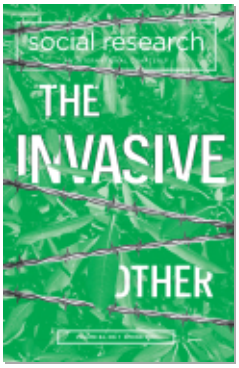
Privacy under Surveillance Capitalism

Jacob Silverman



Social Research: An International Quarterly, Volume 84, Number 1, Spring 2017, pp. 147-164 (Article)

Published by Johns Hopkins University Press

Jacob Silverman

Privacy under Surveillance Capitalism

IN 1982, THE NATIONAL SCIENCE FOUNDATION PUBLISHED A REPORT ABOUT the prospects for teletext and videotex in the United States. The report, written by a RAND Corporation–affiliated think tank known as the Institute for the Future, examined the market potential and public-policy issues of these information-services technologies, which at the time were just two protocols among many competing to be the future of networked communications. (The report, "Teletext and Videotex in the United States," discusses "packet switching," but the word "Internet" does not appear in its 300-plus pages.) Envisioning a range of possibilities for teletext and videotex that spanned entertainment, news, shopping, banking, and other information services, the report also warned that "at the same time that these systems will bring a greatly increased flow of information and services into the home, they will also carry a stream of information out of the home about the preferences and behavior of its occupants" (Adler et al. 1982).

Teletext and videotex may have been banished to the dustbin of technological history, yet the report's warning proved prophetic. But what may have been a cause for alarm to some has proven to be an immense commercial opportunity for others, as personal information and behavioral tracking have emerged as major assets in today's surveillance capitalism (Zuboff 2015). A Senate report estimated the US data broker industry to be worth $150 billion per year (US Senate Committee on Commerce 2013). Data and personally identifiable information (PII) are the new extractive commodities of the age. Often compared to oil, data may be a more renewable resource, albeit

at a cost to privacy, autonomy, democratic accountability, consumer choice, and indeed, the environment (in the form of massive energy costs for data centers, e-waste, and the mining of rare minerals).

With the proliferation of networked devices in our homes and on our bodies, our surrounding environments now overflow with sensors and other data producers. Earlier generations saw some forms of governmental and commercial data collection about the home and what goes on in it. Market research, census records, consumer surveys, loyalty cards, credit bureaus, property records—these were common predigital data streams, and many still exist in one form or another. Now the home—and the activities, behaviors, and preferences of those within it—is becoming transparent, as mappable as a city street. Internet of Things (IoT) devices track the comings and goings of a home's occupants. Roomba, the autonomous robot vacuum, maps the rooms it cleans (although it does not transmit the maps it creates anywhere), and future versions will be able to recognize household objects. Researchers have successfully used slight variations in WiFi signal coverage to map the interiors of rooms and the people in them—in other words, to "see" through walls (Condiliffe 2015). Intelligence agencies are able to use the sounds of computers' fans to exfiltrate data from air-gapped machines (Zetter 2016). Law enforcement officials have begun subpoenaing data and records from always-on, always-listening IoT devices, like the Amazon Echo, for use in criminal investigations (Steele 2016). Subtle vibrations of everyday objects can be measured to reconstruct the sounds in a room (Timmer 2014). Some of these techniques are the product of cutting-edge hacks or secret operations by intelligence agencies, but they reflect a growing technological capacity. What may now be the province of a security service or a rogue tech firm will soon enough be commonplace.

The home was never an inviolable site of total privacy. For some children, women, the disabled, the elderly, domestic workers, or those caught in abusive relationships, the home is neither a place of privacy nor comfortable domesticity, but an arena of contentious power relationships. Children are well-practiced at navigating the

shoals of disclosure with their parents—sharing some information, concealing more, demanding a lock on their door, perhaps, or regularly clearing their browser histories. A great deal of subversive behavior in childhood revolves around keeping information secret from parents and avoiding their watchful surveillance.

In the realm of personal privacy and digital technologies, then, the "invasive other" might be best characterized as those forces of power and authority that collect information about us and exert influence over us. The "other" might be one's boss or parents or a distant government overseer, but the means of surveillance and control are mostly embodied in new digital technologies and data-collection schemes. Central to this paradigm is the objectification of a human being into a data source capable of being parsed, scanned, assessed, and monetized by other, invasive interests. A human being becomes subject to an algorithmic gaze, a machine vision that emphasizes market values like productivity, efficiency, profit, and mitigation of risk and liability.

