# 2

# The Surveillance Machine

In February 2017 an active-duty U.S. Marine Corps cadet stood in line to check in for her new posting at Camp Lejeune, North Carolina. A male infantry Marine stood a few paces behind her. He secretly photographed her. He then posted the photos on a private Facebook page called "Marines United." A call went out for responses and for information about the cadet. Soon comments flooded the image posting on Facebook. The comments went beyond rude. Some suggested forced sexual acts. A few hours later someone, likely a former romantic partner, posted a photo to the group of the woman with her breasts exposed. A retired Marine named Thomas Brennan, working as a reporter for a not-for-profit website called The War Horse, had noticed that the Facebook group that had been founded to help Marines cope with the stresses of combat and return to civilian life had transformed itself into a source of "revenge porn," featuring links to Google Drive folders containing thousands of images of servicewomen from all branches of the U.S. military. A few days after Brennan published his report on the Facebook group, the Marine Corps managed to get the



offensive photographs and links removed. The group was shut down by March. But the photos had spread among the group's members and now rested on the phones or hard drives of hundreds of Marines. Women have suffered harassment and ridicule within their workplaces and in their private lives. Those who discovered that their photos had circulated have been weighed down by fear of being humiliated in professional or even combat situations.[1]

This sort of surveillance and harassment occurs every day around the world. Men successfully exploit the power that visual exposure of women grants them. They coordinate humiliation on a massive scale, empowered by the ease, quality, and availability of small cameras attached to mobile devices linked to applications that promise rapid delivery to a targeted and motivated audience. "Social media" quickly become antisocial for the women who are targeted by this practice. Sometimes Facebook is involved. Sometimes Google services host the material. Some revenge porn, often images that originally were captured with the consent of the subject but later were distributed in anger by a former partner, ends up on sites devoted to the phenomenon. The ubiquity of powerful instruments that record images, videos, and sound has enabled malicious distribution of the most humiliating items, injuring the spirit, morale, comfort, and careers of millions of women. According to the research institute Data and Society, 4 percent of American women—and 10 percent of those under thirty years old—have been the victim of revenge porn.[2]

Every one of us who carries a camera attached to a mobile phone is an agent of surveillance. The camera, as Susan Sontag told us long before Facebook and Instagram, calls to us to use it. It demands our attention to render sights around us for later consumption. Sontag could not have imagined that billions of people would have these cameras and that many would abuse others by taking and posting humiliating photographs. But Mark Zuckerberg could. As we have seen, Zuckerberg decided peer photography would be the key to the future of Facebook. Each incident of peer surveillance becomes part of a massive corporate surveillance system once uploaded to Facebook or Instagram. Images are tagged with metadata revealing time and location. People tag photographs with names of the

people captured, revealing their presence and movements to others. The cameras themselves sit on a device designed for constant corporate surveillance. Most mobile phones track the users' location with global positioning system connections. And the Facebook and Instagram applications on the mobile phone also gather data about the person holding it. This is systemic surveillance. The key to its power is correlation. If I post a series of photographs taken in Charlottesville, Virginia, and tag three Friends who appear in them, Facebook correlates that information with what it gathers about them. Then Facebook can generate remarkably accurate assumptions about the frequency of our meetings, the nature of our relationships, the next circle of mutual acquaintances, and even our relative income and consumer habits. All of this seems harmless unless a Facebook user wishes to cause harm to another or some oppressive state power gains control over this sort of information. Both of these things happen. Peer surveillance connects to corporate surveillance and to state surveillance.

Revenge porn is perhaps the most troubling aspect, but hardly the only one, of the strange media ecosystem in which each of us plays an active role. Because of its reach and power, Facebook often ends up facilitating not just revenge porn but other incidents of humiliation, harassment, and unwanted exposure. Those who wish to do others harm do not have to work too hard to deploy Facebook in their plans. This is yet another example of good intentions going terribly wrong. Facebook makes it easy for us to gather and share. It favors images over text. It sorts people by interest. And almost 30 percent of the world—including almost everyone in North America and Europe—has a Facebook account. Facebook groups, Mark Zuckerberg's answer to the problem of civic degradation around the world, serve as secret societies through which all sorts of mayhem can go undiscovered and unpunished until it's far too late.

