawlers move through the web until the next cycle.

Citation importance is a foundational concept for determining scholarly relevance in certain disciplines, and citation analysis has largely been considered a mechanism for determining whether a given article or scholarly work is important to the scholarly community. I want to revisit this concept because it also has implications for thinking about the legitimation of information, not just citability or popularity. It is also a function of human beings who are engaged in a curation practice, not entirely left to automation. Simply put, if scholars choose to
cite a study or document, they have signaled its relevance; thus, human beings (scholars) are involved in making decisions about a document's relevance, although all citations in a bibliography do not share the same level of meaningfulness. Building on this concept of credibility through citation, PageRank is what Brin and Page call the greater likelihood that a document is relevant "if there are many pages that point to it" versus "the probability that the random surfer visits a page." In their research, which led to the development of Google Search, Brin and Page discuss the possibility of monopolizing and manipulating keywords through commercialization of the web search process. Their information-retrieval goal was to deliver the most relevant or very best ten or so documents out of the possible number of documents that could be returned from the web. The resulting development of their search architecture is PageRank—a system that is based on "the objective measure of its citation importance that corresponds well with people's subjective idea of importance."40

One of the most profound parts of Brin and Page's work is in appendix A, in which they acknowledge the ways that commercial interests can compromise the quality of search result retrieval. They state, citing Ben Bagdikian, "It is clear that a search engine which was taking money for showing cellular phone ads would have difficulty justifying the page that our system returned to its paying advertisers. For this type of reason and historical experience with other media, we expect that advertising funded search engines will be inherently biased towards the advertisers and away from the needs of the consumers."41 Brin and Page outline a clear roadmap for how bias would work in advertising-oriented search and the effects this would have, and they directly suggest that it is in the consumer's interest not to have search compromised by advertising and commercialism. To some degree, PageRank was intended to be a measure of relevance based on popularity—including what both web surfers and web designers link to from their sites. As with academic citations, Brin and Page decided that citation analysis could be used as a model for determining whether web links could be ranked according to their importance by measuring how much they were back-linked or hyperlinked to or from. Thus, the model for web indexing pages was born. However, in the case of citation analysis, a scholarly author goes through several stages of vetting and credibility testing, such as the peer-review process,
before work can be published and cited. In the case of the web, such credibility checking is not a factor in determining what will be hyperlinked. This was made explicitly clear in the many news reports covering the 2016 U.S. presidential election, where clickbait and manufactured “news” from all over the world clouded accurate reporting of facts on the presidential candidates.

Another example of the shortcomings of removing this human curation or decision making from the first page of results at the top of PageRank, in addition to the results that I found for “black girls,” can be found in the more public dispute over the results that were returned on searches for the word “Jew,” which included a significant number of anti-Semitic pages. As can be seen by Google’s response to the results of a keyword search for “Jew,” Google takes little responsibility toward the ways that it provides information on racial and gendered identities, which are curated in more meaningful ways in scholarly databases. Siva Vaidhyanathan’s 2011 book The Googlization of Everything (And Why We Should Worry) chronicles recent attempts by the Jewish community and Anti-Defamation League to challenge Google’s priority ranking to the first page of anti-Semitic, Holocaust-denial websites. So troublesome were these search results that in 2011, Google issued a statement about its search process, encouraging people to use “Jews” and “Jewish people” in their searches, rather than the seemingly pejorative term “Jew”—claiming that the company can do nothing about the word’s co-optation by White supremacist groups (see figure 1.12).

Google, according to its own disclaimer, will only remove pages that are considered unlawful, as is the case in France and Germany, where selling or distributing neo-Nazi materials is prohibited. Without such limits on derogatory, racist, sexist, or homophobic materials, Google allows its algorithm—which is, as we can see, laden with what Diaz calls “sociopolitics”—to stand without debate while protesting its inability to remove pages. As recently as June 27, 2012, Google settled a claim by the French antiracism organization the International League Against Racism over Google’s use of ethnic identity—“Jew”—in association with popular searches. Under French law, racial identity markers cannot be stored in databases, and the auto-complete techniques used in the Google search box link names of people to the word “Jew” on the basis of past user searches. What this recent case points to is another effort to
An explanation of our search results

If you recently used Google to search for the word “Jew,” you may have seen results that were very disturbing. We assure you that the views expressed by the sites in your results are not in any way endorsed by Google. We’d like to explain why you’re seeing these results when you conduct this search.

A site’s ranking in Google’s search results relies heavily on computer algorithms using thousands of factors to calculate a page’s relevance to a given query. Sometimes subtleties of language cause anomalies to appear that cannot be predicted. A search for “Jew” brings up one such unexpected result.

If you use Google to search for “Judaism,” “Jewish” or “Jewish people,” the results are informative and relevant. So why is a search for “Jew” different? One reason is that the word “Jew” is often used in an anti-Semitic context. Jewish organizations are more likely to use the word “Jewish” when talking about members of their faith. The word has become somewhat charged linguistically, as noted on websites devoted to Jewish topics such as these:


Someone searching for information on Jewish people would be more likely to enter terms like “Judaism,” “Jewish people,” or “Jews” than the single word “Jew.” In fact, prior to this incident, the word “Jew” only appeared about once in every 10 million search queries. Now it’s likely that the great majority of searches on Google for “Jew” are by people who have heard about this issue and want to see the results for themselves.

The beliefs and preferences of those who work at Google, as well as the opinions of the general public, do not determine or impact our search results. Individual citizens and public interest groups do periodically urge us to remove particular links or otherwise adjust search results. Although Google reserves the right to address such requests individually, Google views the comprehensiveness of our search results as an extremely important priority. Accordingly, we do not remove a page from our search results simply because its content is unpopular or because we receive complaints concerning it. We will, however, remove pages from our results if we believe the page (or its site) violates our Webmaster Guidelines, if we believe we are required to do so by law, or at the request of the webmaster who is responsible for the page.

We apologize for the upsetting nature of the experience you had using Google and appreciate your taking the time to inform us about it.

Sincerely,
The Google Team

P.S. You may be interested in some additional information the Anti-Defamation League has posted about this issue at http://www.sdli.org/humors/google_search_rumors.asp. In addition, we call your attention to Google’s search results on this topic.

Google

Figure 1.12. Explanation of results by Google. Source: www.google.com/explanation.html (originally available in 2005).
redefine distorted images of people in new media. These cases of distortion, however, continue to accumulate.

The public's as well as the Jewish community's interest in accurate information about Jewish culture and the Holocaust should be enough motivation to provoke a national discussion about consumer harm, to which my research shows we can add other cultural and gender-based identities that are misrepresented in search engines. However, Google's assertion that its search results, though problematic, were computer generated (and thus not the company's fault) was apparently a good-enough answer for the Anti-Defamation League (ADL), which declared, "We are extremely pleased that Google has heard our concerns and those of its users about the offensive nature of some search results and the unusually high ranking of peddlers of bigotry and anti-Semitism." The ADL does acknowledge on its website its gratitude to Sergey Brin, cofounder of Google and son of Russian Jewish immigrants, for his personal letter to the organization and his mea culpa for the "Jew" search-term debacle. The ADL generously stated in its press release about the incident that Google, as a resource to the public, should be forgiven because "until the technical modifications are implemented, Google has placed text on its site that gives users a clear explanation of how search results are obtained. Google searches are automatically determined using computer algorithms that take into account thousands of factors to calculate a page's relevance."44

If there is a technical fix, then what are the constraints that Google is facing such that eight years later, the issue has yet to be resolved? A search for the word "Jew" in 2012 produces a beige box at the bottom of the results page from Google linking to its lengthy disclaimer about the results—which remain a mix of both anti-Semitic and informative sites (see figure 1.13). That Google places the responsibility for bad results back on the shoulders of information searchers is a problem, since most of the results that the public gets on broad or open-ended racial and gendered searches are out of their control and entirely within the control of Google Search.

It is important to note that Google has conceded the fact that anti-Semitism as the primary information result about Jewish people is a problem, despite its disclaimer that tries to put the onus for bad results on the searcher. In Germany and France, for example, it is illegal to sell
Nazi memorabilia, and Google has had to put in place filters that ensure online retailers of such are not visible in search results. In 2002, Benjamin Edelman and Jonathan Zittrain at Harvard University’s Berkman Center for Internet and Society concluded that Google was filtering its search results in accordance with local law and precluding neo-Nazi organizations and content from being displayed.45 While this indicates that Google can in fact remove objectionable hits, it is equally troubling, because the company provided search results without informing searchers that information was being deleted. That is to say that the results were presented as factual and complete without mention of omission. Yahoo!, another leading U.S. search engine, was forced into a protracted legal battle in France for allowing pro-Nazi memorabilia to be sold through its search engine, in violation of French law. What these cases point to is that search results are deeply contextual and easily manipulated, rather than objective, consistent, and transparent, and that they can be legitimated only in social, political, and historical context.
The issue of unlawfulness over the harm caused by derogatory results is a question of considerable debate. For example, in the United States, where free speech protections are afforded to all kinds of speech, including hate speech and racist or sexist depictions of people and communities, there is a higher standard of proof required to show harm toward disenfranchised or oppressed people. We need legal protections now more than ever, as automated decision-making systems wield greater power in society.

Gaming the System: Optimizing and Co-opting Results in Search Engines

Google's advertising tool or optimization product is AdWords. AdWords allows anyone to advertise on Google's search pages and is highly customizable. With this tool, an advertiser can set a maximum amount of money that it wants to spend on a daily basis for advertising. The model for AdWords is that Google will display ads on search pages that it believes are relevant to the kind of search query that is taking place by a user. If a user clicks on an ad, then the advertiser pays. And Google incentivizes advertisers by suggesting that their ads will show up in searches and display, but the advertiser (or Google customer) pays for the ad only when a user (Google consumer) clicks on the advertisement, which is the cost per click (CPC). The advertiser selects a series of "keywords" that it believes closely align with its product or service that it is advertising, and a customer can use a Keyword Estimator tool in order to see how much the keywords they choose to associate with their site might cost. This advertising mechanism is an essential part of how PageRank prioritizes ads on a page, and the association of certain keywords with particular industries, products, and services derives from this process, which works in tandem with PageRank.

In order to make sense of the specific results in keyword searches, it is important to know how Google's PageRank works, what commercial processes are involved in PageRank, how search engine optimization (SEO) companies have been developed to influence the process of moving up results, and how Google bombing occurs on occasion. Google bombing is the practice of excessively hyperlinking to a website (repeatedly coding HTML to link a page to a term or phrase) to cause it to
rise to the top of PageRank, but it is also seen as a type of “hit and run” activity that can deliberately co-opt terms and identities on the web for political, ideological, and satirical purposes. Judit Bar-Ilan, a professor of information science at Bar-Ilan University, has studied this practice to see if the effect of forcing results to the top of PageRank has a lasting effect on the result’s persistence, which can happen in well-orchestrated campaigns. In essence, Google bombing is the process of co-opting content or a term and redirecting it to unrelated content. Internet lore attributes the creation of the term “Google bombing” to Adam Mathes, who associated the term “talentless hack” with a friend’s website in 2001. Practices such as Google bombing (also known as Google washing) are impacting both SEO companies and Google alike. While Google is invested in maintaining the quality of search results in PageRank and policing companies that attempt to “game the system,” as Brin and Page foreshadowed, SEO companies do not want to lose ground in pushing their clients or their brands up in PageRank.48 SEO is the process of “using a range of techniques, including augmenting HTML code, web page copy editing, site navigation, linking campaigns and more, in order to improve how well a site or page gets listed in search engines for particular search topics;”49 in contrast to “paid search,” in which the company pays Google for its ads to be displayed when specific terms are searched. A media spectacle of this nature is the case of Senator Rick Santorum, Republican of Pennsylvania, whose website and name were associated with insults in order to drive objectionable content to the top of PageRank.50 Others who have experienced this kind of co-optation of identity or less-than-desirable association of their name with an insult include former president George W. Bush and the pop singer Justin Bieber.

All of these practices of search engine optimization and Google bombing can take place independently of and in concert with the process of crawling and indexing the web. In fact, being found gives meaning to a website and creates the conditions in which a ranking can happen. Search engine optimization is a major factor in findability on the web. What is important to note is that search engine optimization is a multibillion-dollar industry that impacts the value of specific keywords; that is, marketers are invested in using particular keywords, and keyword combinations, to optimize their rankings.
Figure 1.14. Example of a Google bomb on George W. Bush and the search terms "miserable failure," 2005.

Despite the widespread beliefs in the Internet as a democratic space where people have the power to dynamically participate as equals, the Internet is in fact organized to the benefit of powerful elites, including corporations that can afford to purchase and redirect searches to their own sites. What is most popular on the Internet is not wholly a matter of what users click on and how websites are hyperlinked—there are a variety of processes at play. Max Holloway of Search Engine Watch notes, "Similarly, with Google, when you click on a result—or, for that matter, don't click on a result—that behavior impacts future results. One consequence of this complexity is difficulty in explaining system behavior. We primarily rely on performance metrics to quantify the success or failure of retrieval results, or to tell us which variations of a system work better than others. Such metrics allow the system to be continuously improved upon." The goal of combining search terms, then, in the context of the landscape of the search engine optimization logic, is only the beginning.
Much research has now been done to dispel the notion that users of the Internet have the ability to "vote" with their clicks and express interest in individual content and information, resulting in democratic practices online.\textsuperscript{53} Research shows the ways that political news and information in the blogosphere are mediated and directed such that major news outlets surface to the top of the information pile over less well-known websites and alternative news sites in the blogosphere, to the benefit of elites.\textsuperscript{54} In the case of political information seeking, research has shown how Google directs web traffic to mainstream corporate news conglomerates, which increases their ability to shape the political discourse. Google too is a mediating platform that, at least at one moment in time, in September 2011, allowed the porn industry to take precedence in the representations of Black women and girls over other possibilities among at least eleven and a half billion documents that could have been indexed.\textsuperscript{55} That moment in 2011 is, however, emblematic of Google's ongoing dynamic. It has since produced many more problematic results.

As the Federal Communications Commission declares broadband "the new common medium,"\textsuperscript{56} the role of search engines is taking on even greater importance to "the widest possible dissemination of information from diverse and antagonistic sources... essential to the welfare of the public."\textsuperscript{57} This political economy of search engines and traditional advertisers includes search engine optimization companies that operate in a secondary or gray market (often in opposition to Google). Ultimately, the results we get are about the financial interest that Google or SEOs have in helping their own clients optimize their rankings. In fact, Google is in the business of selling optimization. Extensive critiques of Google have been written on the political economy of search\textsuperscript{58} and the way that consolidations in the search engine industry market contribute to the erosion of public resources, in much the way that the media scholars Robert McChesney, former host of nationally syndicated radio show \textit{Media Matters}, and John Nichols, a writer for the \textit{Nation}, critique the consolidation of the mass-media news markets. Others have spoken to the inherent democratizing effect of search engines, such that search is adding to the diversity of political organization and discourse because the public is able to access more information in the marketplace of ideas.\textsuperscript{59} Mounting evidence shows that automated decision-making systems are disproportionately harmful to the most vulnerable and the
least powerful, who have little ability to intervene in them—from mis-
representation to prison sentencing to accessing credit and other life-
impacting formulas.

This landscape of search engines is important to consider in under-
standing the meaning of search for the public, and it serves as a basis for
examining why information quality online is significant. We must trouble
the notion of Google as a public resource, particularly as institutions be-
come more reliant on Google when looking for high-quality, contextu-
alized, and credible information. This shift from public institutions such
as libraries and schools as brokers of information to the private sector, in
projects such as Google Books, for example, is placing previously public
assets in the hands of a multinational corporation for private exploita-
tion. Information is a new commodity, and search engines can function
as private information enclosures.60 We need to make more visible the
commercial interests that overdetermine what we can find online.

The Enclosure of the Public Domain through Search Engines

At the same time that search engines have become the dominant portal for
information seeking by U.S. Internet users, the rise of commercial medias-
tion of information in those same search engines is further enclosing the
public domain. Decreases in funding for public information institutions
such as libraries and educational institutions and shifts of responsibil-
ity to individuals and the private sector have reframed the ways that the
public conceives of what can and should be in the public domain. Yet
Google Search is conceived of as a public resource, even though it is a
multinational advertising company. These shifts of resources that were
once considered public have been impacted by increased intellectual
property rights, licensing, and publishing agreements for companies and
private individuals in the domain of copyrights, patents, and other legal
protections. The move of community-based assets and culture to pri-
vate hands is arguably a crisis that has rolled back the common good,
but there are still possible strategies that can be explored for maintain-
ing what can remain in the public domain. Commercial control over the
Internet, often considered a “commons,” has moved it further away from
the public through a series of national and international regulations and
intellectual and commercial borders that exist in the management of the
network.\textsuperscript{61} Beyond the Internet and the control of the network, public information—whether delivered over the web or not—continues to be outsourced to the private sphere, eroding the public information commons that has been a basic tenet of U.S. democracy.

The critical media scholar Herbert Schiller, whose work foreshadowed many of the current challenges in the information and communications landscape, provides a detailed examination of the impact of outsourcing and deregulation in the spheres of communication and public information. His words are still timely: “The practice of selling government (or any) information serves the corporate user well. Ordinarily individual users go to the end of the dissemination queue. Profoundly antidemocratic in its effect, privatizing and/or selling information, which at one time was considered public property, has become a standard practice in recent years.”\textsuperscript{62} What this critique shows is that the privatization and commercial nature of information has become so normalized that it not only becomes obscured from view but, as a result, is increasingly difficult to critique within the public domain. The Pew Internet and American Life Project corroborates that the public trusts multinational corporations that provide information over the Internet and that there is a low degree of distrust of the privatization of information.\textsuperscript{63} Part of this process of acquiescence to the increased corporatization of public life can be explained by the economic landscape, which is shaped by military-industrial projects such as the Internet that have emerged in the United States,\textsuperscript{64} increasing the challenge of scholars who are researching the impact of such shifts in resources and accountability. Molly Niesen at the University of Illinois has written extensively on the loss of public accountability by federal agencies such as the Federal Trade Commission (FTC), which is a major contribution to our understanding of where the public can focus attention on policy interventions.\textsuperscript{65} We should leverage her research to think about the FTC as the key agency to manage and intervene in how corporations control the information landscape.

\textit{The Cultural Power of Algorithms}

The public is minimally aware of these shifts in the cultural power and import of algorithms. In a 2015 study by the Pew Research Center,
"American’s Privacy Strategies Post-Snowden," only 34% of respondents who were aware of the surveillance that happens automatically online through media platforms, such as search behavior, email use, and social media, reported that they were shifting their online behavior because of concerns of government surveillance and the potential implications or harm that could come to them. Little of the American public knows that online behavior has more importance than ever. Indeed, Internet-based activities are dramatically affecting our notions of how democracy and freedom work, particularly in the realm of the free flow of information and communication. Our ability to engage with the information landscape subtly and pervasively impacts our understanding of the world and each other.

An example of how information flow and bias in the realm of politics have recently come to the fore can be found in an important new study about how information bias can radically alter election outcomes. The former editor of Psychology Today and professor Robert Epstein and Ronald Robertson, the associate director of the American Institute for Behavioral Research and Technology, found in their 2013 study that democracy was at risk because manipulating search rankings could shift voters’ preferences, substantially and without their awareness. In their study, they note that the tenor of stories about a candidate in search engine results, whether favorable or unfavorable, dramatically af-
fected the way that people voted. Seventy-five percent of participants were not aware that the search results had been manipulated. The researchers concluded, “The outcomes of real elections—especially tight races—can conceivably be determined by the strategic manipulation of search engine rankings and . . . that the manipulation can be accomplished without people being aware of it. We speculate that unregulated search engines could pose a serious threat to the democratic system of government.”