Amidst the profound changes in privacy norms wrought by the advent of digital technologies and cultures, one trend is clear: individuals have been made vastly more transparent, while authorities and corporations have become more opaque. These changes in privacy and surveillance track with growth in the US surveillance state, in the ability of the executive branch to wage undeclared war indefinitely, and in the advent of corporate personhood, which serves as a legal manifestation of a vast expansion of corporate power in all facets of American life. At the same time, individual rights—while lionized in the public discourse of liberty, freedom, and American exceptionalism—have become frighteningly contingent. Rights for voting, free speech, habeas corpus, to consent to searches, and much more are prone to sudden abrogation under laws that reflect a generalized state of emergency. The enforcement of these measures, in turn, is enabled by the institutionalization of mass surveillance, which allows authorities to monitor social media, record phone calls, film public spaces, track vehicle movements, and strictly control passage at bor-

ders with biometric identification. It is now possible for many countries to record virtually all telecommunications and internet traffic within their borders (Villasenor 2011), and the US intelligence community's unofficial mantra of "collect it all" would seem to place it in this class (Nakashima and Warrick 2013).

As these shifts in privacy occur, the home will not become completely transparent, as if lit by klieg lights. The various power relations will not dissolve overnight, nor will all forms of surveillance and data collection be equal. The invasive others will sometimes clash as they reach for their ultimate prize: us. There will be—there are—many privacies, overlapping, intersecting, a cross-hatching of competing data-collection schemes and struggles for consumers' attention. The home, and many of the people and things in it, has been plugged into the tributaries of surveillance capitalism.

The home is also just one context. Thanks to the explosion of social networks, "dataveillance," and networked communications, our once-discrete social contexts are increasingly permeable. The invasive other sees into all aspects of our lives. Many media theorists have turned to the phrase "context collapse" to explain this phenomenon. Essentially, context collapse refers to the dissolution of borders between formerly separate social spaces. Various contexts combine, particularly on social networks, where they are all part of the same informational flux. On Facebook, for instance, one might limit posts to certain people, but by default, one's posts are available to all one's friends (and perhaps the public, too). Your boss, your landlord, your ex, your closest friends, and people who you might have long forgotten about, old online acquaintances who have lapsed into invisibility, buried in your feed—all might see your posts. The change in audience composition in turn affects how we present ourselves, how we write about ourselves, and what we might think constitutes privacy. It is not so easy to calibrate our behavior or expressions for our audience or even to know who our audience is.

This emerging awareness of collapsed contexts could spur a reactionary stance, a sense that one is too exposed. (The often-cited

Dunbar's number purports to represent the number of people that one can maintain an active social network with; the number varies but is often pegged at around 150.) It might be easy, then, to lapse into default forms and gestures—to simply retweet popular memes or cultivate a manicured Instagram page in which nothing seems askew and every filter is carefully applied. On Facebook, you might only share mainstream news articles that flatter the views of your friends. This homogenization of style is an act of public relations. It shows that one fits in, isn't too distinctive, is abreast of the viral zeitgeist. It is also, potentially, the death of the personal. But that's what happens when contexts collapse in upon one another. The audience becomes too broad, the glare of public scrutiny too apparent. Who would want to say the same thing to his grandfather as to his old college roommate? And that is only the fear of a minor social faux pas, rather than the greater fears that often accompany online overexposure: job loss, verbal abuse, threats, a sense of vulnerability, a permanent data trail, a feeling that anyone could be watching.

In April 2016, Facebook found itself facing precisely this problem. A representative of the social network, speaking with a Bloomberg News reporter, claimed that the company was concerned about context collapse. While people were sharing just as much content, they were posting less information of a personal nature and more about news stories and public events. As friend lists grew, people seemed less willing to be open about themselves. "Personal sharing has shifted to smaller audiences on Snapchat, Facebook's Instagram and other messaging services," the article noted (Frier 2016).