The reason Facebook does what it does so well—including amplifying the malicious and cruel acts that so many wish to perpetrate on others—is that it leverages massive amounts of information about its users to effectively sort and send the content it thinks we want to our News Feeds. What makes Facebook good also makes it bad. What makes Facebook wealthy also lets us be crueler. At the root of all this is a system of surveillance unlike any



we have ever seen. And it has reached us in ways we are unprepared to face. Surveillance fosters harassment and humiliation, whether it's from the state or from other people and groups. We can't perform as responsible, informed, engaged citizens of a republic if significant segments of the polis are harassed, silenced, and threatened every time they attempt to engage in matters of public debate. That's the fact right now. And it's perhaps the most acute limitation to the potential of internet platforms to enhance our lives positively.

Facebook has grown into the most pervasive surveillance system in the world. It's also the most reckless and irresponsible surveillance system in the commercial world. If you have been active on Facebook since before 2014 and you interacted with games or applications like Farmville, Mafia Wars, or Words with Friends, then Facebook exported not only a rich collection of your profile and activities on Facebook but also those of your Friends. Facebook has been sanctioned by governments around the world for its practices of collecting, using, and sharing personal data without full or clear disclosure. Yet the company continues to abuse its users, comforted by its popularity and power. In early 2018 when journalists revealed the extent to which a sleazy British political firm called Cambridge Analytica had Hoovered up Facebook data from more than fifty million Americans in preparation for its work to elect a president of the United States, the full range of Facebook abuse finally generated widespread popular attention and condemnation. Social media scholars and privacy advocates had been trying to raise concerns since at least 2010. But before there was a scandal complete with a James Bond–style villainous organization like Cambridge Analytica, few thought deeply about the damage Facebook was doing. A minor movement of Twitter users in the United States promised to #QuitFacebook. Facebook's stock price plummeted during the month of March. Regulators in Europe and the United States took new notice. Thousands downloaded records of what Facebook saved about them only to find that their Android-driven mobile phones had given Facebook records of text messages and calls. The uproar in the United States was strong, but Facebook's global power remained stronger. Still, the revelations of early 2018 presented the best opportunity for reform legislation and public pressure to alter the ways Facebook and other surveillance-based companies would do their business.[3]

## DATA FOR DOLLARS

Back in 2008 I was very careful with Facebook. I saw its hazards—and its benefits—as chiefly social. I established (and maintain to this day) a firm rule against interacting with current students on Facebook. I knew that by "Friending" someone I could peer into aspects of that person's life to which I was not invited. And in those early days of social media few people had developed norms and habits to guide their use of the service. I did not want to know whom my students were dating, what they wore to a Halloween party, or—most of all—what they thought of my courses. I was also pretty careful about what information I posted about myself.

I assumed, correctly at the time, that all Facebook could know about me was what I chose to reveal to and through Facebook. My age, relationship status, and sexual orientation fields remained blank during the first two years of my active Facebook participation. Then one day I thought it was time to come out as a straight married man over forty years old. Once I clicked "married," a strange thing happened. The advertising spaces on my Facebook page filled up with advertisements for services that invited me to contact women for the purpose of having an affair. Suspicious, I removed "married" from my profile. The ads disappeared. In the early days of Facebook its data collection and advertising targeting were so clumsy that the site merely filtered for one or two attributes and pushed ads based on them. In addition, the companies that chose to advertise on Facebook in the early days were often unseemly.

That all began to change around 2010. Like for many, my comfort level with Facebook had increased. I had succumbed to the constant prodding and suggestion that I add more Friends. Though I still scrupulously avoided current students, my circles grew. More of my social and political activities moved to Facebook. To be without Facebook by 2010 was to miss out on what seemed to be essential conversations and events. Even my parents signed up for it. Facebook's user base spread to all walks of life and started touching more countries and more languages, leaving would-be and once-dominant competitors such as MySpace with no sense of mission and no way to make money.[4]



Beyond users' lives and habits, something more important was going on inside the company. Mark Zuckerberg had lured Sheryl Sandberg away from Google in 2008 to be chief operating officer in charge of the business side of the company. By 2010 Sandberg had built an effective data collection and advertising system. The ads on my page began to reflect my professional interests and social connections. One regular ad was for a heavy and expensive leather briefcase like the kind professors in movies carry. It was not a perfect match for my interests (or for professors in general, few of whom would spring for a $250 leather case). But it was far better than ads urging me to cheat on my spouse just because I have one. To accomplish the mission of targeting advertisements deftly, Sandberg needed more and better data about what users did, thought, and wanted to buy. So she embarked on a series of expansions of Facebook's capabilities to track and profile users. Not coincidentally, 2010 was the first year that Facebook posted a profit. It's safe to say that if not for Sandberg and her formidable vision and management skills, Facebook might be a broke and trivial company today.[5]

Facebook is the most pervasive surveillance system in the history of the world. More than two billion people and millions of organizations, companies, and political movements offer up detailed accounts of passions, preferences, predilections, and plans to one commercial service. In addition, Facebook tracks all of the connections and interactions among these people and groups, predicting future connections and guiding future interactions. It even compiles contact information on those who do not have a Facebook account.