In March 2012, the Pew Internet and American Life Project issued an update to its 2005 “Search Engine Users” study. The 2005 and 2012 surveys tracking consumer-behavior trends from the comScore Media Metrix consumer panel show that search engines are as important to Internet users as email is. In fact, the Search Engine Use 2012 report suggests that the public is “more satisfied than ever with the quality of search results.” Further findings include the following:

- 73% of all Americans have used a search engine, and 59% report using a search engine every day.
- 83% of search engine users use Google.

Especially alarming is the way that search engines are increasingly positioned as a trusted public resource returning reliable and credible information. According to Pew, users report generally good outcomes and relatively high confidence in the capabilities of search engines:

- 73% of search engine users say that most or all the information they find as they use search engines is accurate and trustworthy.

Yet, at the same time that search engine users report high degrees of confidence in their skills and trust in the information they retrieve from engines, they have also reported that they are naïve about how search engines work:

- 62% of search engine users are not aware of the difference between paid and unpaid results; that is, only 38% are aware, and only 8% of search engine users say that they can always tell which results are paid or sponsored and which are not.
In 2005, 70% of search engine users were fine with the concept of paid or sponsored results, but in 2012, users reported that they are not okay with targeted advertising because they do not like having their online behavior tracked and analyzed.

- In 2005, 45% of search engine users said they would stop using search engines if they thought the engines were not being clear about offering some results for pay.
- In 2005, 64% of those who used engines at least daily said search engines are a fair and unbiased source of information; the percentage increased to 66% in 2012.

Users in the 2012 Pew study also expressed concern about personalization:

- 73% reported that they would not be okay with a search engine keeping track of searches and using that information to personalize future search results. Participants reported that they feel this to be an invasion of privacy.

In the context of these concerns, a 2011 study by the researchers Martin Feuz and Matthew Fuller from the Centre for Cultural Studies at the University of London and Felix Stalder from the Zurich University of the Arts found that personalization is not simply a service to users but rather a mechanism for better matching consumers with advertisers and that Google’s personalization or aggregation is about actively matching people to groups, that is, categorizing individuals. In many cases, different users are seeing similar content to each other, but users have little ability to see how the platform is attempting to use prior search history and demographic information to shape their results. Personalization is, to some degree, giving people the results they want on the basis of what Google knows about its users, but it is also generating results for viewers to see what Google Search thinks might be good for advertisers by means of compromises to the basic algorithm. This new wave of interactivity, without a doubt, is on the minds of both users and search engine optimizing companies and agencies. Google applications such as Gmail or Google Docs and social media sites such as Facebook track identity and previous searches in order to surface targeted ads for users by analyzing users’ web traces. So not only do search engines increasingly remember the digital traces of where we have been
and what links we have clicked in order to provide more custom content (a practice that has begun to gather more public attention after Google announced it would use past search practices and link them to users in its privacy policy change in 2012), but search results will also vary depending on whether filters to screen out porn are enabled on computers.

It is certain that information that surfaces to the top of the search pile is not exactly the same for every user in every location, and a variety of commercial advertising, political, social, and economic decisions are linked to the way search results are coded and displayed. At the same time, results are generally quite similar, and complete search personalization—customized to very specific identities, wants, and desires—has yet to be developed. For now, this level of personal-identity personalization has less impact on the variation in results than is generally believed by the public.

**Losing Control of Our Images and Ourselves in Search**

It is well known that traditional media have been rife with negative or stereotypical images of African American / Black people, and the web as the locus of new media is a place where traditional media interests are replicated. Those who have been inappropriately and unfairly represented in racist and sexist ways in old media have been able to cogently critique those representations and demand expanded representations, protest stereotypes, and call for greater participation in the production of alternative, nonstereotypical or oppressive representations. This is part of the social charge of civil rights organizations such as the Urban League and the National Association for the Advancement of Colored People, which monitor and report on minority misrepresentations, as well as celebrate positive portrayals of African Americans in the media.

At a policy level, some civil rights organizations and researchers such as Darnell Hunt, dean of the division of social science and department chair of sociology at UCLA, have been concerned with media representations of African Americans, and mainstream organizations such as Free Press have been active in providing resources about the impact of the lack of diversity, stereotyping, and hate speech in the media. Indeed, some of these resources have been directed toward net-neutrality issues
and closing the digital divide. Media advocacy groups that focus on the pornification of women or the stereotyping of people of color might turn their attention toward the Internet as another consolidated media resource, particularly given the evidence showing Google's information and advertising monopoly status on the web.

Bias in Search

“Traffic Report: How Google Is Squeezing Out Competitors and Muscling Into New Markets,” by ConsumerWatchdog.org's Inside Google (June 2010), details how Google effectively blocks sites that it competes with and prioritizes its own properties to the top of the search pile (YouTube over other video sites, Google Maps over MapQuest, and Google Images over Photobucket and Flickr). The report highlights the process by which Universal Search is not a neutral and therefore universal process but rather a commercial one that moves sites that buy paid advertising to the top of the pile. Amid these practices, the media, buttressed by an FTC investigation, have suggested that algorithms are not at all unethical or harmful because they are free services and Google has the right to run its business in any way it sees fit. Arguably, this is true, so true that the public should be thoroughly informed about the ways that Google biases information—toward largely stereotypic and decontextualized results, at least when it comes to certain groups of people. Commercial platforms such as Facebook and YouTube go to great lengths to monitor uploaded user content by hiring web content screeners, who at their own peril screen illicit content that can potentially harm the public. The expectation of such filtering suggests that such sites vet content on the Internet on the basis of some objective criteria that indicate that some content is in fact quite harmful to the public. New research conducted by Sarah T. Roberts in the Department of Information Studies at UCLA shows the ways that, in fact, commercial content moderation (CCM, a term she coined) is a very active part of determining what is allowed to surface on Google, Yahoo!, and other commercial text, video, image, and audio engines. Her work on video content moderation elucidates the ways that commercial digital media platforms currently outsource or insource image and video content filtering to comply with their terms of use.
agreements. What is alarming about Roberts's work is that it reveals the processes by which content is already being screened and assessed according to a continuum of values that largely reflect U.S.-based social norms, and these norms reflect a number of racist and stereotypical ideas that make screening racism and sexism and the abuse of humans in racialized ways "in" and perfectly acceptable, while other ideas such as the abuse of animals (which is also unacceptable) are "out" and screened or blocked from view. She details an interview with one of the commercial content moderators (CCMs) this way:

We have very, very specific itemized internal policies . . . the internal policies are not made public because then it becomes very easy to skirt them to essentially the point of breaking them. So yeah, we had very specific internal policies that we were constantly, we would meet once a week with SecPol to discuss, there was one, blackface is not technically considered hate speech by default. Which always rubbed me the wrong way, so I had probably ten meltdowns about that. When we were having these meetings discussing policy and to be fair to them, they always listened to me, they never shut me up. They didn't agree, and they never changed the policy but they always let me have my say, which was surprising. (Max Breen, MegaTech CCM Worker).

The MegaTech example is an illustration of the fact that social media companies and platforms make active decisions about what kinds of racist, sexist, and hateful imagery and content they will host and to what extent they will host it. These decisions may revolve around issues of "free speech" and "free expression" for the user base, but on commercial social media sites and platforms, these principles are always counterbalanced by a profit motive; if a platform were to become notorious for being too restrictive in the eyes of the majority of its users, it would run the risk of losing participants to offer to its advertisers. So MegaTech erred on the side of allowing more, rather than less, racist content, in spite of the fact that one of its own CCM team members argued vociferously against it and, by his own description, experienced emotional distress ("meltdowns") around it.80
This research by Roberts, particularly in the wake of leaked reports from Facebook workers who perform content moderation, suggests that people and policies are put in place to navigate and moderate content on the web. Egregious and racist content, content that is highly profitable, proliferates because many tech platforms are interested in attracting the interests and attention of the majority in the United States, not of racialized minorities.

Challenging Race- and Gender-Neutral Narratives

These explorations of web results on the first page of a Google search also reveal the default identities that are protected on the Internet or are less susceptible to marginalization, pornification, and commodification. The research of Don Heider, the dean of Loyola University Chicago's School of Communication, and Dustin Harp, an assistant professor in the Department of Communication at the University of Texas, Arlington, shows that even though women constitute just slightly over half of Internet users, women's voices and perspectives are not as loud and do not have as much impact online as those of men. Their work demonstrates how some users of the Internet have more agency and can dominate the web, despite the utopian and optimistic view of the web as a socially equalizing and democratic force. Recent research on the male gaze and pornography on the web argue that the Internet is a communications environment that privileges the male, pornographic gaze and marginalizes women as objects. As with other forms of pornographic representations, pornography both structures and reinforces the domination of women, and the images of women in advertising and art are often "constructed for viewing by a male subject," reminiscent of the journalist and producer John Berger's canonical work Ways of Seeing, which describes this objectification in this way: "Women are depicted in a quite different way from men—not because the feminine is different from the masculine—but because the 'ideal' spectator is always assumed to be male and the image of the woman is designed to flatter him.

The previous articulations of the male gaze continue to apply to other forms of advertising and media—particularly on the Internet—and the pornification of women on the web is an expression of racist and sexist hierarchies. When these images are present, White women are the
norm, and Black women are overrepresented, while Latinas are underrepresented. Tracey A. Gardner characterizes the problematic characterizations of African American women in pornographic media by suggesting that "pornography capitalizes on the underlying historical myths surrounding and oppressing people of color in this country which makes it racist." These characterizations translate from old media representations to new media forms. Structural inequalities of society are being reproduced on the Internet, and the quest for a race-, gender-, and class-less cyberspace could only "perpetuate and reinforce current systems of domination."

More than fifteen years later, the present research corroborates these concerns. Women, particularly of color, are represented in search queries against the backdrop of a White male gaze that functions as the dominant paradigm on the Internet in the United States. The Black studies and critical Whiteness scholar George Lipsitz, of the University of California, Santa Barbara, highlights the "possessive investment in Whiteness" and the ways that the American construction of Whiteness is more "nonracial" or null. Whiteness is more than a legal abstraction formulated to conceptualize and codify notions of the "Negro," "Black Codes," or the racialization of diverse groups of African peoples under the brutality of slavery—it is an imagined and constructed community uniting ethnically diverse European Americans. Through cultural agreements about who subtly and explicitly constitutes "the other" in traditional media and entertainment such as minstrel shows, racist films and television shows produced in Hollywood, and Wild West narratives, Whiteness consolidated itself "through inscribed appeals to the solidarity of White supremacy." The cultural practices of our society—which I argue include representations on the Internet—are part of the ways in which race-neutral narratives have increased investments in Whiteness. Lipsitz argues it this way:

As long as we define social life as the sum total of conscious and deliberate individual activities, then only individual manifestations of personal prejudice and hostility will be seen as racist. Systemic, collective, and coordinated behavior disappears from sight. Collective exercises of group power relentlessly channeling rewards, resources, and opportunities from one group to another will not appear to be "racist" from this perspective.
because they rarely announce their intention to discriminate against individuals. But they work to construct racial identities by giving people of different races vastly different life chances.89

Consistent with trying to make sense of the ways that racial order is built, maintained, and made difficult to parse, Charles Mills, in his canonical work, The Racial Contract, put it this way:

One could say then, as a general rule, that white misunderstanding, misrepresentation, evasion, and self-deception on matters related to race are among the most pervasive mental phenomena of the past few hundred years, a cognitive and moral economy psychically required for conquest, colonization and enslavement. And these phenomena are in no way accidental, but prescribed by the Racial Contract, which requires a certain schedule of structured blindness and opacities in order to establish and maintain the white polity.90

This, then, is a challenge, because in the face of rampant denial in Silicon Valley about the impact of its technologies on racialized people, it becomes difficult to foster an understanding and appropriate intervention into its practices. Group identity as invoked by keyword searches reveals this profound power differential that is reflected in contemporary U.S. social, political, and economic life. It underscores how much engineers have control over the mechanics of sense making on the web about complex phenomena. It begs the question that if the Internet is a tool for progress and advancement, as has been argued by many media scholars, then cui bono—to whose benefit is it, and who holds the power to shape it? Tracing these historical constructions of race and gender offline provides more information about the context in which technological objects such as commercial search engines function as an expression of a series of social, political, and economic relations—relations often obscured and normalized in technological practices, which most of Silicon Valley’s leadership is unwilling to engage with or take up.91

Studying Google keyword searches on identity, and their results, helps further thinking about what this means in relationship to marginalized groups in the United States. I take up the communications
scholar Norman Fairclough’s rationale for doing this kind of critique of the discourses that contribute to the meaning-making process as a form of “critical social science.” To contextualize my method and its appropriateness to my theoretical approach, I note here that scholars who work in critical race theory and Black feminism often use a qualitative method such as close reading, which provides more than numbers to explain results and which focuses instead on the material conditions on which these results are predicated.

Challenging Cybertopias

All of this leads to more discussion about ideologies that serve to stabilize and normalize the notion of commercial search, including the still-popular and ever-persistent dominant narratives about the neutrality and objectivity of the Internet itself—beyond Google and beyond utopian visions of computer software and hardware. The early cyberatarian John Perry Barlow’s infamous “A Declaration of the Independence of Cyberspace” argued in part, “We are creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth. We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity.” Yet the web is not only an intangible space; it is also a physical space made of brick, mortar, metal trailers, electronics containing magnetic and optical media, and fiber infrastructure. It is wholly material in all of its qualities, and our experiences with it are as real as any other aspect of life. Access to it is predicated on telecommunications companies, broadband providers, and Internet service providers (ISPs). Its users live on Earth in myriad human conditions that make them anything but immune from privilege and prejudice, and human participation in the web is mediated by a host of social, political, and economic access points—both locally in the United States and globally.

Since Barlow’s declaration, many scholars have challenged the utopian ideals associated with the rise of the Internet and its ability to free us, such as those espoused by Barlow, linking them to neoliberal notions of individualism, personal freedom, and individual control. These linkages are important markers of the shift from public- or state-sponsored
institutions, including information institutions, as the arbiters of social freedoms to the idea that free markets, corporations, and individualized pursuits should serve as the locus of social organization. These ideas are historically rooted in notions of the universal human being, unmarked by difference, that serve as the framework for a specific tradition of thinking about individual pursuits of equality. Nancy Leys Stepan of Cornell University aptly describes an enduring feature of the past 270 years of liberal individualism, reinvoked by Enlightenment thinkers during the rising period of modern capitalism:

Starting in the seventeenth century, and culminating in the writings of the new social contract philosophers of the eighteenth century, a new concept of the political individual was formulated—an abstract and innovative concept, an apparent oxymoron—the imagined universal individual who was the bearer of equal political rights. The genius of this concept, which opened the door to the modern polis, was that it defined at least theoretically, an individual being who could be imagined so stripped of individual substantiation and specification (his unique self), that he could stand for every man. Unmarked by the myriad specificities (e.g., of wealth, rank, education, age, sex) that make each person unique, one could imagine an abstract, non-specific individual who expressed a common psyche and political humanity.95

Of course, these notions have been consistently challenged, yet they still serve as the basis for beliefs in an ideal of an unmarked humanity—nonracialized, nongendered, and without class distinction—as the final goal of human transcendence. This teleology of the abstracted individual is challenged by the inevitability of such markers and the ways that the individual particularities they signal afford differential realities and struggles, as well as privileges and possibilities. Those who become “marked” by race, gender, or sexuality as other are deviations from the universal human—they are often lauded for “transcending” their markers—while others attempt to “not see color” in a failing quest for colorblindness. The pretext of universal humanity is never challenged, and the default and idealized human condition is unencumbered by racial and gender distinction. This subtext is an important part of the narrative that somehow personal liberties can be realized through
technology because of its ability to supposedly strip us of our specifics and make us equal. We know, of course, that nothing could be further from the truth. Just ask the women of #Gamergate and observe the ways that racist, sexist, and homophobic comments and trolling occur every minute of every hour of every day on the web.

As I have suggested, there are many myths about the Internet, including the notion that what rises to the top of the information pile is strictly what is most popular as indicated by hyperlinking. Were that even true, what is most popular is not necessarily what is most true. It is on this basis that I contend there is work to be done to contextualize and reveal the many ways that Black women are embedded within the most popular commercial search engine—Google Search—and that this embeddedness warrants an exploration into the complexities of whether the content surfaced is a result of popularity, credibility, commerciality, or even a combination thereof. Using the flawed logic of democracy in web rankings, the outcome of the searches I conducted would suggest that both sexism and pornography are the most “popular” values on the Internet when it comes to women, especially women and girls of color. In reality, there is more to result ranking than just how we “vote” with our clicks, and various expressions of sexism and racism are related.
Algorithms of Oppression

How Search Engines Reinforce Racism

Safiya Umoja Noble

NEW YORK UNIVERSITY PRESS
New York
Writing for Algorithmic Audiences

John R. Gallagher
University of Illinois at Urbana Champaign, 608 South Wright Street, Urbana, Illinois 61801
Available online 17 July 2017

Abstract

This article examines the role that algorithms may play as audiences when teaching writing on the World Wide Web. It argues that introducing the provisional term “algorithmic audience” reflects three prior conceptions of audience, including concrete situations, discourse community, and participatory audiences. It then offers a three-part classroom approach: identifying the biases of those who design algorithms, managing metadata, and anticipating audience response. I argue that the term “algorithmic audience” may help students to write for audiences beyond the instructor from within the confines of the classroom.

Keywords: Audience; Algorithm; Web 2.0; Web-writing; Participatory audience

On the World Wide Web, writers have more work than simply writing. In “When Writing Becomes Content,” Lisa Dush notes that writers act as content producers and possess a wide variety of responsibilities (Dush, 2015). Writers, as content producers, contend with marketing, advertising, and programming. This means they take on multiple roles: circulating content on various social media platforms, monitoring website analytics, curating metadata, managing comments, and recirculating older writing to new venues. As writers perform these activities, moving content throughout the web, who or what are these writers producing content for? What role does the term audience play for these writers?

In this article, I address an overlooked aspect of these two questions by suggesting that algorithms may form a critical component of a writer’s audience. I argue that teaching students to write for internet contexts should involve considering the role that algorithms may play as audiences. In doing so, I reaffirm the relevance of the term audience for web-writers while introducing algorithmic audience as a provisional concept for teaching web-writing.

In general terms, an algorithm is a set of instructions for performing a task or solving a problem. A cooking recipe, for instance, is an example of an everyday algorithm. In the context of this article, algorithms as input/output functions process a text and yield a result. On the World Wide Web, algorithms sort, distribute, and organize websites, writing, and content. In doing so, algorithms evaluate, structure, and influence writing and other discursive information. To write for algorithmic audiences means to write for algorithmic procedures, which Kevin A. Brock (2014) describes as “fundamentally involving a set of operations meant to complete a task. These operations demand the computation of one or more variables for the operations to be successfully examined, undertaken, and completed” (1). For example, Google uses algorithms to structure its search results. Social media companies use algorithms to structure what users see in their newsfeeds. Algorithms frequently order and circulate web-writing, such as what stories are “trending” on various social media platforms. Alternatively, the online retail giant Amazon uses an algorithm to determine what products to show customers as they peruse the website. An individual who writes product descriptions on Amazon...
may conceive of the company’s algorithm as an audience. This writer conceives of the various keywords that potential customers would input and the way that Amazon structures its search results. The algorithm is part of this writer’s audience. Writers in these contexts are able to design and situate their content in ways that an algorithm can pick up and prioritize.

As sets of instructions and procedures, algorithms are, at their most basic level, a text written by individuals or teams of designers, coders, or content producers. From this perspective, writing for algorithmic audiences means to write not only for the algorithm’s input/output functions but also for the structure and sociality that goes into that function. If we are to teach students to write and produce content for the Web effectively, then we may consider algorithms as an audience while understanding that this audience can change depending on a host of factors, including nonhuman factors (e.g., changes in code, algorithmic variables, changes in interfaces, and software advances) and human factors (e.g., who writes the code and algorithms, designs interfaces, and decides on software updates and when to implement these updates).