Facebook had calculated the relative decline in personal sharing at 21 percent year-over-year (Frier 2016). This number revealed a great deal about Facebook's strategy and self-image. The statistic is presented exactly as revenues or profits might be, as a percentage relative to the previous year. This metric is clearly something that Facebook values, and it reflects the growing relationship between a company's ability to gather PII and its bottom line. Personal data, behavior, preferences, memories, responses to events, feelings, loca-

tions—these intimate and private bits of information constitute the larger stratum of information that most large tech companies, and certainly all large social platforms, mine for profit. While Facebook is expert at tracking and surveilling its users, it still depends on voluntary disclosures of personal information, on users seeing Facebook as a place in which they can retain a sense of privacy and safety so as to feel comfortable airing out their personal lives. (The invasive other must be hidden from view, even as it monitors everything users do.) This personal information is essential for Facebook's ad-targeting efforts, which seek to match users with advertisements that reflect their interests and concerns. Context collapse describes the company's anxiety that its users may not feel so forthcoming about sharing and that this decline in personal sharing will, in turn, lead to less effectively targeted ads.

At the center of the blast crater left by context collapse stands the smartphone. Here is where all social contexts and data converge, and are made mobile. The smartphone is the universal prosthesis, a veritable Star Trek tricorder or Swiss army knife of omni-utility. It is, increasingly, the vehicle through which many people communicate, entertain themselves, and find their way in the world. It is a constant hub of personally revealing activity, which is why metadata from mobile devices is as important to police officers looking to solve a murder as to a marketer looking to serve up location-dependent ads. And like the Star Trek tricorder, which crew members often jerry-rigged to unlock some new capability in a moment of need, the smartphone is prone to feature creep. New uses are found for its sensors, with more added each product cycle. Smartphones can count steps, track sleep patterns, and perform other kinds of bio-behavioral monitoring, but these and other capabilities were mostly introduced later by independent app-makers and tinkerers who realized that the device's gyroscopes and sensors could be repurposed to track all manner of activity.

Besides its role as the universal tool, the smartphone is a constant companion, a salve against loneliness. With its notifications and

persistent demands for our attention, it asks to be tended to, like a pet. In a time of precarity, the smartphone, or just the Internet writ large, promises something new, a way out of our current situation. There is always something novel to consume. Simply refresh the feed—the archetypal interface of digital life, an endlessly scrolling, algorithmically sorted information-scape; sorted because it's overwhelming, because consumers can't be trusted to handle the informational load coming at them, and because of one of the few ironclad rules of surveillance capitalism: it serves advertisers. Everything comes through a feed: jobs, news, relationships, Uber rides, photos, Amber alerts, trivial entertainments and diversions that help get us through the small interstitial periods while waiting in line or riding the bus. These moments, once spent idly daydreaming perhaps (if one wishes to romanticize), are now ripe moments for information processing and data production.

The smartphone is a personalized surveillance machine, producing ever more granular reports about its user. This individualized tendency—so important to advertisers who wish to target consumers on a personal level with customized appeals—reflects how digital surveillance and data analytics are perfect neoliberal technologies, allowing markets to be the handmaidens of digitization. As we digitize more of the world, we measure and define more of it in terms of specialized metrics. And as so much is tracked and measured, it can be monetized and marketized and subjected to the larger forces of financial capitalism. Prices for anything from taxis to insurance can fluctuate in real time, reflecting ostensibly computer-derived calculations about supply, demand, risk, or market efficiency. Of course, these shifts in pricing may be motivated just as much by a desire to maximize revenue, to see how much a consumer is willing to pay and whether he can be made to surrender to variable pricing schemes over which he has no control. That is why, for instance, online retailers have been experimenting with differential pricing, offering customized prices derived from a customer's personal information. The retailer can point to some dubious promise of personalization or efficiency while padding its margins.

Amazon has indicated that variable pricing structures may be tested in some of its brick-and-mortar stores, which serve—in an ironic reversal of the classic analog-to-digital shift—as veritable laboratories for bringing digital surveillance technologies into the physical world. In these stores, a customer's smartphone and faceprint would identify him, allowing the store's systems to offer different prices for each item for each customer (displayed on a small screen or on the user's own device—to preserve his "privacy," perhaps). And with much of a store's functions automated—McDonald's, for example, is investing heavily in replacing cashier workers with digital kiosks—that other holy grail of surveillance capitalism may take center stage: efficiency. This is one of the fundamental, almost tautological principles underpinning data-driven information technologies. Efficiency justifies everything else. It reflects the perfection of a system and the elimination of bias, waste, and error, which are lamented as all-too-human phenomena.