Facebook exposes us to three major forms of surveillance. We might think of them as three perches or viewpoints. Commercial and political entities are able to exploit the targeting and predictive power of Facebook through its advertising system. Through what we reveal on our profiles, other Facebook users can watch and track us as we build or break relationships with others, move around, recommend and comment on various posts, and express our opinions and preferences. And governments use Facebook to spy on citizens or anyone they consider suspicious, either by establishing Facebook accounts that appear to be those of friends or allies or by breaking through Facebook security to gather data directly.

Facebook itself conducts commercial surveillance of its users on behalf of its advertising clients. Facebook has no incentive to offer any third-party access to the data that it uses to drive user-generated posts and direct advertisements. The commercial value of Facebook lies in its complete control of this priceless account of human behavior. But the interface that Facebook provides to both advertisers and those who run Facebook pages allows them to learn significant amounts about their audiences in general and track the level of response their posts and advertisements generate. To profile users for precise targeting, Facebook uses much of the data that users offer: biographical data, records of interactions with others, the text of their posts, location (through Facebook apps on mobile phones equipped with GPS features), and the "social graph"—a map of the relationships among items on Facebook (photos, videos, news stories, advertisements, groups, pages, and the profiles of its 2.2 billion users). This combination of information allows Facebook to predict user interest and behavior based on what other people with similar attributes and similar connections want, think, or do.[6]

Beyond the data that Facebook gathers from its own core services (Facebook, Messenger, Instagram, WhatsApp, etc.), it allows other firms to connect to Facebook directly through a service called Open Graph. Open Graph is how the music service Spotify interacts with Facebook, using Facebook user names and passwords to enroll and log in to the service. This makes Spotify "social," in the sense that the music one user listens to via Spotify becomes available to her Friends who are also using Spotify, and those Friends' music habits are available to others as well. This creates a mesh of interests that can prompt discovery or recommendations among like-minded music fans. To Spotify, this service amplifies its ability to find new users and maintain established users. To Facebook, it means that more interactions—even outside of Facebook—become part of the larger social graph and thus useful for profiling and targeting. Facebook, through its Open Graph partnerships and the use of tracking cookies that it implants in users' web browsers, is able to gather immense amounts of personal data from people who hardly ever log in to their Facebook accounts. Basically, there is no way to opt out fully from Facebook's ability to track you.[7]



This form of single-firm commercial surveillance seems almost harmless by itself. Facebook lacks a police force, so it can't abuse its power in a way that injures people or denies liberty or property. If it profiles someone inaccurately and targets advertisements improperly, the company just will not generate revenue for that action. When all those data serve Facebook well, leaders of Facebook argue, it provides a more enjoyable and relevant experience to users. No cat owner wants to see a barrage of ads for dog food. No vegetarian wants to see ads for hamburgers. And we generally prefer seeing posts from the people whom we like and think like. There are problems with this sort of filtering, as we will see in Chapter 3. But none of those problems quite qualifies as an immediate risk or danger to users. However, Facebook gathers and deploys much of this information without our knowledge or consent. Facebook does not offer us a full view of how our activities are used. And Facebook does not offer us clear and easy ways to exempt ourselves from this pervasive surveillance. Users might generally understand that the company retains and uses the specific attributes that they post to their profile. But most users certainly do not have a full picture of the depth and breadth of Facebook's activities. Users rarely are informed, for instance, that Facebook buys troves of credit-card purchasing and profile data from the large data marketing firms. A user must poke around or search Facebook's help site to discover this fact. This mix of the information we offer to Facebook, Facebook's ability to track us on the web and in the real world, and the commercial credit data it purchases empowers Facebook and disempowers us.[8]

The chief danger from the Facebook commercial surveillance system lies in the concentration of power. No other company in the world—with the possible exception of Google—can even consider building a set of personalized dossiers as rich as Facebook's. These data reinforce Facebook's commercial dominance in the advertising business (again, mostly shared with Google, which has different ways of tracking and targeting content and advertising but generates many of the same risks and problems). The very fact that we cannot expect another digital media company to generate that much data from that many people and that many interactions means

that—barring strong regulation—serious competitors to Facebook will be rare or nonexistent in the near future.