This article is divided into four parts. I first describe algorithmic audience as a provisional attempt to capture the tension between human and nonhuman factors. I offer two examples of writing for algorithmic audiences and then argue for the term’s pedagogical value. Second, I lay out how this term is applicable to composition’s broader conversations about audience. Third, I describe a classroom approach for integrating writing for algorithmic audiences. Lastly, I identify how algorithmic audiences can move our teaching beyond the platitude of “consider your audience.”

1. An Extended Description of Algorithmic Audience

In using the term algorithmic audience, I aim to capture the tension between human and nonhuman factors when writing and producing content for the Web. On the one hand, algorithms have no agency of their own because someone or something else authors them. In short, algorithms have no intentions. An algorithm may update the results of its instructions and procedures (through what computer scientists label algorithmic efficiency), but it is ultimately a set of procedures—an idea that digital rhetoricians such as Jim Brown (2015) and Steve Holmes (2014) have come to label procedural rhetoric via Ian Bogost’s work—that yields results in predictable ways. In spite of their seemingly autonomous response, these results are authored and require people to write the code that produces them. In this sense, to write for algorithmic audiences means to consider the people who design and program an algorithm.

On the other hand, algorithms are objects distinct from their authors. Because algorithms are fundamentally a set of operations, they can escape the intentions of those who authored them and yield unintended results. They may even make decisions without the consent of those who write them. They have something akin to agency in the sense of having an effect in the world, but without any intention or responsibility for those effects (in both helpful and deleterious ways). That effect comes from algorithms’ programmed purpose, production of results.

Let me offer two concrete examples of writing for algorithmic audiences to highlight the human and nonhuman elements of the term. The first involves Facebook’s algorithmically driven timeline. The second is publishing videos to YouTube. On platforms such as these, individual contributions are just one among millions, if not billions. Writers need to contend with this obstacle to reach their audience. Thus, when teaching students to write for environments on the Web, we often draw on concepts of distribution and circulation, such as spreading writing within and across social media platforms. Students might write blogs or for hobby websites but they also need to circulate their messages on social media sites, e.g., Facebook, Twitter, Instagram, and Snapchat, in order to build, find, and create a readership.

I choose Facebook because it is a useful starting point for students to circulate their content and due to the site’s ubiquity. While many websites have diverse algorithms that prioritize certain characteristics of content, the layout of Facebook’s timeline provides an emblematic moment that captures the tension I previously described. Recent posts can be displayed in Facebook’s newsfeed (RSS feed), but the algorithm defaults the display to “popular,” which emphasizes recent interactions with a post. If a student writes a post that receives numerous “likes” on Facebook, for instance, that post will be prioritized in the newsfeed of that student’s friends—even if it is not the most recent. The student might also comment on an older photograph with many “likes” in order to push that post back into the newsfeed of their friends. By attending to content in this way, the student demonstrates an awareness of Facebook’s algorithm as part of their perceived audience. Teaching this type of awareness and habit means that in addition to teaching students to write

---

1 Other authors have focused implicitly on ways that algorithms yield unpredictable results, including Casey Boyle (2015).
for a particular set of readers, we are also teaching for a set of procedures that highlight content for readers. In this example, the student has demonstrated writing for algorithmic audiences by identifying a particular set of algorithmic procedures (i.e., manipulating Facebook’s interface) that will enable their writing to be read more widely (i.e., by other users).

My second example of algorithmic audiences, publishing videos to the platform YouTube, extends content production further, into considerations for metadata. I choose YouTube because it (a) has been the focus of previous composition scholarship (Dilger, 2010; Jackson & Wallin, 2009; Skinnell, 2010), (b) is an accessible way for students to engage public audiences beyond the bounds of a classroom, and (c) is a common platform that writing instructors have encountered in a pedagogical context, whether producing or consuming videos. Let’s posit that students decide to start a YouTube channel for a classroom assignment about public multimodal composing, perhaps documenting campus protests. They receive permissions to post the videos, record the videos, and upload them to YouTube after careful hours of editing. Who is going to watch them? How do they “consider their audience”?

Students can “consider their audience” in two ways. On the one hand, students may consider the various people interested in their protest videos, e.g., other students, faculty, community members, and the media. On the other hand, they can focus on ways to increase the circulation of their videos by thinking through how users find their videos. That is, they can think of their audience as the processes and procedures by which YouTube prioritizes their videos. This latter perspective asks students to think of YouTube’s algorithms, i.e., its processes and procedures, as their audience. Because students cannot guarantee any particular groups of users will view their videos within the context of a semester’s timeframe, thinking about an algorithm as an audience allows them to take action within the confines of a classroom while still engaging in public rhetoric.

To do so, students in this example ought to label their videos with certain strategic keywords in the title, description, and tags (Fig. 1).

Known as metadata, this type of information asks students to consider how their readers would find their content and what kinds of steps they need to take to increase their videos’ circulation. While other compositionists have touched on metadata for the purposes of surveillance (González & DeVoss, 2016) and networks of “women’s pedagogical and administrative contributions” (Graban, 2013, p. 173), connecting the act of writing metadata as a way of reaching viewers helps to frame the algorithm as an audience.

To elaborate on this connection, students might consider how to categorize their campus protest videos, add a location (even if it’s not accurate), enable or disable comments, or allow ratings (Fig. 2).

Students need to consider the menu (Fig. 2) in order to determine to how they might receive attention effectively (i.e., what kind of attention? how much attention?). In terms of attention, YouTube’s algorithm ranks certain channels higher for uploading videos with consistent content, meaning that students need to upload multiple videos over the course of time to garner more views and viewers. Likewise, videos that are watched in their entirety, rather than piecemeal, are ranked more highly; students need to produce quality videos from start to finish in order to increase circulation. More engagements with videos, such as comments, like, and shares, ranks videos higher in YouTube’s algorithm and enables more users to view students’ content. To write content on a YouTube channel involves considering YouTube’s algorithm as an audience. These examples show concrete ways that students could write for an algorithm as an audience.

An algorithmic audience, as a term then, is valuable for web-writing because it pairs human and nonhuman factors while retaining a pedagogical connection to writing and rhetoric. Through its inheritance of the rhetorical tradition, audience retains a core emphasis on how rhetors conceive of their listeners or readers. In the classroom, audience traditionally stresses how student writers perceive people as their readers. Using algorithmic audience emphasizes that
people (e.g., teachers, student peers, friends) will still read web-writing and content, but other readers exist, including corporate search engines like Google and Bing as well as social media algorithms. Pairing algorithm with audience emphasizes a pedagogical orientation for writing on the World Wide Web.

2. Algorithmic Audience as an Extension of Audience Paradigms

This section situates the term algorithmic audience in composition and rhetoric scholarship in order to show how the term reflects our concerns with teaching audience. As a concept, audience has been a crucial component of the composition classroom because teaching audience awareness encourages students to step outside of their perspectives and develop a vision for their argument from the perspective of their readers. Writing for algorithmic audiences, i.e., writing for search engines, databases, and rich site summary (RSS) newsfeeds, reflects this perspective by asking students to write for a reading procedure outside of their own perspectives. This approach extends three theories of audience: (1) audience is an overdetermined term that can usefully be taught through concrete situations; (2) through what we call a discourse community, audiences can influence the writer by influencing the language of a text; and (3) participatory audiences play a role in the creation of writing and content.

First, writing for algorithmic audiences requires writing for specific or concrete algorithms. No approach is singularly correct when writing for algorithms. To write for Google’s (PageRank), Facebook’s (formerly EdgeRank), or Twitter’s (“trending”) algorithm means writing with different expectations, purposes, and discourses for each algorithm— and, of course, the biases of people who program and can change algorithms without warning. Writing for algorithmic audiences requires knowledge about specific algorithms and the context surrounding that algorithm— an idea reflecting the rich history of teaching audience.

Lisa Ede and Andrea Lunsford’s canonical “A udience A ddressed/A udience I nvoked” (1984) advocates for such a specific context by moving audience beyond a static abstraction. As Ede and Lunsford write, “One way to conceive of ‘audience,’ then, is as an overdetermined or unusually rich concept, one which may perhaps be best specified through the analysis of precise, concrete situations” (1984, p. 168). To teach audience, whether as a construct of the writer or as a writer contending with actual readers, means to teach students how to negotiate the specificity of situations and deliberate on writing concrete particulars. The original address/invoke paradigm formulates audience as a balancing of the writers’ perception of the concrete reality of their readers and the rhetorical role the writers’ want their readers to adopt (address and invoke are both constructions of the writer).
Like the canonical address/invite paradigm, writing for algorithmic audiences asks writers to interact with specific, concrete readers—or, more precisely, specific reading patterns and procedures. While the original address/invite paradigm was inadequate for algorithmic audiences because it did not involve real readers, other scholars have updated the address/invite paradigm, updates that enable it to have shared resonance and application to algorithms. In “Representing Audience,” (1996) Ede and Lunsford expand the paradigm by accounting for ideological and institutional power relations. Likewise, Robert G. Roth’s “The Evolving Audience” (1987) and Robert R. Johnson’s “Audience Involved” (1997) added real readers to the address/invite paradigm because they did not see enough change in, or collaboration with, actual audiences. Roth employs “evolving” and Johnson uses “involved” to describe audiences who are no longer the construct of the writer but are concrete specific readers (or groups of readers).

Writing for algorithmic audiences reflects this updated, nuanced address/invite paradigm by attending to the various perceived and real algorithms, along with power relations. For instance, writers can’t address or invite Google’s PageRank in the abstract. Web-writers need to involve an algorithm in their writing processes, see how it evolves (Roth, 1987), and account for various institutional influences on the algorithm (Lunsford & Ede, 1996). They need to write, build, interact, and develop web-content in order to discover the ways PageRank detects that writing; they need to consult with (“involve”) the algorithm as an audience and revise it based on the results discovered.

The second way writing for algorithmic audiences can be viewed as extending composition’s conceptions of audience is that algorithms influence the language writers use to produce text, an idea echoed in the term discourse community. Discourse community is metaphor2 for the way a community exerts influence over the way individuals conceptualize and express ideas. The metaphor has been helpful for describing particular groups of communities who have specialized ways of thinking, acting, being, and believing—or “(writing)-doing-being-valuing-believing combinations” (Gee 1990, p. 142). The influence of an algorithm parallels the influence of discourse community.

When writing for Google’s PageRank algorithm, for example, effective writers are met by expectations and demands of how that algorithm will “read” (process) their content and writing to order its results on Google’s homepage. Like a discourse community, PageRank does not force writers to produce content in certain ways. Rather, if a writer demonstrates PageRank’s values, then the writer will reap rewards—much like a writer illustrating the values within a discourse community. Because writers know that PageRank will value websites written in certain ways, they might consult Google’s Search Engine Optimization Start Guide3 (SEOSG), which lays outs ways to write and design content so that PageRank will place their website’s content higher in its search results. The SEOSG, which is more explicit than a discourse community, provides a description of PageRank’s and, partly, Google’s values.

While I cannot touch on all of the values presented in SEOSG, I will briefly touch on the way PageRank can influence titles and writing habits. For titles, the SEOSG states that writers should (a) “accurately describe the page’s content,” (b) create unique title tags for each page, and (c) “use brief, but descriptive titles” (5). For general writing practices, the SEOSG urges writers to (a) “write easy-to-read text,” e.g., labeling images, writing without spelling and grammatical mistakes, (b) “stay organized around a topic,” (c) “create fresh, unique content,” and (d) “create content primarily for . . . users, not search engines” (15). According to the SEOSG, PageRank values accurate, unique, and brief titles as well as writing that is focused, not repetitive, and aimed at users not algorithms (there is a bit of irony here). Like a discourse community, PageRank actively shapes the rhetorical language and conventions as the writer produces content, designs the website, and writes individual webpages. And, as with a discourse community, a writer can choose to ignore PageRank’s values, perhaps discovering latent values which Google’s designers are unaware. Or the writer may choose to write for another algorithm—a different discourse community.

The third way the term algorithmic audience draws on and extends composition and rhetoric’s conception of audience is through the participatory role readers may play in the creation of writing and content. In addition to media critics like Henry Jenkins and Philip Napoleon, Elizabeth M. Weiser, Brian M. Fehler, and Angela M. González’s Engaging Audience: Writing in an Age of New Literacies (2009) brings to light issues of interactivity between writer and audiences in the 21st century. In this edited collection, Ede and Lunsford update their canonical piece a second time with a short text, “A mong the Audience,” (Lunsford and Ede, 2009) that asks the field to consider audience in light of

---

2 Joseph Harris (1989) has critiqued the concept of discourse community as being “little more than a metaphor” (15) and Mary J. Reiff (1996) has argued James E. Porter’s (1992) use of discourse community in Audience and Rhetoric—one of the most extensive texts about discourse community in composition—problematically portrays members of a discourse community as being too “homogenous” and text-based (Reiff 1996, p. 109).

readers' participatory role in interactive media, and the rest of the collection responds to this call. Algorithms add to the perspective of participatory audiences by incorporating audience response—i.e., comments, call-and-response writing, discussion forums, and "qualitative affordances" of social media platforms such as likes, shares, and retweets—into elements that writers might anticipate and predict (Tarsa, 2015, p. 22).

Algorithms do so by reorienting feedback from participatory audiences into results. They treat concatenations of readers', viewers', and listeners' feedback in predetermined systematic ways that organize feedback. The participatory response of readers consequently becomes a concern for writers contending with current and prospective audiences because that response could change the way algorithms process writers' texts. As an example, when Facebook's defunct EdgeRank algorithm picks up a writer's content, more readers may have the opportunity to read it; understanding the algorithm as a possible audience in this way is a crucial writerly habit. EdgeRank accounts for the ongoing reception of texts posted, reacted to, shared, and circulated on its site from composite audiences in the "ue" of the following equation:

\[ \sum u_e w_e d_e \]

\( u_e \) = user affinity, \( w_e \) = weight of content, \( d_e \) = time decay or lapse

To briefly explain this notation, user affinity measures interactions between users. If two users are in a relationship or tag each other as related, user affinity increases. User behaviors such as commenting, clicking, liking, sharing, or tagging a post will also yield higher user affinity. Weight of content \( w_e \) means that certain types of writing are more important than others (i.e., a photo with text is weighted higher than a photo alone, comments are worth more than likes, sharing photos and videos are worth more than links, etc.). Time decay \( d_e \), in the context of Facebook's environment, means that recent content is more valuable than older content. Writing, e.g., content, with higher (1) user affinity, (2) weight of content, and (3) time decay will appear to more Facebook users.

In terms of participatory audiences, the algorithm incorporates the responses, feedback, and reactions of readers \( u_e \). To write a popular status update on Facebook, for instance, not only requires an effective post at a good time of day, but also requires that other people like, comment, share, and react to it. Further, the designers of Facebook constantly tweak EdgeRank, which in turn means that writers looking for audiences on Facebook need to monitor and observe the extent to which they effectively communicate to readers. To write for EdgeRank as an algorithmic audience thus means to write in ways that anticipates, and accounts for, audience participation.

Algorithmic audience, as a term, thus extends three of composition's theories of audience, e.g., concrete situations, discourse communities, and participatory audiences, into 21st century writing contexts. The term takes prior concerns with teaching audience and applies them to 21st century pedagogical issues. Writing for algorithmic audiences powerfully integrates production, distribution, and circulation while developing an ongoing sense of managing those aspects and updating one's writing accordingly.

3. Writing for Algorithmic Audiences in the Classroom

Having described how algorithmic audiences extend three conceptions of audience—specific audiences, discourse communities, and participatory audiences—I outline a classroom approach that integrates writing for algorithmic audiences. This approach might be part of a broader unit on teaching audience awareness or its own unit in an upper level English class (as it was in my classroom). My three-part approach draws upon Estee Beck's (2015) understanding of both nonhuman and human factors for classroom audiences: "Because networked culture is as much about the hardware, software, and immaterial algorithms as it is about the people and the cultural codes embedded within those systems, a theory that moves past a binary between humans and objects as tools helps usher in new lines of research and conversations about object agency" (2015, p. 135). Beck's approach accounts for both algorithms and their designers. I will describe each part of this approach conceptually and then offer teaching examples for each concept.

4 By composite audiences, I mean "...people differing character, loyalty, and functions" who express themselves online (Perelman and Olbrechts-Tyteca 1969, p. 21). While Frank Myers (1999) has picked up on composite audience in terms of political argumentation and Mike Duncan (2011) in terms of polemical ambiguity, compositionists and rhetoricians have only recently started to think about the ways imagined and actual audiences are composites in online environments (Breuch, 2015, p. 121).
To briefly offer context to this pedagogy: I taught an upper level English course titled, “Internet Rhetoric and Writing,” in the fall of 2015. In this class, students engaged with readings about commenting culture, trolling, and representations of race and gender while designing their own websites. The goal of this class was to encourage students to produce, circulate, and manage content on a consistent—daily or weekly—basis. Content for websites was up to them; they developed topics ranging from television show reviews (both written and podcast form), technology reviews, videogame tips, flash fiction blogs, fashion advice (this student won an internship in the UK for this blog), salsa dance culture, and career-oriented professional portfolios. In order to assist students’ in conceptualizing audiences, I created a two-week long unit titled, “Writing for Algorithms.” This unit came during the latter third of the class so that students had already created a significant collection of content. This unit is the basis for the approach I offer in this article.

The first part of this classroom approach asks students to consider the designers and programmers of algorithms when they write for the Web. The second part asks students to manage and curate data that algorithms can process, such as tagging, search functionalities, and qualitative affordances. The third part of the approach asks students to develop an anticipatory and imagined perspective for algorithmic audiences. After these each part, I discuss the specific assignment given to students. The approach consequently develops an awareness of algorithmic regulation, which Steve Holmes (2014), by way of Tim O’Reilly, argues “uses real-time measurement to determine whether certain outcomes are being achieved and, in turn, relies on algorithms (rules) to make adjustments based upon the received data.”

3.1. The values and ideologies of algorithms’ designers and programmers

The first aspect of writing for algorithms asks students to identify and investigate the values of an algorithm’s designers, programmers, and architects. Many companies offer a sense of their values and ideologies through marketing and advertising. Other, more concrete, examples can be found, including the aforementioned SEOSG. Google offers the SEOSG as a guide for writing content but it also reflects the values of PageRank’s designers and engineers. Considering the non-neutral input/output structure of algorithms through various documents helps students recognize that algorithms are subjective.

I ask students to research and read documents like the SEOSG, terms of service agreements, white papers, corporate statements, and other mundane grey literature companies publish in order to assist students in identifying the values of designers, the engineers who write code, and denaturalizing algorithmic equations. By denaturalizing the ideologies, institutions, people, and technologies that factor into the results of algorithms, students can effectively critique the way their web-writing is read and received by audiences.

Contending with the values of the designers and programmers crucially deciphers the inherent bias of algorithms by helping to reveal the black box culture of internet culture. Journalism critic Chava Gourarie (2016) points out that algorithms “encode human bias” and have “inherently unfair design tics” because they look for patterns in their input. In my class, we looked for such “tics.” Such pattern-recognition calls attention to writing that doesn’t fit a designer’s or a programmer’s preconceived notions—writing at risk for being abused or ignored. Writers who do not produce text that fits the pattern identification of algorithms are thus at risk—writers who are too frequently women, people of color, and other individuals that computer programmers, often white men, do not consider.

In my classroom, students attempt to have their websites ranked highly by PageRank (from “googling” their name or a phrase associated with their website). This approach connects the production, distribution, and circulation of writing within ideological frameworks that may be overlooked in social media venues or other popular internet environments. Students critique their own websites, often noting that in order to satisfy the values of PageRank, they had to sacrifice elements of their personal writing styles. Students examine how the changes made to their websites’ architecture (known as meta-descriptions and meta-tags in HTML) alter Google’s search results, which yield ideological discussions of algorithms.