Here we brush up against the essentially positivist nature of today's surveillance capitalism, which is characterized by feedback loops, the assumed "neutrality" of algorithms, and the ideological notion that computers carry an inherent authority—i.e., they can never be wrong. The system, with its impressive processing power, its enormous storage capacity, and its multitasking capabilities, is treated as a more neutral arbiter than a human being, for whom efficiency and speed might be less important values than ethics, deliberation, or questioning assumptions. A human store clerk can converse with a customer and make nuanced decisions about how to interact with her, while a digital kiosk is limited to binary decisions based on a crude data profile. A consequence of this kind of thinking is that digital systems incorporate error and bias, like racism, in a self-reinforcing manner for which there are few incentives to provide a fix. Responsibility gets abstracted away, as undesired outcomes are attributed to quirks in the system or some kind of human misunderstanding. Code, from the perspective of a user who has no ability to change it, is law.

Consider the example of predictive policing software, increasingly a preferred tool for forward-thinking metropolitan police departments. Often this software is furnished by private companies that use crime data that may already be the product of unjust, racist, or otherwise politicized policies. A black neighborhood might generate an abundance of crime data (and be designated by the system as high crime) because racist politicians or police commanders have historically subjected these communities to overpolicing and discriminatory treatment. The raw data, however, doesn't see these complexities. That data is then plugged into software that uses proprietary algorithms to perform a threat assessment of a particular house or individual—a determination that might be passed along to an officer in the field. On his way to answer a call, an officer might learn that Joe Steve living at 2666 Elm is "high risk," which may affect his approach to the scene, but he has almost no information about how that determination was reached. More perniciously, the threat assessment may be presented as a quantified metric, as a so-called "threat score" of, say, 85, which implies a degree of mathematical certitude. But this number is largely meaningless, even if the officer knows the range of possible scores. He still doesn't know how the data was collected, or whether it's accurate at all, and he doesn't know how the software reached its decision because its algorithmic decision-making process is a protected commercial secret. The problems extend up the institution's hierarchy, as the police force's management doesn't understand the inner workings of this software because a private company is under no obligation to share that information.

In the same way, we cannot know how Google determines its search results or what factors are influential in how Facebook sorts its news feed. Some outcomes may be adverse, but we can never fully investigate or understand them because they are concealed behind the veil of algorithmic secrecy. A study can then find that Google searches for names commonly thought to be African-American produce ads for bail bondsmen and arrest records—clearly a product of discriminatory thinking—but without greater transparency surrounding Google's

highly sophisticated ad network, it's impossible to know why such searches produce racist ads alongside them (Sweeney 2013).

Digitization, automation, and the parsing of the world through algorithmic systems allow for the swift movement of information and capital. They may even advance a kind of efficiency. But this all proceeds according to an inhumane market logic that elides complexity and, in the name of individual freedom, actually stifles personal privacy and autonomy. We can see, in the predictive policing example, how flawed data becomes legitimized within a larger system that carries the imprimatur of mathematical authority. It also points to an important distinction in varying types of privacy, between an individual's privacy in relation to other individuals, and between an individual's privacy in relation to machines. This latter type, which might be termed "data privacy," concerns what surveillance, data collection, analytics systems, and software know about us. It is the datafied version of oneself, spread between varying networks, databases, and systems of sorting and assessment.

These varying informational selves increasingly dictate access and opportunity in the world—whether one might get a job, or whether one might be investigated by police. But they also exist within a larger framework, where so much data production is machine-to-machine, with no humans in the loop (even if the actual data may describe a person). The financial motive behind digitization is to make the world machine-readable, to provide more processes and behaviors to surveil and digitize, and to use these new streams of information to monetize more of life. But in this welter of information, humans can seem secondary, at least insofar as informational production is concerned. As the artist and writer Trevor Paglen notes, most images now are made by machines to be consumed by other machines. "The fact that digital images are fundamentally machine-readable regardless of a human subject has enormous implications," he writes. "It allows for the automation of vision on an enormous scale and, along with it, the exercise of power on dramatically larger and smaller scales than have ever been possible" (Paglen 2016).

To see this bifurcation of privacy between the personal and the data selves, consider a photo shared on Instagram. A person's decision to stage, capture, and post a photo carries with it implied considerations about who might see it, how she wants to appear, and whether she feels comfortable offering it up for something like public consumption. These are valid and natural privacy concerns, but these fears about one's personal privacy exist in parallel to another process, namely the photo's consumption as a data object. From this perspective, the photo is even more exposed than the person it depicts. The photo is parsed by object and facial recognition programs; marketers scan it to see how their clients' products are appearing; metadata reveals to advertisers where the photo was taken; law enforcement and intelligence agencies run the photo's comments through sentiment-analysis software, looking for illegal activity or signs of radicalization; shady bots appear using the photo as an avatar; untold numbers of computers in data centers and internet hubs around the world chop up the photo and transport it around as packets of information, producing records about its transit in the process. The photo's lifecycle and all the useful information that may be extracted from it extend far beyond the view or control of the person who posted it.

These variations in privacy may lead anyone—from advertisers to police officers—to manipulate people. In short, they know more than you. The process of automation on a vast scale leads to thoughts of what mass-scale coercion, enabled by this flow of data, might look like. Not all forms of suasion are equal. One study found that women were shown lower-paying listings in online job ads—a result of sexism manifesting itself in the ads' decision-making engine (Yachot 2016). Facebook has studied hundreds of thousands of users, without their consent, and found that it can provoke slightly happier or sadder emotions and observe them traveling, as a contagion, through the network (Kramer, Guillory, and Hancock 2014). The invasive other here becomes a pathogen, a vector for inducing the behavioral and emotional responses desired by the network's corporate owners.

Facebook has also, perhaps more nobly, found that encouraging users to vote increases voter turnout (Corbyn 2012). This study, while reflecting a heartening truism about the benefits of civic participation, appears more malevolent if you consider how this knowledge might be repurposed. Could Facebook encourage people in some districts to vote while saying nothing to others? With its vast power to sort the information users see and to prod people toward certain behaviors, could it influence the fate of elections, not to mention specific policies? And would we ever know if it did?

The prospect seems increasingly less fanciful. The election of Donald Trump as president provoked some soul-searching in this regard, with focus landing on the subject of "fake news." Before the election, this was seen as a perverse but mostly harmless internet phenomenon, but it later came to be seen as a major problem, a symptom of a deeply dysfunctional informational and news culture. As much merit as there is to this idea, there is also the necessary caveat that fake news is sometimes a matter of epistemological debate. Some stories or websites or forms of reporting are obviously fiction. Others are more subtly designed to manipulate, reflect a political bias, lie by omission, or otherwise mislead, but they might not be strictly fake. And allegedly "real news" can still produce horrific outcomes—inciting a needless war or demonizing a vulnerable population.

Still, the outcry over fake news reflects, like the criticism over Facebook's contagion study, a concern that network effects can be manipulated to illiberal or harmful ends. (It is also a reminder that calling a communication "viral" describes both a means of transmission and its unmanageable, pathogenic character.) After the election, members of the Trump campaign's previously secret data-mining operation bragged to journalists about their micro-targeting abilities on social media (Lever 2016). Users were targeted with highly personalized ads, direct appeals based on the person's data profile. Whether or not this kind of granular targeting was as successful as its proponents claim, it certainly reflects the greater ambition of using PII data profiles to target and manipulate large populations. And barring

legislative prohibitions against this kind of tactic, tech companies and political campaigns seem to be among their most likely users, particularly as these practices are refined.

One worries what happens when facial-recognition technology improves and proliferates ever further, enabling relative conveniences like Amazon's automated brick-and-mortar stores while ensuring that people can be identified, by a host of unknown actors, wherever they go. One dark scenario is the "Minority Report" option, as in the film where public advertisements, cameras, and sensors scan Tom Cruise's eyes and provide him with personalized offers and ads wherever he goes, with advertising flowing from one interface to another. Much of this technology already exists, and advertisers are focused on tracking users wherever they go, including across devices, and (by closely tracking behaviors) distinguishing between multiple users sharing the same device.