I use Gourarie’s three-step process for buttressing discussions of these experiments. Gourarie understands this algorithmic subjectivity in the following ways: “Algorithms can generally be broken down into three parts: the data that goes in; the ‘black box,’ or the actual algorithmic process; and the outcome, or the value that gets spit out.

---

5 Grey literature is a category of self-published writing, typically from a company, that is written from the perspective or persona of an institution rather than individual.

6 For an extended discussion of the term “black box,” see Frank Pasquale’s *The Black Box Society* (2015).
Human constructs, we can attend to algorithms as persuadable, subjective writing activities rather than objective features of internet communication. By offering students ways to identify the biases of those who produce algorithms, writing instructors can effectively assist student writers to see that writing for algorithmic audiences involves a rich understanding of the way culture becomes infused into seemingly objective writing activities like search engine optimization, website development, and circulation of content. Raising awareness of algorithms as dominant ideological structures can assist students in identifying the power structures that undergird the dissemination of web-writing.

As a concrete example of pedagogy, I ask students to write reflections that I call *algorithm narratives*, which discuss students' efforts to identify the values and ideologies of a chosen algorithm. I task students to research their chosen algorithms in three ways: by drawing on academic and online resources, by performing qualitative research by contacting the companies that program the algorithms, and by conducting first-hand experiments with the algorithm(s) to determine what kind of writing and content it favors. Most students chose to write about relatively well-known algorithms, such as Google's PageRank and Facebook's EdgeRank, although some chose to write about more opaque algorithms like those on dating websites. Students frequently noted in their narratives that companies are loathe to share their values for both proprietary and public-relations reasons. They frequently remarked that "black boxes" are meant to stay closed and mysterious. Their algorithm narratives document these difficulties while providing a concrete way to access issues that are often intentionally obscured.

### 3.2. Management of Metadata and Analytics

Analyzing the data that goes into an algorithm assists students with developing concrete writing practices—what we might call technical literacies—for how an algorithm reads and processes text. Interrogating the components of web-writing assists students in seeing how metadata, such as tagging, search functionalities, and qualitative affordances, can function as input that students should integrate into their conceptions of audience. When developed in concert with one another, these components illustrate that writing for algorithmic audiences involves managing and monitoring web-writing.

Identifying how algorithms read metadata, e.g., data that provides information about other data, assists student writers in producing texts for algorithms because it helps to describe context for texts. While metadata has been around since before the advent of the web, notably through the card catalogue system in libraries, it has become significantly more widespread with the prominence of internet searches. In the context of web-writing, metadata includes the language of a webpage (e.g., HTML, JavaScript, CSS) and what kind of information the author(s) has deemed relevant (i.e., keywords). Identifying metadata and its relationship to how a text is discovered and distributed therefore involves attending to the writing around a text as well the text itself.

Tagging, search functionalities, and qualitative affordances, as types of metadata, are examples of the writing surrounding a text. When an algorithm indexes a text, it also indexes the input of readers, who may tag that article or post with additional information, thereby adding more input to an algorithm for which writers did not account. Search functionalities are often based around the order and structure of websites. Likewise, qualitative affordances will shape how algorithms process a text. In rhetorical terms, the *arrangement* of a website and *delivery* of the site's content is crucial to how algorithms determine their results.

I encourage students to produce, curate, manage, and monitor this kind of metadata in addition to the web texts they create. To ensure their content is read, students sign up for a program that tracks their website's analytics (page views, duration of page views, etc.). I task students with writing weekly progress reports to their peers about their website's activity and comments, which are a concrete type of metadata that can accompany initial texts. In sharing these reports during class, students help one another find ways of circulating their content that are effective for their specific purposes. A circulation strategy students frequently discussed in their reports leveraged commenting in blog or online article comment sections and on social media threads. They would find an article relevant to their content and write a short comment along with a hyperlink (the URL) back to their own website. This activity generally drove up their metrics and metadata, e.g., page views, and frequently allowed them to garner participatory audiences, via comments, for their websites. These reports and activities aim to inculcate a heightened awareness of search engine and algorithm biases as well as strategies for managing information surrounding their writing. Developing metadata awareness assists students in deciphering how to manage and monitor their websites from a holistic perspective.
3.3. Anticipating Audiences

Based on managing metadata and analytics, students may consider how algorithms and their results could change over the course of time. They imagine how to write for audiences across geographical and geopolitical cultures in the present and future. This pedagogy adopts what communication scholars Eden Litt (2012) and David Russell Brake (2012), by way of Ervin Goffman, have labeled imagined audiences in electronically mediated environments like chat rooms and social media. Compositionist Lee-A nn K astman B reuch (2015) has picked up on an actual/imagined tension with respect to reaching global audiences while meeting local audiences’ needs (using M innesota’s website of the 2010 A ffordable Care A ct). Imagining audience(s) across space and time for internet environments requires anticipating how audiences might read and distribute texts.

As part of writing for algorithmic audiences, anticipating audience participation assists students with understanding how algorithms incorporate texts into results. Because the operational logics and regulations of algorithms are ongoing, writing for them involves not publishing and distributing once but in a continuous manner. The implication here is that timing matters in a recursive manner, as algorithms yield different results on different days, times, and places. Students anticipate how readers will read in not only one future but at different times and places in many futures.

In terms of examples, I encourage students to circulate their writing multiple times so that algorithms would pick up their content. Because one link, post, or tweet often gets lost in the overload and time decay of newsfeeds and timelines, my students consider when they would distribute their writing (e.g., when to tweet, when to post a blog post), the frequency of distribution (how often to publish for audience), and the reception of that distribution (i.e., who has commented, what kinds of comments were received, what were the qualitative affordances received). Students share content on Twitter with an assortment of hashtags, hoping that targeted, imagined audiences would retweet content. In order to manage online discussions, students develop commenting policies for their websites to combat the misogynistic, homophobic, and racist vitriol that often appears in comment sections. As I mentioned previously, they often comment on relevant blogs and websites that aligned with their purposes with a link back to their websites—a crucial strategy for building a readership. In this sense, students anticipate the various ways their content may be delivered and re-delivered, with the possibility for endless circulation.

In keeping a focus on circulation, I ask students to imagine audiences through usability testing. Students rewrite content—blogs posts, podcasts, videos—after initial production in order to vary their results if algorithms do not display their content to audiences effectively. They optimize the website’s architecture (titles of webpages, HTML tags, paragraph structures, sentence syntax, and word choice) according to the algorithm they imagine writing for—often the SEOSG so that PageRank would yield their website higher in its rankings. Usability testing functions as a way to evaluate the extent to which they anticipate their audiences effectively—something that is extraordinary difficult to do in composition classrooms where instructors are often an authoritative audience.

I ask students to keep a log documenting the changes they make to their websites and how those changes alter where their websites fall within search results. In these entries, students often hypothesize how small tweaks in content or different types of content, e.g., text, images, and video, could change search results. Then students make those edits to observe changes in actual search results. I ask them to document their content changes through alphabetic text and series of screenshots. This documentation process encourages students to think of a website as a changing ecosystem rather than a static document or space.

4. A Classroom Solution to “Consider Your Audience”

This last section addresses the way that writing for algorithmic audiences may assist writing instructors with building audiences outside the classroom that can nevertheless be addressed from within the classroom. To write for audiences beyond the teacher has long been a source of consternation for classroom-based writing instruction, as Robert Brooke and John Hendricks’ Audience Expectations and Teacher Demands (1989) eloquently tackled. That is, students in the confines of a classroom only seem to have one audience: the instructor. As a provisional solution, algorithmic audiences can assist teachers and students with escaping this problem of audience in the confines of a classroom. When writing for algorithmic audiences, the algorithm becomes an audience that yields a result. This allows students to escape the influence of the instructor as the audience for student writing. Through peer collaboration, students can help one another to write for algorithms because they can see the different outputs an algorithm may yield. It remains
Algorithmic audiences are thus highly relevant to compositionists because they can help instructors to push students beyond the platitude “consider your audience.” Algorithms change our approach to writing by asking students to evaluate the reception of a text during the production process of that text (i.e., what will the algorithm yield when it processes a student text?). They reframe the reading of texts as an ongoing process that not only requires editing but an updatable, malleable form of revision involving monitoring and managing of content that occurs on a continuing, emergent basis. They encourage students to write not only for a pre-existing audience but also to find and anticipate an audience repeatedly. While algorithmic audiences ought to be part of a broader pedagogy for teaching audience awareness, the concept can assist with resolving the classroom problem of writing for audiences outside a classroom from within the confines of that classroom.

John R. Gallagher is a visiting assistant professor at the University of Illinois, Urbana-Champaign. He researches participatory Internet writing culture, especially online comments. He is currently working on a book-length manuscript about the way online commenters and reviewers generate conversations through their rhetorical strategies.

References


Day 4: Sousveillance and Strategies for Activism
Everyone Watches, Nobody Sees: How Black Women Disrupt Surveillance Theory

Surveillance
Our picture of surveillance needs to factor in not just tech developments, but the cultural standards that have bred surveillance, especially towards black culture, as part and parcel in our world.

by Sydette Harry on October 6th, 2014

What the hell is you looking for? Can’t a young man get money anymore?

It kind of pains me to call Mason Betha prophetic, but 17 years ago when “Looking at Me” hit the Billboard charts, the Harlem native pretty much described the current state of surveillance and tech in America. Especially for black people and doubly so for black women.

Surveillance is based on a presumption of entitlement to access, by right or by force. More importantly, it hinges on the belief that those surveilled will not be able to reject surveillance — either due to the consequences of resisting, or the stealth of the observance. They either won’t say no, or they can’t.

Discussions of stolen celebrity selfies often miss the “by force” aspect of the breeches, instead focusing on salacious details. Surveillance is part of the information age, but it has always been part of abusive dynamics. As opting into surveillance becomes increasingly mandatory to participate in societies and platforms, surveillance has been woven into the fabric of our lives in ways we can not readily reject.

Being watched is not just an activity of Big Brother-style surveillance, but also fannish adulation and social enmeshment. As Black women have been historically denied the ability to consent to surveillance, modern discussion of watching and observing black women needs better historical context. When I’nasah Crockett points out how black women online have constantly been portrayed as “raving amazons,” one of the unspoken through lines is how easily media, even on the left, believes dissecting black women, tracking their online habits, consuming illegally obtained images of them, and demanding education is a “right”. Black women cannot say no, and do not need to be in any way respected or fully informed about how they will be studied or used. Media collects the data of black activity and media production as a weapon, without black participation. The lack of black participation can be unintentional or intentional, but usually ends in gross appropriation, clumsy “admiration”, willful erasure or a troublesome combo of all three. Combined with historical blindness, racist condescension and content desperation, the modern surveillance of black women too often results in the same historical abuse and erasure of black women.
When Patricia Garcia says that the big booty era has finally arrived as a “high fashion” moment, but credits Jennifer Lopez and Iggy Azalea, it erases the very real abuse that black bodies have suffered for those exact body types, that were surveilled to produce the standard that Garcia hands over to Lopez et. al. She writes:

“Rihanna shows up to the CFDA Awards practically naked with her crack fully on display and walks off with a Fashion Icon Award. Perhaps we have Jennifer Lopez to thank (or blame?) for sparking the booty movement.”

Suggesting the way to Rihanna’s 2014 moment was paved by Lopez shows a dangerous laziness towards the stated goal of body positivity. Rihanna’s moment was a direct tribute to Josephine Baker, another black woman often sexualized and placed under surveillance, not just for celebration of her uniquely black body but for her participation in World War II and the civil rights movement. Garcia’s “cultural surveillance” ends up being a contextless mess that insults both Rihanna and Baker.
Writing for Salon, I pointed out that Media has no idea how to talk about race, and more recently I am convinced they do not actually care to learn. Unfortunately when covering Black women, this inability or unwillingness to learn defaults to common stereotypes at best and complete cultural propaganda at worst. That unwillingness create a vacuum of knowledge, as history repeats itself over and over.

Take Alessandra Stanley's profile of Shonda Rhimes in the New York Times: a cringe-worthy attempt at “complimenting” Rhimes' stereotype-breaking television output that instead relies on empty surveillance of black characters while Stanley offers no evidence of having actually watched the shows she cites. Stanley's descriptions of Rhimes and her work are filled with words like “angry, terrorizing and sassy,” recalling Crockett's angry amazons perfectly while perpetuating and prolonging logic that for decades kept Viola Davis from being the leading lady
Stanley describes. Her piece ignores multi-year plot developments as well as a wonderful opportunity to discuss Rhimes’ accomplishments as possibly the only non-white-male with multiple, simultaneous network TV hits. Her surveillance provides little in the way of edification and a lot in codifying uncomfortable catch 22’s for black women and privacy: visibility is part of achievement in media, but is it worth it when even at the pinnacle of your success the only thing made visible is the racism of those observing you?

Even more difficult, how do you fight back?

Under Surveillance, Over Exposed

Steven Mann’s concept of sousveillance centers on wearing portable cameras and technology to record activity, but I would like to expand it to include all forms of using tech to jam surveillance. Mann, a pioneer in the field of wearable computing and computation photography, framed the concept of wearable cameras functioning as recording data for the user, not an outside network. Hashtags, street recordings, phone taps can all be looked at as ways of using tech to push back against surveillance. #Yourslipisshowing in particular was used to fight #4chan surveillance of black women. Crockett, user @sassycrass, and a community of black women (myself included)
used the hashtag to expose 4chan board members who declared “war” on black feminists by tracking and attempting to infiltrate their “ranks.” The attempt was foiled mostly by how their racist caricatures of black women (much like Stanley’s) were so jarringly incongruent with reality.

However, sousveillance often requires large amounts of disclosure to be effective and ultimately negates privacy even more. Hasan M. Elahi responded to being incorrectly surveilled by making a project of displaying his personal information. Similarly, Black women’s responses to abusive surveillance has often been heart-rending accounts of personal trauma and exposure of personal networks. What goes unmentioned is that social capital and safety are often key to being able to go public with sousveillance as a strategy. Mann and Elahi – credentialed, well-known professors – have a much easier time of saying they agree to be watched than those on the margins.

Stacia L. Brown offers a beautiful examination of the ramifications of ahistorical surveillance, discussing representation as well as more diverse media sources as counter-tactics. As Brown points out in response to Garcia’s flippant mess: “It isn't about who gets credit for popularizing the ‘big booty.’ It’s about who is erased and minimized in the process.”

Her recommendations are solid but also bring up a very real question: for populations whose fundamental problem under surveillance is the inability to declare privacy and boundaries, what kind of solution is being made to expose one's self “voluntarily,” to invite more observation into one’s life?

The response to these articles and continued moments of ahistorical abuse and sometimes outright violence are a version of cultural sousveillance. Black women must lay themselves bare, exposing trauma and constantly excavating painful historical memory to gain sympathy and respect. Surveillance must be used as sousveillance, with the records generated by the intrusive observation of blackness, used to bolster black testimony.

Buzzfeed has an article that is a triggering reminder of the murkiness of this dilemma. While being one of the few places to acknowledge how Daniel Holtzclaw, a predatory policemen targeted black women, it also notes how he used surveillance, and even the more stringent sousveillance to track black women to abuse. To emphasize the gravity of his offense, once again black women’s trauma is made public with overly specific details on the abuse of his victims.

More disturbingly have been the deaths of three black men: Eric Garner, Michael Brown and John Crawford III, all murdered by police. In all three cases there was video/photo evidence of the deaths that circulated the internet, and in Brown’s case, even AFTER the mother requested it stop. Crawford's death is a disturbing illustration of the interplay of surveillance and sousveillance with historical discrimination. The police who ultimately ended his life were responding to a report, via citizen surveillance, that he had been observed with a gun. The surveillance video which showed him being shot? Still not enough for indictment.
Why must black death be broadcast and consumed to be believe, and what is it beyond spectacle if it cannot be used to obtain justice?

History Repeating

When Janay Rice was assaulted by her husband, it became a rallying cry for domestic violence and resulted in job creation for white feminists. What stuck out immediately was the ease at which the surveillance aspects were skipped over. Echoing a similar leak of a private moment that targeted the Knowles-Carter family, little discussion was made of how a culture of intrusion seemed to focus on the abuse of black women as breaking news without asking about breaches of boundaries.

That the same online communities that continually prodded and mocked black women are incubators for sex criminals who expose private pictures of celebrities isn't shocking, it's inevitable. They watched the world not care, why should they anticipate consequences now? Predators are often wrongly pictured as targeting the defenseless, when they also target the undefended. Black people, women particularly have historically been able to defend themselves, but have also been shown to be undefended. The problem is not that they can't fight back, but that their fight and the record of what they were fighting is erased and sanitized for easier consumption.

When Laurie Penny and Lola Okolosie claim a victory over racist and sexists online, they willfully

Photo CC-BY ibkod, filtered.
erase the original problem of targeted women not wanting to be surveilled, and shut down conversations about how that issue can be addressed. If they have won already, what does the trauma of the women used in that success matter?

Just recently, threats to “expose” Emma Watson’s nudes turned out to be a prank to “draw attention” to attacks on feminists. The very real trauma of women — who even after they were transgressed were asked to answer for it like they had committed the crime — becomes a “gotcha” moment. A time to ask what factors lead to the abuse of women and where it starts — usually with black women expressing feminist or anti-racist ideals — becomes covered in really uncomfortable racist/classist overtones, namely: “What happens if this happens to a white woman we actually care about?!” Even as women of all colors have been fighting for years to make legislation against revenge porn.

When Janay Rice was assaulted by her husband, it became a rallying cry for domestic violence and resulted in job creation for white feminists. It’s a cry that does not truly encompass the necessary complexity of the problem in the NFL, or give anything at all to the attacked woman. This major step to “address issues” still hinges on making a black woman’s personal affairs heartbreakingly public and assuring that no one who represents her voice — which has asked for very different things than advocacy — will be heard.

What We Call Surveillance
What we have decided to call surveillance is actually a constant interplay of various forms of monitoring that have existed and focused on black people, and specifically black women, long before cameras were around, let alone ubiquitous. Surveillance technology is a dissemination of cultural standards of monitoring. Our picture of surveillance needs to factor in not just tech developments, but the cultural standards that have bred surveillance, especially towards black culture, as part and parcel in our world.

Elahi can use the intrusion into his privacy to further his work. But if all you want to do is have space to mind your own business, handle your family issues in private, or exist without interference, sousveillance isn't an answer... it's a reminder of defeat. If what you want is representation as you are, what do you do when the reality is ignored for the easy win, even when it leaves you worse than before?

What is the solution for being constantly watched, if no one sees you at all?
Knowledge of the depth and extent of the potential dangers facing our society often leaves people feeling understandably dazed and powerless. But the story is not one of unremitting gloom.

Sousveillance and public opinion

To some degree, surveillance cuts both ways. Thanks to the prevalence of video and phone cameras, ordinary citizens now have a means of ‘watching the watchers’ and recording their observations, an activity known as ‘sousveillance’ (literally ‘watching from below’). Although many ‘sousveillance events’ are little more than self-indulgent stunts (World Sousveillance Day appears to have involved nothing more provocative than taking still photographs of CCTV cameras), other activists have had major impacts on society. Sousveillance does offer the possibility of logging at least some of the corrupt or illegal practices of the authorities and their agents in such detail that there is no opportunity for ‘plausible deniability’.

Perhaps the first effective example of watching the watcher occurred on 3 March 1991 when George Holliday filmed four officers of the LAPD mercilessly beating a lone black man,
Rodney King. King was on parole for a robbery conviction at the time, had failed to stop the car he was driving and had jumped several red lights and stop signs before he was pulled over. The police claimed that King had tried to resist arrest and continued to resist even while being hit with batons. However, the video showed King immobile on the ground and the police continuing to belabour his inert body regardless. The incident became something of a *cause célèbre* and was a major factor in the LA riots a year later. During the ensuing trial only one of the policemen was found guilty, partly because a segment of the video (not widely shown by the media) showed King getting up and attacking a policeman.