Alarming as these possibilities are, they represent the quid pro quo of personalized digital services: total surveillance. Surveillance remains the preeminent business model of the internet. The possibilities for suasion and influence, for outright manipulation, are now more apparent. But the discourse surrounding these issues remains immature, and all too often policymakers pay tribute to the independence of the information-aware consumer without considering the fundamental role of corporate power. No one wants to think that he is a rube or is subject to manipulation by unseen forces (not least for the paranoia this betrays). But it would be reckless to deny that these kinds of capabilities—the power to observe almost everything someone does, to control what he sees, to push him with alerts, ads, and opportunities—could eventually be leveraged on a large scale. That is precisely what civil libertarians warn against in discussing the dangers of mass government surveillance, and the mass corporate surveillance of public and private life seems no different. These systems are, in the end, deeply intertwined. Private companies sell personal data to government agencies. They depend on federal contracts and lobby for favorable legislation. Intelligence agencies make

backroom deals with telecom giants like AT&T and security firms like RSA. And where deals can't be made, intel agencies hack into internet backbones, pillage databases, and use existing ad networks to surveil web users, turning the ostensibly benign commercial surveillance of web browsing into a covert intelligence-gathering operation. In the larger digital economy, it is hard to disentangle one from the other, especially as personnel increasingly flow from government intelligence agencies and hacking teams to more lucrative opportunities at private cybersecurity firms.

Amidst this array of compromises, ethical disasters, and opportunities for manipulation, how can the surveillance-driven internet economy be opposed? One response is to embark on some program of digital hygiene or security planning. Securitize the self: this is the smart, informed consumer's response. He uses Tor, Signal, and other encrypted, anonymizing products. He opts out of all that he can, prefers open-source software, updates his devices and software frequently. He might use a password manager, get a PGP key, and take other security measures, such as installing alternative operating systems like Tails or Qubes. Gradually, he begins to think like a spy, speaking of attack surfaces, advanced persistent threats, adversaries, opsec, and all other manner of jargon. It is him, alone, against the invasive, pathogenic forces arrayed against him. This kind of clandestine thinking has its place for some—dissidents, journalists, diplomats, artists—but it is largely an indulgent form of spytalk, one that reflects underlying principles of secrecy, vigilance, self-reliance, and suspicion of others. It is also an essentially consumerist and individualist response, which precludes showing much solidarity with a larger public (except in the form of using the same expert-approved encrypted chat apps). The larger result is a vast disparity in privacy conditions and outcomes. Privacy itself becomes a boutique good, affordable to those who know how to navigate this tangled landscape of best practices, firmware updates, threat assessments, cryptographic keybases, and virtual private networks. All this feverish activity also reveals how liminal privacy is, particularly data privacy. A person may succeed in obfuscating his

data trail, in masking his activities from marketers and perhaps even some intelligence agencies. But there is always, it seems, another leak that must be patched, and not all can be. Some major telecoms, for example, install surreptitious "super cookies" that monitor a phone's browsing information and prove near impossible to remove. Verizon sells location data to marketers—something that no Verizon customer can avoid, unless he places his device in a Faraday bag.

When we recognize how much labor is involved with these activities—labor that technology firms may successfully harness for profitable data about user behavior—their insufficiency becomes clearer. So does the inherently reactionary nature of this kind of thinking. By undergoing these regimens of digital hygiene and securitization, we are operating on the terms of surveillance capitalism, fashioning personalized, market-based solutions for the problems of personal privacy and exploitation of PII. While one should not dismiss pragmatic acts like reforming government regulations or empowering the press to report on abuses, we would still be acting within the current paradigm, which fails to acknowledge privacy as a shared, social good, one that benefits everyone, particularly the most vulnerable. Some form of radical change necessitates going beyond tinkering with or challenging surveillance capitalism on its own terms; it will require a dramatic, seemingly unthinkable alternative. In this context, a militant rejection of digital technologies, even a kind of Luddism, is understandable, provided it is foregrounded in such a critique. A person tarred as a Luddite is not rejecting "technology" or a specific gadget or modernity itself. She is rejecting the monetizing and mediation by commercial interests of all her communications. Or she is protesting tech companies' wrapping their regressive politics in the slick package of techno-liberation. Or perhaps she just wants to own the things she owns, to not have her possessions spy on her, to not have every choice and action be fed into a great analytic mega-machine whose ultimate purpose is to extract more money, knowledge, attention, or small strategic advantage out of her. She wants the invasive other, which operates through the larger forces of surveillance capitalism and digital technologies, to leave her alone.

We are all entangled in these networks of information consumption and production. The occasional rebel or eccentric forsakes mobile devices entirely, or someone who is destitute finds no use for them. But they are not off the grid—there is almost no possibility of such. Their personal information is still being sold to and from private data brokers and government agencies. Automated license-plate readers scan their cars and track their movements. Insurers study their purchasing habits or social media accounts for signs of liability. Other digital traces of their actions prove surprisingly enduring and fluid, showing up in unexpected places. They become data objects, whether they know it or not. From this position of entanglement, it can be hard to see outward, to imagine other possibilities. But for how long can increasingly personalized surveillance and the rhetoric of consumer empowerment go hand-in-hand? When will consumers realize that what has been peddled as convenience is really a kind of infantilization, swaddling us in personalized services while depriving us of autonomy and choice? It is time to start envisioning other paradigms, whether they be social networks without metrics, communications without surveillance, or business models that do not depend on personal data. It may be all of these or something else entirely, but down one of these roads lies the future, if not progress.

REFERENCES

Adler, Richard P., Hubert Lipinski, Michael Nyhan, John Tydeman, and Laurence Zwimpfer. 1982. *Teletext and Videotex in the United States: Market Potential, Technology, Public Policy Issues*. New York: McGraw-Hill.

Condiliffe, Jamie. 2015. "Wifi Networks Can Now Identify Who You Are through Walls." *Gizmodo*, Oct 28. http://gizmodo.com/wifi-networks-can-now-identify-who-you-are-through-wall-1738998333.

Corbyn, Zoe. 2012. "Facebook Experiment Boosts US Voter Turnout." *Nature*, Sept. 12. http://www.nature.com/news/facebook-experiment-boosts-us-voter-turnout-1.11401.

Frier, Sarah. 2016. "Facebook Wants You to Post More about Yourself." *Bloomberg*, April 7. https://www.bloomberg.com/news/articles/2016-04-07/facebook-said-to-face-decline-in-people-posting-personal-content.

Kramer, Adam D. I., Jamie E. Guillory, and Jeffrey T. Hancock. 2014. "Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks." *PNAS*, June. http://www.pnas.org/content/111/24/8788.full.pdf.

Lever, Rob. 2016. "Big Data Helped Trump Even after He Scorned It." *AFP*, Dec. 3. https://www.yahoo.com/news/big-data-helped-trump-even-scorned-034851943.html.

Nakashima, Ellen, and Joby Warrick. 2013. "For NSA Chief, Terrorist Threat Drives Passion to 'Collect It All'." *The Washington Post*, July 14. https://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html?utm_term=.9a7dc6a10358.

Paglen, Trevor. 2016. "Invisible Images (Your Pictures Are Looking at You)." *The New Inquiry*, Dec. 8. http://thenewinquiry.com/essays/invisible-images-your-pictures-are-looking-at-you.

Steele, Billy. 2016. "Police Seek Amazon Echo Data in Murder Case." *Engadget*, Dec. 27. https://www.engadget.com/2016/12/27/amazon-echo-audio-data-murder-case.

Sweeney, Latanya. 2013. "Discrimination in Online Ad Delivery." Harvard University, Jan. 28. https://arxiv.org/ftp/arxiv/papers/1301/1301.6822.pdf.

Timmer, John. 2014. "Researchers Reconstruct Human Speech by Recording a Potato Chip Bag." *Ars Technica*, Aug. 5. http://arstechnica.com/science/2014/08/researchers-reconstruct-human-speech-by-recording-a-potato-chip-bag.

United States Senate Committee on Commerce, Science, and Transportation. 2013. "A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes." *US Senate Office of Oversight and Investigations Majority Staff*,

Dec. 18. https://www.commerce.senate.gov/public/_cache/files/bd5dad8b-a9e8-4fe9-a2a7-b17f4798ee5a/D5E458CDB663175E9D73231DF42EC040.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf.

Villasenor, John. 2011. "Recording Everything: Digital Storage as an Enabler of Authoritarian Governments." *Brookings Institution*, Dec. 14. https://www.brookings.edu/research/recording-everything-digital-storage-as-an-enabler-of-authoritarian-governments.

Yachot, Noa. 2016. "Your Favorite Website Might Be Discriminating Against You." *ACLU*, June 29. https://www.aclu.org/blog/speak-freely/your-favorite-website-might-be-discriminating-against-you.

Zetter, Kim. 2016. "Clever Attack Uses the Sound of a Computer's Fan to Steal Data." *Wired*, June 6. https://www.wired.com/2016/06/clever-attack-uses-sound-computers-fan-steal-data.

Zuboff, Shoshana. 2015. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization." *Journal of Information Technology* 30: 75–89.