More recently, in November 2006, widely-viewed footage on YouTube revealed a UCLA police officer assaulting a student in the university library. The important point here is not merely the act of sousveillance, but the publicising of examples of abuse to the widest possible audience. For example, in August 2007 three police officers of the Sûreté du Québec (Quebec Police) infiltrated a demonstration against the leaders of Canada, Mexico, and the United States at a meeting of the Security and Prosperity Partnership (SPP) in Montebello, Quebec. The demonstrators claimed that the officers were *agents provocateurs*, there to provoke an incident that would discredit the demonstration and allow the deployment of riot police. When the head of the Quebec police denied the allegations and publicly stated that there had been no police presence, a sousveillance video screened on YouTube revealed that he was lying. He quickly revised his statement to say that while police might have been placed among the protestors, they were there as peaceful observers only. Scrutiny of the sousveillance video showed them to be masked, wearing police boots, with at least one holding a rock. At one point Dave Coles, president of the Communications, Energy and Paperworkers Union, had to order the three masked
police ‘observers’ away from a confrontation with the line of riot police.

The practice of sousveillance has now spread to the developing world. Organisations such as ‘Witness’ in the USA lend video equipment to human rights activists around the globe, and have led to exposes such as Operation Fine Girl, detailing rape as a weapon of war in Sierra Leone.¹

But despite such advantages, the balance of power remains vastly in favour of the Big Boys, whose technological reach and firepower will always vastly outweigh that of the individual or action group. Regulation in the form of ‘codes of practice’ is regularly ignored; legal restrictions are flouted, or made obsolete by rapidly changing technology. Those attempting to implement the global surveillance strategy can only be defeated by a groundswell of public opinion, and by privacy activists willing to fight a long, sustained campaign to raise public awareness. There are parallels here to the eco-warriors of the 70s – dismissed for decades as ‘idealistic greenies’, they refused to buy into the ‘resistance is futile’ or ‘this is progress’ mantras that are promoted so consistently and so effectively by both government and major corporations. Many commentators felt that their goals, though laudable, were idealistic and unrealistic. Yet the eco-warriors persisted, and today much of their agenda is now accepted as mainstream.

Australia provides a perfect, and timely, example of the need for public awareness and the power of public opinion. In 1986 the Australian government signalled its intention of issuing a national identity card (the Australia Card Bill, or ACB). The rationale behind the move was the usual mix of catching benefit frauds and apprehending illegal immigrants, with the added implication that ‘only those with something to hide had something to fear’. Most Australians were quickly sold on the idea, with opinion polls showing an 80 per cent approval of the proposal.
Then, slowly at first, but with increasing insistence, questions began to be asked on civil liberties and privacy. When the public heard that the number of government departments intending to require the ID card had leaped from three to 30 their suspicions grew, and were confirmed by the minutiae of the Bill, which listed a host of restrictive penalties. Cardless persons could not be hired or paid (fine for doing so: A$20,000), would be denied access to pre-existing bank accounts, could not cash in investments, give or receive money from a solicitor, or receive funds from unit trusts. They could not buy or rent their own home. If your card was destroyed and you could not prove that its loss was accidental there was a $5,000 fine or two years in prison (or both). Failure to produce your ID on demand at a tax office incurred a A$20,000 penalty. Cardless sick and unemployed people, pensioners, widows and invalids would be denied benefits.

Nor was this likely to be the limit of the repressive measures envisioned for the people of Australia. Aware of possible resistance, the card’s architect, the Health Insurance Commission, suggested a plan which discussed the incremental stealth strategy used in so many surveillance proposals with surprising honesty:

One possibility would be to use a staged approach for implementation, whereby only less sensitive data are held in the system initially, with the facility to input additional data at a later stage when public acceptance may be forthcoming more readily.

A parliamentary joint select committee found against the card, pointing out the serious civil liberties implications and warning of a fundamental change in the relationship between citizen and state. Newspapers on the right and left raised their voice against the Bill and many famous Australians joined the clamour. Public opinion, now fully informed, swung solidly against the
ID card and within a few weeks the 80 per cent approval had metamorphosed into an astonishing 90 per cent opposition to the Bill. Faced with a protest of monumental proportions, the government backed down.

It would be nice to report that the victory was permanent. Unfortunately, Thomas Jefferson’s old adage on freedom\(^2\) applies with a vengeance to surveillance. While the Australian public quickly lost interest in the ID card issue, their rulers simply bided their time. Two decades later the concept reappeared, when former Australian Prime Minister John Howard announced a scheme (national card; linked to a massive central database; essential to stop fraud and benefit cheats etc) that looked suspiciously like the old ID card idea. But Mr Howard insisted that the two concepts were poles apart and engaged in some outrageous doublespeak to prove it. Just as the UK ID card had become an Entitlement Card, so now the Australian ID was metamorphosed by the magic of political sophistry into the all-new Access Card. Nor was the card to be mandatory for all Australians. ‘It will not be compulsory to have the card,’ Howard told journalists, adding however that ‘it will be necessary for everybody who needs a card to apply for one.’ As, from 2010, the provision of health and social services will be denied anyone without an Access Card, then except for those guaranteed lifelong health and prosperity, the card is essential to all Australians. Surprisingly, the scam seems to have worked; the lessons of the 80s have been lost, and a step-wise, stealthy approach has lulled a continent’s population into acceptance. This is all the more surprising when other, less intrusive methods of establishing identity are now available.
Designing out surveillance: the privacy card

The UK administration, along with many Western governments, continues to insist on the necessity of ID cards linked to massive databases. These databases, and their interconnectivity, are responsible for a huge number of privacy and civil liberty concerns, not least of which is dataveillance. But as much as the UK government might wish it, there is simply no need for biometric patterns on ID cards, e-passports and the like to be checked against a central database. The pattern can be stored within the smart card itself, with the comparison exercise being performed within the card – which would then say simply ‘Yes’ or ‘No’ to the system. In the case of e-passports with fingerprint biometrics, the owner of the passport would place their digit against a fingerprint reader which would then capture the data and convert it to a transitory biometric template. The machine would then electronically interrogate the e-passport and determine if the pattern it had just recorded was the same as the pattern held on the passport. If the patterns matched, identity would be confirmed – and all without resort to any central database.

We can have secure identity without recourse to centralisation. Indeed, there are no technological barriers to the production of a comprehensive ‘privacy card’ which would act as a buffer to prevent information being centralised. Such a card could disguise the identity of its owner and scramble personal information so as to prevent the collection of sensitive data in large databases by large organisations.

Of course, such cards would still depend upon RFID technology to be effective, leaving the owner vulnerable to a scanning attack by illicit card readers, and a consequent risk of ID theft if the encryption protecting the data is broken (not
to mention the location and surveillance dangers of the technology). Unless we forgo RFID entirely there does not seem to be any way of avoiding such threats. But rejecting RFID passports is by no means a bad idea – other more secure methods of checking and verifying such documents already exist.

Ingenia Technology have developed ‘Laser Surface Authentication’ (LSA) which allows any document, including a passport or ID card, to be positively identified by virtue of its unique individual surface qualities. When paper or plastic laminate is made, each sheet ‘sets’ in a one-off configuration dependent on a variety of factors such as fibre orientation, temperature and humidity. The surface of each sheet is as unique as a human fingerprint – it is impossible to counterfeit. The newly-developed Ingenia technology can scan any document to reveal this ‘LSA fingerprint’ of its surface properties. The system dispenses with any data chip; it is ‘read-only’ and, once scanned, a record of the document’s surface features is stored on a database along with non-biometric details of its owner. When the document is rescanned the appropriate details – name, address, etc, of the owner – can be instantly displayed.

This is a highly accurate system, which not only makes false matching unlikely but allows counterfeit passports to be detected immediately (those documents lacking a database presence would be invalid), and can even detect whether a photograph or name has been altered.

The Royal Academy of Engineering has pointed out that LSA scanning is far more secure than the government-favoured RFID solution. In addition, the Academy's report points out that it 'could also offer privacy gains, as the amount of information on the database available to the person scanning a passport can be controlled – it could be limited to just a name or a photo or even just the assurance that the passport is a genuine passport issued by the appropriate country. This technology could
be used for ID cards. Instead of ID cards having chips on them or information printed on their surface, they could be linked to databases in the same way. Provided the database is secure, then individuals' privacy and security is protected. Alternatively, more advanced privacy schemes are possible where the LSA fingerprint is used as an encryption key for locally held personal information. Traditional technologies such as 2D barcodes can be used to carry the information on the card itself. This offers the same immutability of data as would occur if it was held on a central database, combined with the inability to make identical copies.

Instead of using such advances that could easily circumvent the known vulnerabilities of RFID-based cards, the UK government (and now the European Union) seems hell-bent on deploying one of the few systems which absolutely require the establishment of huge central databases. The question is, of course, why? And the next, cui bono? It is most definitely not the citizen. Bureaucracy and big business are the only winners here.

LSA scanning is just one of a number of privacy-enhancing technologies (PETs) which essentially act as countermeasures against the PITs (privacy invasive technologies). The web can be surfed anonymously via sites such as Turbohide.com; web 'cookies' can be filtered; encryption of personal data can prevent corporations (though not governments) from obtaining data; network design and software code can produce a marked regulatory effect; privacy preference tools and smart agents can likewise help to keep the surveillance society at bay. But most countermeasures are for the computer aficionado – those lacking knowledge, awareness or even the wherewithal to implement the available PETs will always remain in the majority.

Some forms of electronic communication, such as email, are still possible anonymously via 'remailers' and other arrangements, who manage a succession of intermediary-operated
services in which (like cells in a resistance or espionage organisation) each intermediary knows only the identity of those adjacent to it in the chain. ‘Pseudonymity’ is also possible, where substantial protections are put in place, but can be removed under defined legal circumstances. While ‘anonymity’ sites raise questions of what purpose they may ultimately serve (criminal and terrorist organisations will find them particularly useful), ‘pseudonymity’ has its own problems, in that the power to override protections is normally in the hands of government or corporations and, as Roger Clarke has commented, ‘governments throughout history have shown themselves to be untrustworthy when their interests are too seriously threatened; and corporations are dedicated to shareholder value alone ...’

Privacy Impact Assessment

The similarities between the environmental protests of the 1970s and today’s anti-surveillance activism point up a method to slow down or stop the deployment of harmful surveillance systems. With our ‘greener’ perceptions, the Environmental Impact Assessment (EIA) is now accepted practice throughout the developed world whenever new building or infrastructure developments are mooted. An EIA allows for a review, in advance of any building work, of any possible environmental effects that may accrue from the proposed project. Recently, there have been demands that a similar Privacy Impact Assessment (PIA) be required before the rollout of new surveillance procedures. This call has been heeded in some countries, and both the USA and Canada have mandated the technique for all federal-level, public-sector projects where personal data is processed. So far the UK government has shown interest in the idea, but without moving to any mandatory requirement. This is unfortunate, as
at present new information systems and methods of processing and transferring data between and across departments are often established with little or no regard for privacy concerns. When things go wrong, operators are faced with the challenge of mending the system, often with costly 'bolt-on' solutions that compromise efficiency. Or, as often as not, the problem is simply ignored. A report for the information commissioner by the Surveillance Studies Network explained that, in simple terms, a PIA may be seen as:

- 'an assessment of any actual or potential effects that an activity or proposal may have on individual privacy and the ways in which any adverse effects may be mitigated.'

- 'a process. The fact of going through this process and examining the options will bring forth a host of alternatives which may not otherwise have been considered.'

- an approach and a philosophy that holds promise by instilling a more effective culture of understanding and practice within organisations that process personal data.

- a form of risk assessment, which therefore cannot escape the uncertainties of identifying and estimating the severity and likelihood of the various risks that may appear to privacy, life chances, discrimination, equality and so on.

- a tool for opening up the proposed technologies or applications to in-depth scrutiny, debate and precautionary action within the organisation(s) involved.
• like PETs, premised on the view that it is better to build safeguards in than to bolt them on.

• an early-warning technique for decision-makers and operators of systems that process personal information, enabling them to understand and resolve conflicts between their aims and practices, and the required protection of privacy as set out above or the control of surveillance.

• Ideally, a public document leading to gains in transparency and in the elevation of public awareness of surveillance issues and dangers may be realised; in turn, it may assist regulatory bodies in carrying out their work effectively.

PIAs are long overdue in the United Kingdom, but they are not the whole story. As we have seen, surveillance encompasses more than simple privacy concerns. The time is ripe for an expansion of the PIA concept to one of Surveillance Impact Assessment (SIA), allowing for a review which would encompass the totality of surveillance effects, both individual and societal. As the Surveillance Studies Network report states:

What an ICT innovation, a new database, or a new audio-visual scheme for monitoring public places or private shopping precincts implies for personal autonomy and dignity, social solidarity, or the texture of social interactions, is not an inconceivable line of enquiry that could become institutionalised as a set of practices and requirements before those surveillance possibilities are implemented.

Despite it being merely common sense and natural justice to ask such basic questions, such a Surveillance Impact Assessment
requirement would demand a painful shift of worldview for government, corporations, and privacy regulators alike. But it is a change they must make if we are to support and maintain such basic values as trust, goodwill and a belief in the democratic process within our increasingly fractured society.

Direct action

If all else fails, it is still possible to organise effective protests against some of the worst excesses of the surveillance society. It is surprising how much surveillance actually depends upon the cooperation or acquiescence of the individual under observation or from whom data is required. The UK government’s own figures – made public grudgingly, after three years’ delay – reveal that 30 per cent of the UK population is predicted to refuse to cooperate with ID card checks. Should this figure rise to over 50 per cent (as may well occur when the full impact of the ID legislation becomes apparent), the whole scheme could well become unworkable. In addition, workers in the surveillance business may have philosophical issues about the use to which the data they collect is put; they can quite easily disrupt or modify this data collection, degrading its value.

Using cash and postal mail services serves to disconnect you, to some degree, from the surveillance web. Refusing store cards of any colour prevents further entries under your name on marketing lists; obtaining cards in false names further confuses the marketers (anti-surveillance advocate and former MIT professor Gary Marx has obtained store cards in the names of both Karl and Groucho Marx). In a similar way, forms and documents that demand an overabundance of personal details may be filled out with imaginary information. Small errors in
the spelling of names, addresses and other details will create multiple entries in the databases and make successful data-matching less likely. Workers who key in information from forms can similarly introduce deliberate mistakes, and even greater disruption is possible from computer programmers erasing databases (and backups), or introducing logic bombs, Trojan horses and similar disruptive programmes. As Brian Martin has pointed out, a simple magnet can corrupt computer disks. It is even possible to make your own RFID 'fryer' to frustrate clothing tags and ID cards alike, although this practice is fraught with risk and should be discouraged.

Unfortunately, such methods have serious limitations: they may have nuisance value but, given the size and complexity of the surveillance web, they are little more than pinpricks in the hide of the surveillance behemoth. And they are individual acts, performed for the most part in secrecy. But other, more overt strategies are possible.

The south coast town of Brighton is not normally associated with direct action in any shape or form. But on 10 May 1997, two hundred individuals joined together in what was Britain's first coordinated attack on a CCTV camera system. According to one activist magazine, 'Public ridicule of surveillance cameras is effective in diminishing their power – and more importantly their dignity – and making them highly visible to people who have simply got used [to them] as street furniture.' The protesters were creative in their approach: over 2,000 black and yellow posters carrying the words 'WARNING You Are Being Watched By Closed Circuit Television' were stuck up in toilets and other public spaces, provoking argument and indignation; lasers were used to 'blind' the cameras; posts carrying the cameras were 'occupied'; one camera was hoodwinked with a bag; the highlight of the day came 'when a blow-up doll, the sort available from sex shops, was hoisted to the top of a camera pole and
some rather embarrassed firefighters were dispatched with their ladders to remove her.\textsuperscript{12}

The protestors demonstrated a sophisticated knowledge of both the psychology and the technology of CCTV:

More fun can be had trying to destabilise the confidence in the relationship between the camera operator and the police on the ground. For example, some sea-front boy racers were caught pouring liquid from a petrol can onto a car in front of a CCTV camera. When the police raced to the scene, the lads got out some sponges and said they were just cleaning it (the can contained water) ... Making plays in front of a range of cameras simultaneously sends a direct message to the control room that we are watching them watching us. Identical masks can be used for protection and confusion ... Many cameras use microwaves to send information back to the central control room, and these can be disabled using reflective industrial foil strips attached to helium-filled balloons at the correct height. Camera poles can be useful ‘Lost Children Stations’. Simply make a sign and give balloons to children waiting under the cameras. Now who would take a balloon off a child?

But despite the satisfaction such demonstrations engender, we should not fool ourselves. Present resistance efforts are better than nothing, but they still take place within a general and growing surveillance environment – small victories do not equate to a dismantling of the panoptic whole. ‘Who will watch the watchers?’ is a critical question; but then, so is ‘Who will watch the watchers of the watchers?’ and so on \textit{ad nauseam}. The truth is that even with the biggest budgets, the most advanced technology and the best will in the world, no system we can set in place will be invulnerable to subversion. Human ingenuity combined with human craving for superiority and power will
always find a way around restrictions. Examples abound: the Constitution of the United States of America explicitly states that control of the nation’s money supply should rest with the state. And yet we have a private bank (the cunningly named Federal Reserve, which has nothing to do with the US government and can be found, should you choose to look, among the white ‘business pages’ of the US telephone directory), co-owned by seven private banks, at least three of whom are not even US entities, doing just that and essentially dictating the economy of the USA. Despite appearances to the contrary, Alan Greenspan and his successors are private businessmen to a man.

That such a subterfuge can be perpetrated on the American people, against the explicit prohibition of the Constitution, is a timely ‘heads-up’ to all those concerned with the intrusive nature of modern corporate and governmental structures; we must beware of taking appearance for substance, of confusing high-sounding declarations, voluntary codes and toothless legislation for effective regulation and relevant laws that will vigorously pursue any miscreant with custodial deterrent sentences. The surveillance network is huge, and continues to expand and pry into ever more sensitive areas of our lives. Only comprehensive legislation, and the outright banning of some of its more intrusive offshoots, will control surveillance’s worst excesses. Individuals and pressure groups can help cut holes in the surveillance web, but until public opinion sets its weight behind such lone voices, it will be difficult indeed to stem the tide. As Ericson and Haggerty have pointed out: ‘In the face of multiple connections across myriad technologies and practices, struggles against particular manifestations of surveillance, as important as they might be, are akin to efforts to keep the ocean’s tide back with a broom — a frantic focus on a particular unpalatable technology or practice while the general tide of surveillance washes over us all.’

235
OUR DATA BODIES

RECLAIMING OUR DATA

INTERIM REPORT | DETROIT

JUNE 15, 2018

TAWANA PETTY, MARIELLA SABA, TAMIKA LEWIS, SEETA PEÑA GANGADHARAN, VIRGINIA EUBANKS
This report carries a Creative Commons Attribution 4.0 International license, which permits re-use of Our Data Bodies content when proper attribution is provided. This means you are free to share and adapt ODB’s work, or include our content in derivative works, under the following conditions:

**Attribution.** You must give [appropriate credit](http://creativecommons.org), provide a link to the license, and [indicate if changes were made](http://creativecommons.org). You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

For the full legal code of this Creative Commons license, please visit [creativecommons.org](http://creativecommons.org).
## Table of Contents

Introduction .................................................................................................................................. 1

About This Report ......................................................................................................................... 2

About Our Team ........................................................................................................................... 3

Who Funds This Work ................................................................................................................... 3

Additional Acknowledgments ....................................................................................................... 3

What We Know: City Perspectives on Data Collection and Data-Driven Systems ....................... 4

Charlotte ................................................................................................................................... 5

   Background ........................................................................................................................... 5

   Word on the Streets ........................................................................................................... 6

Detroit ..................................................................................................................................... 12

   Background ......................................................................................................................... 12

   We Didn’t Get Here By Accident ........................................................................................ 14

Los Angeles ............................................................................................................................. 18

   Background ......................................................................................................................... 18

   Power Not Paranoia ............................................................................................................. 19

Our Data Bodies: Commonalities Among Us ............................................................................. 24

Predatory data-driven systems routinely hold us back and prevent us from meeting basic needs ...................................................................................................................................... 24

Data-driven systems unfairly divert us from resources we are entitled to and need to survive. ................................................................................................................................................ 26

Data collection feels extractive and takes a serious emotional toll on us. .............................. 27

The hurt and the harms of data-driven systems connect to past systems of discrimination and exploitation against members of marginalized communities ................................................. 29

Our strategies for self-defense and survival keep us connected and feeling whole .............. 30

Our policies, priorities, and visions for the future focus on just models of governance, economics, and criminal justice, and on guarantees for our human rights ........................................... 31

Our Reflections and Future ......................................................................................................... 33
Introduction

Our Data Bodies (ODB) is a research justice project that examines the impact of data collection and data-driven systems on the ability of marginalized peoples to meet their human needs. For the past three years, ODB has been working in three cities—Charlotte, North Carolina; Detroit, Michigan; and Los Angeles California. To date, we have completed nearly 135 in-depth interviews with residents of these cities’ most historically marginalized neighborhoods. Our project combines community-based organizing, capacity-building, and rigorous academic research.

Our goal is to find answers to three main questions:

- *How do marginalized adults experience and make sense of the collection, storage, sharing and analysis of their personal information?*
- *How, if at all, do marginalized adults connect their ability to meet their basic material and social needs to their inclusion in (or exclusion from) data-based systems?*
- *What strategies do marginalized adults deploy, if any, to protect their digital privacy, self-determination, and data rights?*

Through collective community building and analysis of the stories we’ve collected, the ODB project has identified many similarities in how people across the three cities experience data collection and data-driven systems. Patterns have emerged like insecurity and targeting, resignation and resistance, the separation of family—whether through incarceration, detention, deportation, or foster care systems—and speak to the way that individuals are forced to trade away their data to attain basic human needs.

Our community members describe the experience of being forced to engage with intrusive and unsecure data-driven systems because of their membership in groups that have historically faced exploitation, discrimination, predation, and other forms of structural violence. They’ve shared with us their experience of being caught in a cycle of injustice and the impact this feedback loop has on their livelihoods.

Our interviewees also tell a story of wanting both privacy and the ability to be seen and heard as whole human beings. Charlotteans, Detroiter, and Angelinos are resilient in spite of persistent and destructive forms of surveillance and profiling. They believe in their humanity, value human relationships, and want respect and recognition in and beyond the systems of data collection that try to govern their lives.

Overall, surveillance and data collection are deeply connected to diversion from public benefits, insecure housing, loss of job opportunities, and the policing and criminalization of our communities. Whether an error or something they have overcome, people’s data stays with them—far longer than more advantaged groups, and its impacts are profound.
About This Report

The work that we present is the culmination of years of working with our communities and building on popular education, critical literacy, and other participatory strategies to identify the productive ways in which people want data collection and data-driven systems in our lives. In January 2016, when Center for Community Transitions (CCT) in Charlotte began its involvement with ODB, CCT had been strengthening its support structures for reentry, including teaching digital know-how and skills in a city strategizing the growth of healthy digital infrastructure. When the Detroit Community Technology Project launched ODB efforts in Detroit, it had been extending a model of digital stewardship and principles of digital justice to demystify citywide open data initiatives, co-design community wireless networks, and use digital technologies to strengthen human connections amongst Detrotiers. In Los Angeles, when Stop LAPD Spying Coalition (SLSC) launched its ODB efforts, SLSC had been seeding Power Not Paranoia, an organizing framework that exposes the impacts of and deepens collective resistance to surveillance and policing.¹

Since ODB efforts launched, this collective, community-based work continues to grow. Our interactions have included countless community meetings, interviews, focus groups, and workshops that bear witness to the lives and experiences of individuals as they confront data collection and data-driven systems in the process of meeting basic human needs. These interactions ground our work and show us how community-driven practices and visions will continue to take these conversations into the future.

In the pages that follow, we present our interim findings. We have combed through our interviews to identify commonalities and differences that are emerging between the cities. In the process, we have attempted to honor the diverse histories and contexts of our interviewees and the particularities of the neighborhoods in which they live. Our interviewees come from:

- Five districts in Detroit
  - District 2,
  - District 3,
  - District 5, and
  - District 6
- Several pockets of Los Angeles
  - Skid Row,
  - Public housing projects in Southeast LA, and
  - Other neighborhoods that serve as home to LA’s unhoused populations
- Neighborhoods scattered across seven different zip codes of Charlotte,
  - 28201
  - 28205
  - 28206

We are grateful for the time our interviewees gave us and for their continued interested in our broader, collective efforts.

**About Our Team**

ODB is a five-person project concerned about the ways our communities’ digital information is collected, stored, and shared by government and corporations. We are:

- Tamika Lewis: A Charlotte-based organizer and artist whose primary focus is advancing Queer People of Color and marginalized communities;
- Tawana Petty: A mother, anti-racist social justice organizer, author, and poet, born and raised in Detroit, Michigan;
- Mariella Saba: A mother-to-be in Los Angeles who practices popular education, cultural work, and healing arts, to collectively, creatively, and healthily uproot the genocidal set-ups of our global dis-ease;
- Seeta Peña Gangadharan: A mother and research justice organizer born in New Jersey and working in London; and
- Virginia Eubanks: A writer, teacher, and welfare rights organizer from Troy, NY.

We are a predominantly women-of-color research team that is interested in how technology can intersect with social, economic, and racial justice.

**Who Funds This Work**

This work is made possible in part by a grant from the Digital Trust Foundation. The Digital Trust Foundation was set up by Facebook after losing a class action lawsuit. DTF funds projects that promote online privacy, safety, and security. We are also thankful for support from Institute of International Education, Media Democracy Fund, and Mozilla Foundation.

**Additional Acknowledgments**

We are also grateful to staff at Center for Community Transitions, Detroit Community Technology Project, Los Angeles Community Action Network (SLSC’s organizational home), and Stop LAPD Spying Coalition. In particular, we want to thank Myra Clark (CCT), Diana Nucera (DCTP), and Hamid Khan (SLSC) for welcoming ODB into these organizations and for their leadership.
What We Know: City Perspectives on Data Collection and Data-Driven Systems

Since 2016, the ODB Project has been listening deeply to the concerns, analyses, and self-defense strategies of communities targeted for intensive data collection by government agencies and corporations. In each city, we identified a specific set of experiences that would serve as a lens to focus our explorations. In Charlotte, we focused on the experience of re-entry, of returning from jail or prison back to your home community. Here, we were interested in how data impacted all areas of re-entering people’s lives—their housing, community relationships, social service experiences, etc.—but we dug most deeply into how re-entry data affected the search for employment.

In Detroit, we focused on the experience of foreclosure, evictions, and water and utility shut-offs. Here, we were interested in how your “data trail”—the collected digital record of your past decisions, resources, and interactions with government—impacts your access to the basic human rights of shelter and water. Our relationship with the Detroit Community Technology Project (DCTP) also reminded us to be attentive to how affordable and secure access to the internet created benefits and new opportunities.

In Los Angeles, we focused on how data and digital surveillance impacts the experience of housing or houseless. At Jordan Downs, one of the country’s oldest public housing projects, we asked community members about how data collection, sharing, and analysis shaped their experiences of a $1 billion redevelopment plan they fear will displace them. In Skid Row, and throughout the city, we also spoke with unhoused residents about how data affected their experience of finding shelter and navigating the criminalization of homelessness and poverty.
Charlotte

Background
A beacon of the New South, Charlotte’s population has transformed dramatically over the past century. As one of the country’s most important financial centers, the city is undergoing dramatic demographic changes that include a forty percent increase in residential population over a ten-year period and growth in per capita income that outpaces that of the entire state.²

However, Charlotteans do not reap the benefits of Queen City’s booming economy equally, and many argue these changes link to a longer history of gross inequities due to the displacement and forced labor of Black populations.³ According to a 2014 study, the city ranked last out of 50 large cities for income mobility.⁴ Skyrocketing rates of income inequality combined with segregation, mass incarceration, and the hollowing out of middle-class jobs have overwhelming contributed to the racialized disparities that exist now. According to Bureau of Justice Statistics, while Blacks make up 22% of the state population, they account for 55% of the incarcerated population.⁵ At the county level, police are more likely to arrest Blacks than Whites for marijuana possession: out of nearly 2,000 arrests in 2014, 91% were Black, while the remaining 9% were White.⁶

---

Meanwhile, the city spends millions to equip police with body cameras in the name of countering bias and promoting accountability of law enforcement. These cameras did not prevent officers from shooting dead Keith Lamont Scott in 2016, nor did they help to bring justice or increased accountability to the citizens of Charlotte and to the Scott family. When community outrage boiled over in the streets, Charlotte Uprising was born, and today organizing efforts continue for broader criminal justice reform. While Charlotte holds a place in history books for its centrality in racial equality and civil rights movements, the severity of current-day racial disparities and the fierceness of residents fighting back now define the city.

Our work in Charlotte grapples with the impact of data collection and surveillance on people who have past convictions or arrest. In the 50 interviews we completed for the Our Data Bodies project, we heard from a multitude of community members who are currently trying to harness the economic successes of the city during their re-entry process. These interviews highlighted the connection between data collection and data-driven systems to barriers of employment, services, and housing.

Word on the Streets...
By and large, Charlotte’s community members identified their criminal record as a critical piece of the cycle of injustice that perpetuates immobility, lack of opportunity, criminalization, discrimination, and systemic exclusion. Their stories describe how the stigma of being a “criminal” has negatively impacted their ability to meet their basic human needs while making them more susceptible to digital surveillance, police targeting and identity theft. They frequently highlighted the ways in which a criminal record holds people back.

Some themes that have emerged from our analysis:

My data doesn’t represent who I am.

Whether criminal records or bad credit, people expressed concern and frustration about the unrepresentative nature of data collected about them and how it is used to profile them as they reenter society. They emphasized that a low credit score or criminal records reflect the choices, judgments, or actions they made in their past, most due to scarcity, being young, or survival.

I mean, the credit score part, I really don’t think that represents who I am, because first of all, I don’t really even understand that. I understand that it needs to be at a certain level, but I just don’t get why you need that. It’s not necessary to me. I mean I’d rather have no credit than bad credit. I’m just saying, what is the point. – Nabresha

---

And even though their circumstances have changed, Charlotteans themselves have transformed, and have “served their time,” people are haunted by the profiles that follow them from place to place or job to job and impact their ability to move forward. These records—a kind of data trail, do not give others a full sense of who they are and where they want to go in life.

*I have a criminal background. It’s 15 to 30 years old. I plead guilty to worthless checks. It was 2003. Again, that’s almost 15 years ago, but it’s still held against me and it still hinders me. It makes it extremely hard to get employment, permanent employment. Basically, all of my jobs have been temporary positions or contract positions.* – Jill

In our data-driven society, people desire for their humanity to be respected and honored. In countless interviews, we heard people say they want to be seen as their full selves, as entire human beings—not as their profiled selves. People talk about having moved past their mistakes and wanting to rid themselves of that history.

*I think just mainstream society period is like once you have a criminal record, no matter if you stole bubblegum when you was 16, it’s like you’re a criminal. You’re a bad person… I think once you get a criminal record everybody looks at you like Trayvon Martin. And that’s pretty sad that they even have to bring his name up in a situation, but it’s like, you know, if you would really sit down and get to know me, I’m a very intelligent person. But if you’re just going off this paper, then it’s like…* – Bonnie

**The system isn’t all bad. It’s the people with decision-making power and policies that hold me back.** People matter to data collection processes and modulate the impact of data-driven systems on their daily lives. Individuals on the front lines of institutions and who receive or process information—such as with an application for a job, housing, or other social services—have the power to hold people back. Our interviewees described two kinds of individuals who process their data: 1) people who come from similar backgrounds, such as individuals with a criminal record who are now administrators; and 2) people who come from opposite backgrounds, such as people who do not have any relationship to or understanding of the criminal justice system or mass incarceration.

*A lot of people forget where they come from and a lot of people ain’t been through some things to realize where they could go. In other words, they abuse it. They misuse it. … [A] Black lady, Pam, she used to be out here. She forgot where she came from. She used to be homeless, on drugs, under that same bridge down there, buying drugs, doing everything…. I came in there from work one day to eat lunch, and they were giving out boots. I didn’t have enough time. I said, “Pam, can you save me boots? I’m still staying there until I get off.” She said, “What size do you wear?” I said, “I wear a size 9.” She goes in there and looks and goes, “Now, I got a 9 ½.” I said, “I can wear them. I’ll just put on a pair of socks.” She said, “No, you told me you wear a size 9. You*
can’t get these.” She wouldn’t give me the work boots because it was a half size too big. – Joker

The worst thing I ever heard was, “You probably should give up on finding a job.” He was like, “I don’t even know why you came today because you know you got a background, you know it’s recent, and you know most places are not going to hire you so you probably should just stop trying. Go to school or something.” – Karriem

Our interviewees also talked about the multiple ways in which company policies or procedure interferes with their ability to move past a criminal record. Charlotteans shared stories about how frank they were about past arrests or convictions, how well they performed in a job interview, and how recruiters assured them of their ability to be hired only to find out days or weeks later that someone in human resources or elsewhere blocked their employment, despite the candidate’s honesty.

I had extensive history in the medical field and I had an interview with the manager, she hired me right on the spot. I was upfront about my background, and so she said that she would do a drug screening. Even though I told her about the background, it was still their policy to run one, so I said fine. She gave me my start date and tell about the benefit package and this and that, and so within two weeks, I received a certified letter from them. They didn’t even call me. They sent a certified letter, I guess their human resources, and was like we can’t hire you. We have to rescind our offer. Yeah. They rescinded the offer based on the background check... I was devastated. – Debra

This event happens with companies and agencies that work with local organizations to hire individuals who have been previously incarcerated,

I actually tested for a data entry position back in February here with Goodwill. I had to come in and take a test, data entry test with keystroke testing, and everything worked out fine... She said I did exceptionally well on the test. My skills exceeded what they were looking for. She said, hey, you should have no problem getting this position, so I didn’t hear anything else from her. Three days went past. I said, well, let me call her, and just check the status. When I called her, she said, “Oh, everything was fine. It’s just that they don’t hire anyone that has larceny.”

It was really, really discouraging. I mean, it’s just hard, and sometimes it just makes me want to give up... I’m a single mom. I have a 14-year-old, and I have custody of my 4-year-old granddaughter. It’s like it really discourages me because it makes me feel like, hey, you’re never going to advance. – Jill

When candidates are highly qualified, knowledgeable, and have the credentials to fulfill a position, Charlotteans are turned back by companies’ policies whose hiring criteria rely on criminal records rather than people’s ability to perform and advance.
I would say it’s the policies and procedures of the company. Number one, whatever created those, whether it's the board of trustees, members of the organization, whoever. Those people that created those policies, I think it comes from the top. If you are a CEO of a company and you say we are felon friendly and I expect to have people with colorful backgrounds here, you’re going to have a really good company, in my opinion. You’re going to have people that go above and beyond because they want that opportunity to show.

– Kristie

I will reach my goal if I just put my best foot forward.

Community members have an awareness of how systems are currently working, but they are resilient and persevere despite the difficulties of reentry, repeated denials, and barriers to personal prosperity.

To me when I was in prison or what not, I heard a lot of people that came back... people that was even out here in this world tell me it’s hard out here in this world and jobs ain’t hiring. But to me, different strokes for different folks and what not. In my case, I had to have to gain the attitude to basically do something with myself. You know? By doing that I went forward. As I went forward opportunity came to me. I took advantage of that opportunity. To me personally, my experience I’m going to say it ain’t so much jobs not hiring or you get turned down because in life you can get turned down regardless. There’s so much, if you got the ambition to continue going, regardless if you been turned down or not, so it’s all on your decision and what you want for yourself. I got opportunity to basically come out and show them that you know, change is available. Change wasn’t just available to me but you know, change is available to anyone that want to take hold to it. – Jeremiah

They have a deep understanding of how data driven systems, their criminal records, systematic oppression, and discrimination impacts their viability and ability to take care of their basic human needs, but that doesn’t deter them from trying, no matter how difficult it gets, with the hope of getting the break they need.

I know I can go to a library and print me out a resume and send my resume or just keep my resumes with me or send them out to people and let them know I’m struggling; I’m homeless; I had a couple jobs; I don’t have too bad of a record. I still can get on my feet. It’s all a matter of who’s going to help you, who’s going to let you in the door. – Young Boy Dez

All in all, they keep a positive mindset in order to move forward, focusing on the future they want to create for themselves

Yeah. You’ve got to keep motivating. You have to always encourage yourself, even now, after the fact, you have to encourage yourself because if you don’t, you’ll give people power over you. Your situation should not have power over
you. You should have power over your situation. It makes you feel bad but then you keep going somewhere down the road a no is going to turn into a yes and then you can get the money, get the work. People work towards getting it rectified and paying it off. – Diddo

We want systems that work for us, not against us.
From public welfare to reentry organizations to prospective employers that welcome returning citizens, many support systems do not appear to offer the help people need. These support systems brand individuals a certain way and chastise them if they do not fit the mold. People want and need help in meeting their basic human needs—be it shelter, medical care, a job, and more. But we heard many talking about the difficulty of accessing services, feeling stigmatized, and getting fed up to the point of wanting to give up, leave shelters, or quit Charlotte.

At this point where I am right now, I feel like I benefit from these services, but right now, I feel like if I was to go ask them or anything, they would look at me funny like, “You grown man. You’re old enough, able-bodied...”They give me a stare, “You aren’t supposed to be here. What are you doing here?” It’s just like a funny room. I feel like I will be near homeless, starving to the bones... to even step into that atmosphere...They make me feel like, "You can get a job." You don’t know, for somebody that’s my age and my position, it’s pretty hard to ask for services. It’s like they play on your manhood. That’s what I get a feeling of. These people look at me funny. [Like] I don’t need nothing, but I do need help. – Lamont

A catch-22 emerged in some of the descriptions people shared: in order to access different social services, such as childcare, you need to meet a requirement or stipulation. For example, when reentering, people need to a to enroll in a class or classes, but they take place during the day and interfere with the times needed to engage in a job search process. Without evidence of a job, a person is barred from maintaining access to services, acquiring additional support, or finding help through social programs. We heard people say the incompatibility of these reentry requirements with the vicissitudes of daily life discouraged them and made them want to go back to their old lives. They also describe how the data-driven systems use and collect their information in order for them to receive the service, and how judgment and isolation is very much a part of those experiences.

She helps me with that, but I feel like I don’t want to let nobody know what I’ve been through. I feel like they’re judging me. Just like when I got to the herb (Urban Ministries), they always ask you for the digits [social security number], but I feel like I’m homeless, you all are using the information from me to just get money from me. It’s my social security number. I’ve been going through the herb about 10 years, so I feel like you all been drawing money from me for 10 years. – DO
Systems are communicating but not for my benefit.
Even though our interviews highlighted that data-driven systems are not all bad, it is mostly the policies and individuals that block them, they do agree that these systems communicate with each other, but not to help community members, just for the sole benefit of the data collector.

They’re not. But then they’re talking to each other when they’re giving out your information and trying to sell or make a profit off of it. So when it comes to taking money from you or when it comes to you needing information from them, they’re not willing to give it out, but when it’s giving information out for profit, they’re going to do it… If I don’t pay my taxes, you’ll send a cop to my house, because they don’t play with taxes. If you don’t pay your taxes, they will send a cop to your house and they will arrest your ass within a couple days. Same thing with rent, if you don’t pay that rent, they evict that ass, but when it’s time for you to get money from them or you need documentation from them, “Oh, well, you need to fill out this form. It’s going to take 10 to 15 business days for us to process the request, and it’s going to take another additional seven to 10 business days for us to send it out to you.” – Quincy

Some things might keep you from getting the job. Credit score might keep me from getting a job. My background might be keeping me from being able to get a job. Then I can’t pay for the necessities. I need to be able to pay lights, water, gas and keep a roof over my head. Then that way, you’re selling me short. You’re selling my information but you’re not selling it to where it benefits me – Diddo
Detroit

Background

Once the industrial center and the fourth largest city in the United States, Detroit is a crucible of social transformation and participatory democracy, where residents—as the African-American folk saying goes—have been making a way out of no way for decades.\footnote{James Boggs and Stephen M. Ward, Pages from a Black Radical’s Notebook: A James Boggs Reader (Detroit, MI: Wayne State University Press, 2011); Dianne Swann-Wright, A Way out of No Way: Claiming Family and Freedom in the New South (Charlottesville: University of Virginia Press, 2002).}


Any “renaissance” the city has experienced is profoundly uneven in its distribution. The comeback story omits that only 7.2 square miles or 5% of the city’s total area forms part of the revival. Detroit led the country in unemployment and child poverty rates in 2013, and in 2015 the Federal Communications Commission found that 40% of residents lack access to broadband internet, highest among big cities. Between 2011 and 2015 the city foreclosed on one in four homes due to overdue property taxes, and a dense area of foreclosures and property seizures extend across the city with the exception of the downtown area and a few neighborhoods.

Meanwhile, beginning in 2014, the Detroit Water and Sewage Department—an agency shouldering nearly $6 billion in debt—announced that it would target homes with unpaid bills, tweeting “If you’re stealing water, we’re coming after you.” In past years, residents have watched their water bills increase by as much as 119 percent, and an estimated 40 percent are delinquent on bills. An estimated 100,000 Detroiters have seen their water shut off since the
water authority initiated the effort.\textsuperscript{21} Power shut-offs also affect low-income Detroiters, and the energy authority is under recent investigation for computer glitches that led power loss for approximately 9,000 customers.\textsuperscript{22}

In a city where African-Americans make up over 80\% of the population, foreclosures and shutoffs follow a discriminatory history of institutional racism that stretches back to the economic upheaval that led to the Great Migration and brought thousands of black folks to Detroit. But contemporary Detroit also draws on its history as a center of human resilience, from the legacy of James and Grace Lee Boggs Center and Detroit Summer to Michigan Welfare Rights Organization, We the People of Detroit, and more.

**We Didn’t Get Here By Accident**

Our work in Detroit is situated within this context, and against a backdrop of recent crises for residents of the Motor City. The Detroiters with whom we spoke entered into the conversation about data collection and data-driven systems by reflecting on information collected or used by the city. In the 33 interviews we completed,\textsuperscript{23} Detroiters shared a range of stories that ran from the impacts of predation and bad credit to property misclassification and social media surveillance. Frustration with data-driven society is palpable, though not immutable. The Detroiters we spoke with combined talk of pervasive data collection, human needs, and the state of an unequal city.

*I don’t trust data-driven systems, though data could be used for better.*

Detroiters expressed a distrust of data systems, though acknowledged that data could be used in positive ways and made suggestions towards that end. Be it third parties, the state, or commercial predators, Detroiters expressed distrust of data collection on individuals. But our interviewees also talked about the possibility for change, including the idea of meaningful consent, targeting for the promotion of collective resources or quality-of-life improvements, as opposed to punitive data collection.

*Like maybe there needs to be some protections on how corporations access data. Like maybe there’s too much free reign. Maybe like, maybe this isn’t the right language but I’m thinking the reversed permit where a normal permit says you have to have—well, it’s not that you have to have this much money but you*


\textsuperscript{23} Due to unexpected circumstances, our analysis only uses 28 interviews. Seven audio files were corrupted and these stories were not retrievable.
have to pay this much money to do this type of thing. In this instance you didn’t have this much money you cannot do this type of thing. So if you have $500 million you just can’t access all publicly accessible data in the state or even in the city. So that prevents, I don’t know it might not 100% prevent monopolies, but you can maybe significantly prevent monopolies from having free reign and free access to data that’s going to make them more millions. - Tachalla

And so, I think limiting outright, like how that data can be used and what data can be collected, would be a start. And then also, just in general, having some sort of policy for, like, mandatory consent and, like, being able to opt out of getting… of giving certain data but still being able to get a service. Like, even all the way down to, like, if you download an app and they’re like, “We want to access to all of these things.” Like, no. You be able to either consent to that or, like, consent to giving them only access to certain things like the very specific things that they need in order to function. Like, maybe you don’t need access to all of my contacts with your Instagram, and I’m just going to be posting pictures. Maybe you only need to access my pictures. But a lot of the systems are, like, either… it’s not really like consent if, like, you just can’t have this thing that everybody uses unless you give us this. - Unicorn

The changes I would make would be to have data that is intentional and targeted and centering people in the middle of those decisions. So, data would be created for the people and with people as opposed to on people and against people. Data would be done in a way that is an instrument and a tool to support their uplift and the uplift of their consciousness and the quality of their lives. It would be used to map and visualize so that people’s understanding was centered in coming together and being their own solutionaries. It would be places of a tool for skill sharing and learning. It would put health as a priority. It would put our children’s education as a priority. It would mean that there would be no persons without housing if they so choose. It would be a pairing so we would be looking for ways to place people in homes as opposed to using data as a justification for pushing people out of homes. - Ollie Mae

I’m unfairly punished for bad past decisions.
A lot of people we spoke with in Detroit identify the punitive effects of the credit report. They feel like low credit functions as a penalty or mark against them, when predators are also part of the picture. Detroiters sense that a predatory market facilitated or enabled a bad consumer choice or behavior they made and that they receive the brunt of blame. The impacts of bad credit are severe and hinder people from meeting their basic needs.

So I’ve made a number of purchases throughout my life. Some of those included school loans. Some of those were other stupid credit card loans. Regardless they were loans. Granted, I haven’t paid many of them back yet, that data has been transferred between other credit card companies. So it creates this cumulative credit score that I have. That credit score determines my
access to future monies. So like a signal to how well I can pay back future money and that affects how much I’m able to do in the short near term future. – Tachalla

If your gas gets cut off, it’s going to impede your lights. If you gas and your lights are in jeopardy of being cut off, that information is reported on your credit. If you need to move or you’re buying a home it just affects everything. – Sunflower

I got a ticket when I was nineteen, twenty, and that ticket kind of snowballed into this whole long thing of like, basically like a huge mountain of debt in terms of that, that I was stuck up under for like ten years, or so. – Tom

I believe in privacy, but I don’t think there’s much I can do to protect it. We spoke to people who desire and care about privacy, but who feel like they have no choice but to give up information. From the minute you are registered at birth to the streets you roam to the everyday transactions in which you engage—our interviewees talked about pervasive data collection that they experience and the frustration that creates.

Oh, God, I don’t even—yeah, I just feel like if I’m going to have a bank account, if I’m going to register my car, if I’m going to have healthcare, I just don’t even—I’ve sort of given up on trying to protect privacy. – Anonymous (Detroit)

I mean your face is not even your own anymore. Your face is being captured by cameras. – Da Hive

They’re dictator. Because you sign that certificate that allows them to do that; that birth certificate allows them dictatorship. – Sean Michaels

I really believe that every button that is pushed collects something about you. – Bebop

My identity plays a role in how data systems treat me. By and large, Detroiters felt that race and economic status play a role in their interactions with data-driven systems.

I feel like my identity is inseparable from my digital presence. – Anonymous (Detroit)

I truly believe that who you are, what you look like, your identity is your digital footprint. – Bebop

We’ve never seen, no culture or group of people on the face of the earth have seen as much monitoring and as much lack of privacy that we have experienced in the last 20 years. Or even 15 years since 9/11. It’s really important that we know the old saying giving up your freedom for security. – Da Hive

I’m often concerned how my orientation will play a role in someone denying me of my liberty at some point in the future. – Justice Black
Oh, goodness, identity, right, right. Yeah, that identifier helped me become a dataset for a further dataset of receiving state assistance, but by a state that created that system where I needed that when if you could’ve just paid me a damn living wage I wouldn’t have to have it. – Terrence

Car insurance. That’s what I’d be penalized with. I didn’t show up in a database for having clean tags and proper insurance. So that sucks. Yeah, which of course is being disproportionately used in a black city and you can talk about history and redlining and how current insurance rates they you know, they instantly go up across the borderline between Detroit and other cities, black, white that whole thing. Yeah, so, that’s ways in which I’ve been penalized. – Tachalla

I am forced to become—and feel—like a number.
People we interviewed spoke about becoming data points in a larger system of services—both commercial and government—that treats them as a statistic as opposed to a human.

I don’t know. I just feel like a number. I don’t even know. – Lola

I know utility companies definitely leverage the need of what you need as a basic tool for survival to capture all of your information, from your Social Security number to your birthday, to your name, which are all primary tools of identity theft. You need those things now to even have utilities. – Renita

We know everything in this system is based on numbers. So, they associate your name with numbers. Whether it’s a credit card, your driver’s license, which now has a metallic strip on the back of it. Every other source of ID that we’re really forced to have now you can’t even get an ID without five pieces of ID. So, to me these are ways of collecting data on you. Whether it is through the DMV. Social Security. All of these entities that are keeping this data and they are cross-referencing this data. So, that they pretty much know everything that you are doing, whether it’s your bank cards, you know. So, they are all tied in. – Luca
Los Angeles

Background
Los Angeles is the third largest metropolitan economy in the world and, in 2017, the annual count of people who are homeless saw a 25% increase. Skid Row, a neighborhood the size of 52 square blocks, has the highest concentration of unhoused individuals in LA County, and an estimated 33% of parolees released in the area settle here.24

In Skid Row, property speculation and development is having drastic and traumatic effects on the unhoused community. The wealth pouring into downtown is pushing out Skid Row residents, as gentrification replaces single residence occupancy (SRO) units with live/work lofts. In 2015, the city re-regulated “streets sweeps,” classifying, all but in name, possessions of the unhoused as trash to be cleared.25 A recent study found just 9 usable toilets at night for a street-based population of almost 2,000, far below United Nations' mandates for human rights and well-being.26

Low-income residents of public housing are also under assault. Jordan Downs is home to one of the country’s oldest public housing projects. In 2017, unemployment affected approximately 50 percent of its adult residents and that average family earnings totaled about $1,250 per month.27 Here, anxiety and harassment plague residents as the city moves forward with $1 billion redevelopment plan that will raze 700 units and replace them with 1,800 mixed income apartments. Jordan Downs’ poorest renters fear being forced out in order to make way for higher earning residents willing to pay market rate for new housing.28


Nickerson Gardens, and Imperial Courts, with surveillance cameras. More recently, Los Angeles Police Department partnered with a CIA-backed company on the forefront of predictive policing and deployment of facial recognition software on parts of its vast CCTV network to search for “matches” to a closely guarded and problematic gang database. Data mining on an unprecedented scale is now being utilized in the name of fraud detection and benefits management for government services.

Power Not Paranoia
As marginalized communities push back—such as a drive for Skid Row to have basic and immediate needs met without criminalization, and residents in Jordan Downs organize to keep their housing with dignity, health, safety, and environmental concerns met through the Human Right to Housing Collective—our work in Los Angeles emerges against the backdrop of gross inequalities and considers resistance to surveillance, whether by police or other collaborating state actors such as the Department of Housing and Urban Development. The Angelinos with whom we spoke entered into conversation about data collection and data-driven systems by reflecting on housing and the interplay between data and housing authorities, law enforcement, commercial actors, and more. Across our 50 interviews, people honed in on the exacting toll of a perpetual state of being watched and counted to the detriment of human dignity and human relationships. Angelinos want to be seen and heard not watched, and they shared experiences from the impacts of navigating a culture of surveillance and control through a range of systems that manage human needs and rights.

Some themes that have emerged:

Data is a power relationship.
Data collection often diminishes the agency and limits the self-determination of targeted individuals and communities. Digital profiles and statistical risk models in social services, child welfare, law enforcement, and housing replace the full, collective stories of our lives with decontextualized, ahistorical, and individualized data. The abstraction of our experience and full humanity into categories, types, and ratings is a form of dehumanization, and the process can be deeply traumatizing.

In our conversations with people in Los Angeles, we learned data collection and data-driven systems represented unequal power dynamics in their lives. People described being in various situations of control and of having to give up one human right for another. These processes and systems curtail people’s movement and interfere with people’s ability to be free, agents of

their own destinies. People shared stories of feeling the weight of the institutions—primarily law enforcement and social services—that assert their authority and create and maintain hierarchies: data controllers on high and data “subjects” on low, seen as a scourge or less than. 

*I’m free in physical terms, but I wear a shackle around my ankle, so they know where I am, the places I go to, where I spend time, what places I’ve visited, so having that shackle is like having a spy over my shoulder, on top of me all the time, my whole life. Given that I need to wait for my immigration status to be solved, my political asylum case sets many restrictions regarding which services I need and can access, health services, housing, that I could acquire. They set restrictions because one of the conditions to my freedom is not becoming a burden to the state, according to them. But rather, they don’t want me to be a burden but they don’t give me a work permit either. They don’t want me to be a burden but I’m… I can’t travel to other states to be able to broaden my horizons and my job opportunities. They don’t allow me to leave the state because if I leave with this shackle on, it sends them a warning and that would immediately mean that they send me back to jail.* – Valeria

*Data systems are a set-up.*
Our interviewees understand the collection, storage, sharing, and analysis of data as part of a looping cycle of injustice that results in diversion from shared public resources, surveillance of families and communities, and violations of basic human rights. Connected to the experience of power and powerlessness, the theme of “set-up” concerns the ways in which data collection and data-driven systems often purport to help but neglect and fail Angelinos. Interviewees described these set-ups as “traps” or moments in their lives of being forced or cornered into making decisions where human rights and needs are on a chopping board. When using social services to meet basic needs or expecting that a 9-1-1 call in an emergency will bring health and/or safety support into their homes or communities, our interviewees spoke about systems that confuse, stigmatize, divert, repel, or harm. These systems—or the data they require—give people the impression of helping, but they achieve the opposite. They ask or collect, but rarely give, and that leads to mistrust, disengagement, or avoidance. Furthermore, systems perpetuate violent cycles when they are designed to harm, criminalize, maintain forced engagement.

*I believe that housing is a trap door. I believe where this system was actually set up in order to aid and assist people, that that process has been lost. I believe that this was supposed to be almost as a stepping stone as you begin to get yourself together this was supposed to be a way for you to be able to save and maybe acquire the things that you would need for the next step. Unfortunately it’s not like that. Because if you make any more you can’t save any more to move anywhere because you can make anymore, they want more. So it’s not actually a helping process. It’s more like a hindering process. It’s keeping you exactly where you are, in need of them at all times… We have what’s called an annual review where every year even though we’ve applied to be here it’s*
almost like you have to apply and reassure them that you are poor and doing bad in order to stay here. So it’s not actually made to help you do any better. It’s actually made to keep you right where you are. – Mika

Data-driven systems tear me, my family, and my community apart.
Interviewees describe the effects of powerful, unequal data collection processes as an emotional, psychological, and physical toll, with traumatizing effects. In the context of struggle between Los Angeles’ most marginalized residents and institutions that claim but do not provide the safety or support they advertise, wrong labels, misclassification, and misinterpretation of data profiles are life-changing events, such as the separation of children from their parents.

Junior: Ever since I was a child, I've been running from them [law enforcement] because they took me away from my mom. They would come to our house and try to get me. They would come and get me. I’d run from them because I didn’t want them to take me away from my mom.
Mariella: Were they trying to separate you from your mom?
Junior: Yeah.
Mariella: Like Child Protective Services?
Junior: Yeah. Maybe I probably would have went to a good family or something, but I didn’t want to get taken away from her.
Mariella: Yeah, of course. I hear you. Did they take you away?
Junior: Yeah. They took me to a foster home.
Mariella: They did.
Junior: The first day I left. I came back. It was in Palm Springs. I hitchhiked all the way back over here.
Mariella: Wow! How old were you, if it’s okay to ask?
Junior: About eight or nine… I don’t even know how I made it. It was crazy. It worked out…I had to jump down the wall. It was a two-story building because we were on the top floor, literally. Then I came back over here and I was happy to see her…Then they took her and then she got busted and she went to prison for like four or five years. It was all chaos. I got into the neighborhood.

Data collection and data-driven systems feed into a culture of fear and suspicion.
Pervasive and comprehensive surveillance by law enforcement is front and center for our interviewees, and their tactics of data collection and use of data-driven systems connect to the experience of over-policing, feeling fearful of being watched and profiled as a suspicious or a person of interest.

In my experience, even if you don’t want to interact with them, law enforcement will find ways to stop you and collect your data. – Janet
Because if we go and request our information, since our papers are there with Immigration, we are scared that now, that this president is in office, it may harm us in some way.

Everything you do in this country, good or bad, it’s used against you. Does it have an impact on your family? Of course it does! A very negative impact. Those who suffer most are always the children. What are we creating? Panic, fear, sadness. – Guadalupe

Data systems write me off for being poor.
Our interviewees find that day in and day out data-driven systems—and sometimes the people behind them—treat them poorly for being poor. Data collection and data-driven systems leave them feeling exposed, as if asking for help is something to be ashamed of.

So I realized that here in the United States, the people who are poor have no systems set up for them to get out of poverty. On the contrary, they are… The moment you are poor, you enter into a maze. …[I need a] system that helps makes you feel like a human being, right? …[A] system with which I work together and not one that saves me or rescues me from anything, because I don’t need for anyone to rescue me or save me. – Marco

Harmful systems…try to separate. “OK, he’s poor, he’s rich.” You are worth more because you are rich; you are worth less because you are poor. – Guadalupe

I want to be seen, not watched, and heard, not harmed.
In Los Angeles, we heard our interviewees differentiate between helpful and harmful systems. The primary sentiment focuses on a human element: in the myriad points of contact that people have with different systems of collection, they desire a respectful interactions where people hear communities’ needs and systems help them rather than punish them for trying to meet their needs. Angelinos want systems to recognize the contexts that shaped their current trajectories and the opportunities that lay before them, rather than systems that categorize them or put them in box.

I think personal information is interesting to think about. Because a lot of our personal information in kind of the spirit of this project does not refer to the information like our soul transformation that occurred or like how it impacted us when a grandparent died. That’s a deep personal information, right? But so often I remember reading when I was maybe as young as 13, maybe older… that Google is actually able to identify you off of your age and birthdate and that is actually a unique identifying thing. I don’t know if I am remembering that correctly, but I do remember it was three pieces of information that felt very actually impersonal to me, like your birthday, your age, where you live. That is enough to be a unique identifier. – Opulence
We have solutions and strategies to keep us human.
Despite feeling tracked and trapped by data collection, interviewees have shared innovative strategies for survival and self-defense. They have talked about blocking, avoiding data collection, expungement, FOIA requests of their records, and building alternative communication systems that support human dignity and self-determination. They offer compelling policy prescriptions: minimize the amount of data that is collected, for example, or use a level of data privacy common to healthcare in other settings.
Our Data Bodies: Commonalities Among Us

In the process of analyzing our interviews, we have come to understand and define data bodies as follows:

Our data bodies are discrete parts of our whole selves that are collected, stored in databases, the cloud, and other spaces of digitally networked flows, and used to make decisions or determinations about us. They are a manifestation of our relationships with our communities and institutions, including institutions of privilege, oppression, and domination.

This definition flows from what we are hearing about people’s desire for human relationships or connections and for human connection that involve mutual recognition and respect. The themes we hear across the three cities point to the hardships and violence our interviewees experience as data bodies.

Predatory data-driven systems routinely hold us back and prevent us from meeting basic needs.

Interviewees express feelings of vulnerability in being exposed to systems they experience as predatory. When applying to jobs, browsing the internet, signing up for social services, filling out forms, Charlotteans, Detroitors, and Angelinos we spoke with share experiences of being preyed upon, hounded, or harassed. They feel at risk to those who ask for their information. Annoyance is part of the equation, but so are real financial impacts.

Just like those telemarketers be calling. As soon as they call, I hang up. “I’m called to reference on your credit card.” “I don’t own a credit card. How do you get my number?” Then they got one that say you can block them, and they still call back. I don’t understand how they get it if I’m blocking you and you still call back two or three days later. I don’t understand that… Same number. One talking about you done won a trip to Miami and send them $700 Yeah, right. Picture that… With that information, I think they scam it. – J (Charlotte)

Since I’ve gotten on Medicaid. So then I got an Obama phone, and the first thing I noticed is that I’m getting calls all the time from credit card companies… [A]nd then also, what I was told was the reason why—the economic justification for the free Obama phone for people on Medicaid is so that they keep their doctors’ appointments. Isn’t that creepy? – Anonymous (Detroit)

Amy Black (Los Angeles): I’m going to say hindrance would be when they popping up all those “Find your loan, fix your credit, check you credit for free, all you need is a small five second… and put your email and put your birthday.” But then I tell you, all they need is what? Sometimes just your birthday. See so that could be a hindrance because I remember one time I did apply for a loan
on the internet…

Mariella: Were you looking for it or did it pop up?

Amy: No, it just… something that’s either in your email or on Facebook says, “Hey, we can do this with you. If you’re a business owner or you’re going to school whatever put this here you’ll find out if you’re approved in five minutes.”

So I’m going to see if I can get approved in five minutes, and what I got in five minutes was a phone call saying that I own them money and they didn’t even gave me no money. If I tell you, the guy was calling me, calling me, calling me, calling me… [A]t the end of the day I was getting harassed like crazy, and I never got no money.

Credit scores are part of people’s account of predatory data-driven systems and play a big role in keeping people down. Over and again, our interviewees mentioned credit being used in job and housing applications to make unfair interpretations of who they are.

Debra (Charlotte): The credit offers from Credit Karma, right, from Credit Karma. When you sign up for Credit Karma to view your credit report, they do different credit card. Not so much commercials, but advertisements will pop up. They’ll have a list. You would be a good candidate to get this if you’re trying to rebuild or anything of that nature. That’s probably where, now that I’m thinking about it. Yeah.

Tamika: Credit Karma is for tracking your credit.

Debra: Tracking your credit. You’re checking your credit report, seeing if anything is matching. To see if everything is matched up… Then they still put the advertisements in there. They do… They’ll say if you’re trying to rebuild or establish credit…

Tamika: Get in more. Get in debt.

Debra: This will be good for you. Yeah. That’s what they do.

Nowadays, you need credit for almost every single damn thing. They even get your credit for a job, like if you don’t have a good credit score, some jobs will deny you because it makes you think you’re more at risk to steal. It labels you almost like a criminal if your credit is not good. What the fuck does that have to do with you stealing? My integrity is not attached to my credit just because I made a couple of bad decisions and maxed out that credit card doesn’t mean I want to go out stealing and robbing cash registers. It’s just that I’ve fallen on hard times. – Quincy, Charlotte

Knowing your credit, knowing your scores, knowing how much you make, what you buy. So they can target you for giving a loan or not giving a loan. Deciding what you can have or not. – Janet (Los Angeles)

When you go to apply for apartments and they do your credit check, that’s harmful because, see, if you had a 720 of a credit score and every time an apartment company run your credit, you know what they do? It brings down your credit score, so you’ll no longer be a 720, and I think that’s harmful
because these people making you pay for you to destroy your credit. Your $35, $25 fee to tear up your credit. Right. – Amy Black (Los Angeles)

Data security factors into the equation, and a significant number of interviewees talked about identity theft, as well as the lack of support to recover their losses.

I’ve had instances of, what you call this, identity theft and that was real. I ended up even going all the way, having to like bail myself out of jail based on that. Because they went and started a bank account and things like that. So that went into the system and then got me into having warrants out for my arrest and things like that. So that was an instance where that was in the data system where somebody used my name and took all of that. So it was a long time for me to work my way out of that whole situation... [E]ven when I thought that I’d handled everything, it was still like a last thing that I hadn’t been that I didn’t know about and it was still there. There was still a warrant out, because it was somewhere else they went and used checks to write bad checks with my name. – Brenda (Detroit)

My identity was stolen twice already... Once, they asked for a loan from the bank and ended up owing almost 20,000. And the other time, my permit, my social security, everything was stolen from my house... [I]n fact, the Bank of America manager, I was telling her “why am I owing so much, if I’m not withdrawing money.” Back then I was getting child support. I had three jobs, and I didn’t need to withdraw money from the bank. And the papers arrived. And once it arrived, [a child’s] dad was there, and he said that I owed more than 10,000... And I did go to the police. [And] I went to Housing and told them what had happened... And the truth is that I went bankrupt. And I had to pay I can’t remember 1,500 or 2,000. – Evelyn (Los Angeles)

Data-driven systems unfairly divert us from resources we are entitled to and need to survive.

Related to predatory systems, most our interviewees feel that commercial and governmental data systems block them from accessing the resources and relationships that they need to survive and thrive. For Charlotteans, Detroitters, and Angelinos, online applications, intrusive data collection, and digital tracking divert them from accessing basic human needs such as jobs, education, housing, food, and social services. This diversion is accomplished through various means: policies block new migrants and returning citizens from accessing their human rights; needlessly complex systems create bureaucratic hurdles to benefits; disproportionate scrutiny makes families feel unsafe and produces stigma and shame.

If you’re a felon, you’re not eligible to receive any benefits. That’s that. – Code Blue (Charlotte)

The Michigan Department of Health and Human Services...the only thing that makes [their data systems] helpful at all is that sometimes it’s the only way you
can get connected to them. I finally realized that I could maybe email my caseworker. They don’t give you the full email address. You’ve got to figure out, okay, if they say, “A. Dickerson,” that’s the only information they give you. They leave you to figure out, “Well I guess @michigan.gov, dot whatever,” and see if that works... [T]hey’re holding all of these important chips and all of this information, and it’s difficult so often to interact with that and find out what that means. ... [T]alk about a brain buster. – ODB (Detroit)

So, knowing that this electronic system that we live in has basically got us separated from the water that we need to swim towards in order to live, we’re all struggling on the sands of the beach, trying to get back to the water. – General Jeff (Los Angeles)

This dynamic of diversion is shaped by applicants’ inadequate access to online tools, and intensified when they feel that they have to release very sensitive or stigmatizing information about themselves. Information imbalances lie at the center of this process. Interviewees feel that they are hypervisible: they have to share all kinds of personal information about themselves, but this kind of data is not what they need to meet their basic human needs. Rather than the two-way, reciprocal relationship of seeing and being seen, they feel closed and secretive state agencies or corporations treat them like an “open book,” leaving them vulnerable and insecure. This kind of one-way scrutiny means that every move they make feels under investigation, but simple information that would dramatically improve their lives is hard to find. This suggested to many of them that data-driven systems serve more to reinforce existing power relationships, rather than to disrupt or equalize them.

Data collection feels extractive and takes a serious emotional toll on us.

Our research participants spoke at length about feeling uneasy, frustrated, overwhelmed, frightened, and angered by their experiences with data collection. When interviewees felt that their data trails were being used to single them out for scrutiny or punishment, negativity towards data-driven systems intensified. Similarly, they felt especially intense when institutions that our interviewees already found alienating or stigmatizing, including law enforcement, the medical system, public housing, and the public assistance office, were the ones collecting the data. When they lack control over how their data is used, digital scrutiny feels most paralyzing and dangerous to them.

Tamika: How does this, like the sharing of this information in general make you feel?
Assata (Charlotte): Child, stressful. And like a damn, like a, like a, like it just looks like you’re plagued. Like with the, what did they used to say back in the day, a red letter or whatever? Like you are plagued. Like I feel like it’s like some...
Tamika: Like you are like an outcast?
Assata: Yeah, that. Like an outcast, and it’s something that can’t escape.
Tamika: Okay. Like it’s following you.
Assata: Yeah, like it follows me.

Should I give them information that allows me to get this healthcare that is subsidized, not free, and be a part of a health system that does not yield positive results? I struggled with giving them motherfuckers my information. Still do because I have a serious health challenge, but I don’t want to give the information to a system that harms, that is not something that I’m in alignment with. ... [I feel] pissed off. ... I have a problem with being a number and a statistic. That alone is not a good feeling. – Terrence (Detroit)

[The housing authority] placed us in a very, very, very difficult situation. We’re scared when we go there; we go into that office. Thinking: “What are they going to look for, what are we going to say, what are we going to do?” ... If my cousin comes to live here to be happy, to share, or got out of prison, they will be investigating. It stops you in your tracks. Every human being has the chance to be happy, ... to be part of society without being scared or feeling guilty about moving forward. And [criminal records checks are] what stops us here. That because you did something that cannot be corrected for some time, but you’ve been through the process, you made up for it... [and housing says] “If you’re going to come and live here, I will check your criminal record.” That puts the human being down, so that he won’t want to move forward.” No, they’ll be checking up on me.” So it’s like a dagger in your heart. – Angélica (Los Angeles)

Many of our research participants felt like the process of data collection, analysis, and sharing is dehumanizing. They felt that their experiences were being extracted and abstracted, leaving a decontextualized data body that is less complex than their lived experience and understanding of themselves. Our participants feel boxed in—or boxed out—by the limited opportunities to self-define in data-based life. What’s more, they feel that technologies, people, and other entities are manipulating their narratives for their own ends, especially to criminalize them or their communities. They reminded us that their stories, and their lives, are richer, fuller, and more complex than any data profile could ever capture.

You don’t know my situation. You don’t know my struggle. You don’t even know where I come from. Don’t judge a book by its cover. That's my motto. You can’t look at me and say, “You don’t need nothing. What are you doing here?” ...That’s how I feel going to ask for DSF help or Social Services help, food stamps, EBT. Go in there, [they] look at [you], “You’re asking for EBT?” – Lamont (Charlotte)

They don’t really have any real idea of who I am and what I am...They’re probably...looking up my name and seeing what I’ve been connected to. If they have some kind of number that identifies me, that number can tell them a lot about me, but it might not tell them why I’m doing what I’m doing.” – Sam (Detroit)
Being in a foster home, you are your mother’s child, with that Social Security, birthday, and name. That’s all you are... [a] Social Security number. Now, because I’m going to a foster home, the police are being called, so now my name is in the police system... Now you’re easily to be criminalized because you’re already in the system of the database of the police. So from the police now they’re calling social workers, which is the DCFS, Department of Children and Family Services. ... Now you went from momma’s belly to the police car or the police data, now DCFS data, now DCFS data has got to go through their process and then now we’re going into someone’s home. ... It’s all a chain of command. Everybody is getting paid off of you, basically. – Amy Black (Los Angeles)

The hurt and the harms of data-driven systems connect to past systems of discrimination and exploitation against members of marginalized communities.

People feel targeted and profiled because of their race or ethnicity, economic status or class identity, age, gender, sexual identity, housing status, criminal record, or any combination thereof.

Niggie (Charlotte): I think because my identities are so visible they make me stand out more. In terms of data collection, data typically collects more information on any type of like thing it determines is an outlier or like extra. So a queer black person is definitely going to be hypervisible. I am rather highly visible to a surveillance system. I think that sucks a little bit. Like if I was a white man I could be a little more...

Tamika: Fluid?
Niggie: Yeah. You know what I’m saying?
Tamika: How has that impacted you?
Niggie: I mean I think it definitely helps aid in like who they choose to arrest. I’ve definitely been arrested. I think many times because of those identities. And because of the visibility that those identities bring.

I was refused to vote. I couldn’t vote because my gender on my ID didn’t match. – Freida (Detroit)

The sentiment that racial difference marks people in different ways with different consequences plays out in unmistakable ways during conversation about data collection and data-driven systems.

Like I said, as being identified through a number, so that number tells them who I am. I dated a white woman, and she was Italian. I ain’t never had a school loan. I always paid off my houses and my cars. I never went into default. She went into default. She had a school loan that went into default, but her credit always stayed better than mine. I was always wondering, “How does your shit stay better than mine? I paying my bills. You ain’t paying your bills. – Sean Michaels (Detroit)
I think this type of systems in place is very detrimental to human needs because of what color your skin is that bases it on the type of services and the way you’re going to be treated by the public systems such as mental health, health services, dental services, housing, services... Like me, even though I am a Latino, but I’m more of a English-Latino. And you wouldn’t think that because my name is Amy Black. You might even think I was a black girl, right? But I’m not. When see the name Amy black on the paper they’re going to think what? That I’m a black person, but when they see me they’re going to say, “The name don’t fit the person.” Our interviewees connect these disparities to a longer history of mistreatment. – Amy Black (Los Angeles)

Take for instance, I served in the same war as my white counterpart, but it's much easier for them to get benefits. We don’t have to go through as much—I mean, we have to go through more than they have to go through to get benefits. It’s almost like we have to—sometimes it has to be an act of Congress to get the benefits that were due to us. It’s always been that way, even before World War II. – Hatman (Los Angeles)

Our strategies for self-defense and survival keep us connected and feeling whole.

Despite feeling stressed, sad, and overwhelmed by digital scrutiny, dehumanized by data profiling and surveillance, and diverted from accessing their basic human needs, our interviewees still work to change their lives and share their stories. Scholars and policy-makers write that people feel a sense of resignation in the face of ubiquitous data collection. We found that this was often true. Many of our interviewees described feeling that new data-based systems are inevitable, and that their communities will most likely bear a disproportionate share of their negative consequences.

But people aren’t ready to acquiesce or give up their power.

I don’t think I’ve surrendered to the fact that they’re just going to do what they’re going to do. – Sam (Detroit)

It is important sometimes for us to also take stock and to recognize that even if we are the poorest and the least protected, even if we have made the worst mistakes, we have the right, the opportunity to love ourselves. Because we also have to. We have to keep our spirits up. – Marco (Los Angeles)

I’m going to say that’s why this is important, this work is important. That’s why it’s important we talk about it, important that I do something about it, so that we can bring exposure to the wrongs. – Kristie (Charlotte)

In each of the three cities, our interviewees confront and challenge predatory data-driven systems or invasive data collection to feel whole again and to experience safety and belonging with others. On balance, these strategies include obscuring data trails about themselves, keeping track of how they’re tracked, and setting the record straight. Here, the record refers to things like credit scores, arrests versus convictions, outdated files with Child Protective
Services, and property classifications. These strategies also involve reestablishing bonds with others and with the land, such as through eating local, healthy food, sharing food with others, or being “off the grid.”

**Our policies, priorities, and visions for the future focus on just models of governance, economics, and criminal justice, and on guarantees for our human rights.**

People that we spoke with want to see communities governed, including in ways that are inclusive to all.

*I would educate the younger folks so that it would be a means on how to not fall into some of the other traps the older folks have fallen into by just being out here and not really paying attention to policies. Because policies are in place, but do you understand the policies?* – Sunflower (Detroit)

*Get rid of emergency management and the march toward austerity, the march towards small government, because the smaller our government gets, the harder to access it gets.* – Lilith (Detroit)

*I think that the information that would be very important not to focus on how the rich people live. It would be more important to focus on how the minority lives. To include them in each of the decisions that the government makes.* – Guadalupe (Los Angeles)

*[T]hose people who are infringing on our rights, those people who are basically, you know, holding us in slavery and bondage. ... I would just change the system of white nationalism, and I would just get rid of that whole system.* – Bonnie (Charlotte)

At the same time, our research participants talk about creating a culture of sharing and empathy.

*I would establish the return of the commons. I mean, this is the stewardship of the land, the water, the air.* – Da Hive (Detroit)

*Everybody would be happy. Everything would be green. Flowers. It would be so beautiful. People would be like, “Oh yeah, come over and eat today.” ...People wouldn’t suffer.* – Rita (Los Angeles)

*[I]f we killed capitalism and created something that was for all of us. We could do that with the data and it would be a good thing. We would have to collect data. But we would be collecting it and we wouldn’t be using it against each other.* – Jean (Detroit)

Our interviewees want changes in data systems that improve criminal justice systems and transform the carceral state.

*I think that there should be some transparency into data... Especially in North Carolina with the inability for us to have our own discovery prior to applying for*
it or prior to our trials, I think that it really leaves us in this very ambiguous spot where we don’t know what’s being said about us. – Chloe (Charlotte)

A lot of these jobs require a clean driving record, and for the last eight, nine, ten years I’ve been trying to get my driver’s license back. I have to pay $500 reinstatement, then I have to do this $100 assessment just to get my license back, never mind actually drive a car. ... Jobs should hire you so that way you can clean up your record. That way you should drive instead of saying no, you can’t drive. Have some kind of work incentive to pay off your fine, pay off what you owe the DMV instead of just having to pay them money. Have a swing-door system. Come in, do X man-hours, and we’ll give you back your license. – Johnny D (Charlotte)

There should be agreements between employers and ex-offenders about releasing information. With any reentry programs or any halfway houses, there should be some kind of agreement about release of information. That allows the community to remain safe but at the same time the person not to be punished. – Jack (Charlotte)

From communication to privacy, from shelter and rest to food and water, and more, our interviewees want to see their basic human rights respected.

Accessibility to the internet is just as important as other basic human rights, because it’s a way for people to provide means for their family or to find means for their family. – Lola (Detroit)

You have the right to not give out your information if someone asks, even on a form, you should have a “Not applicable” button... You do not have the right to sell my information without my knowledge. Hell, if you sell my information, give me a cut, bitch. Throw me some cash. We copyright books and media, why can’t we copyright our own damn information? – Quincy (Charlotte)

Nobody’s water need get turned off. We got enough water for everybody. – Maria (Detroit)

Either give motherfuckers a living wage, or create conditions where we don’t need capital and capitalism. – Terrence (Detroit)

[We] don’t ask for anything more than a place to keep on living and where we can feel ok to have, say, a minimum wage, to help us buy clothes for our little girl, or pay for school, so they can be better. – Angélica (Los Angeles)
Our Reflections and Future

Our next steps in this project include creating a final report that captures our findings in all three cities and sharing them out to a broader audience. As always, we will lift the everyday experiences of marginalized people in our communities. We also want to remain visionary, and to contribute to a body of knowledge and practice that will help our communities be safe, just, and abundant in the digital age. Systems can be created for good and can function as communication that sustain human relationships and support our lives. As we move forward, we will continue to highlight alternatives focused on sustaining healthy communities.

The ODB Project team believes that issues of data justice are urgent and crucial to our movements. We do not underestimate the scope of the challenges before us. But three years of working side-by-side with our communities, and hearing their stories, have also left us with a profound sense of gratitude and hope. Our interviewees talked about self-defense and community survival, not surrender. They shared visions for a future of abundance, justice, and equity. They demand agency and self-determination in their own lives, and they believe that change is possible.

We captured this dynamic in framework suggested by the Stop LAPD Spying Coalition, an ODB research team partner: “Power, not Paranoia.” For us, “Power, not Paranoia” highlights the resources and resilience of our host communities. It acknowledges that people closest to problems have the best solutions for them. And it underscores our commitment to reporting the reality of digital scrutiny on the ground while providing opportunities to build power, nurture relationships, and create capacity for long-term visionary change.

We hope you will join with us in this vital work.

For updates and to find ways to connect, join us at https://www.odbproject.org/.