But there are other dangers that come with Facebook having and holding all of this information on us. They come from the two other surveillance positions: peers and states. Many common behaviors of Facebook Friends sever our images or information from our control, regardless of how careful any individual is with privacy settings. Other Facebook users can act maliciously, especially when relationships degrade. And other Facebook users might be more promiscuous in their habits of tagging photographs of people who would rather not be identified beyond a tight circle of known Friends. Beyond this, Facebook profiles can be abused for the purposes of public shaming, harassing, or exposing personal information to outsiders. What we put on Facebook is often carefully selected and managed, a constant if exhausting exercise in self-promotion and self-presentation. That means that Facebook profiles are rarely if ever full and accurate portrayals of our lives and personalities. That's one reason Facebook goes to great lengths to monitor and record our actual activities and movements. We might want everyone to think we are vegan, but we might slip up and eat at Burger King in a moment of weakness. We should not have to reveal such moments to our Friends. But Facebook ensures that it knows us better than our friends and family members do. Still, the fact that Facebook profiles are inaccurate or inauthentic portraits of complex human beings means that actions and reactions by others peering at them can generate unfair or harmful reactions. Jokes can be misread. Declarations of loosely held opinions could blow up into misreadings that cause social conflicts. Facebook was designed to limit our interactions and exposure to the circle of those we trust. It no longer functions that way.[9]

Despite the promises Facebook makes to its users, there are many ways that it ensures users lack control over their information. Privacy journalist Kashmir Hill noticed in 2017 a curious phenomenon. Facebook was recommending that she "Friend" people she hardly knew or did not even know of. She asked her readers if they had had similar experiences, especially any that led to awkward or possibly harmful encounters via Facebook. Social workers and therapists reported being connected with clients despite never



exchanging private information with them. A sperm donor was urged to connect to the child of a couple to whom he had donated sperm, despite the parents not wanting the donor to have contact with that child. Hill discovered that a Facebook feature called People You Might Know urged people to upload the address books from their computers or phones. Those email addresses and mobile phone numbers served as identifiers to Facebook profiles. And because Facebook's social graph traced connections among profiles, the People You Might Know feature had the ability to connect people who were quite distant, estranged, hostile, or even violent toward each other. Because no user could control what information lies in another's address book, no user could opt out of the feature. Users are at the mercy of other people and their understanding of how Facebook uses personal information. "A one-night stand from 2008, a person you got a couch from on Craigslist in 2010, a landlord from 2013: If they ever put you in their phone, or you put them in yours, Facebook could log the connection if either party were to upload their contacts," Hill wrote. "That accumulation of contact data from hundreds of people means that Facebook probably knows every address you've ever lived at, every email address you've ever used, every landline and cell phone number you've ever been associated with, all of your nicknames, any social network profiles associated with you, all your former instant message accounts, and anything else someone might have added about you to their phone book." And there is nothing anyone can do about that. Users are tricked at the moment they register with Facebook to upload their contacts for the sake of convenience. Facebook never invites users to consider the consequences of that action.[10]

State uses of Facebook are even more troubling. States do have the power and right to imprison and commit violence against citizens and those they consider threatening. State power leverages Facebook in two ways. First, and most common, we have seen authoritarian leaders in various countries monitor Facebook activity and track suspected dissidents and journalists. They use Facebook and WhatsApp to generate campaigns of harassment against perceived enemies and critics. States can use bogus profiles to infiltrate Facebook groups devoted to reforming or challenging the government, or even groups that offer support to gay and lesbian people. The 2013 revelations

by Edward Snowden that the security and intelligence services in the United States and the United Kingdom had managed to tap into the data flows of Facebook, Google, Apple, Microsoft, Yahoo, and other companies showed just how vulnerable Facebook users are to state surveillance power. As long as Facebook retains such a rich source of intelligence, states will try to infiltrate the system.[11]

## ENEMIES OF THE STATES

Cinema can help illustrate some of the major concepts of privacy and surveillance. Filmmakers have an understandable interest in the technologies and ethics of surveillance. After all, they watch people for a living and present actions and images to a broad public. There is a long-running conversation about surveillance in cinema. It starts with the work of Fritz Lang. *Metropolis*, from 1927, uses the power of police surveillance for social control of workers as a central theme. *M*, from 1932, is about everybody watching everybody, sort of like Facebook and Instagram today. Recent films about surveillance have included *Captain America: The Winter Soldier*, from 2014, and *The Circle*, from 2017, an adaptation of the dystopian novel by David Eggers about a company not unlike Facebook.

Consider two American films, twenty-four years apart, both starring Gene Hackman as a reclusive surveillance expert. The difference between the work done by Harry Caul, the naive, emotionally stunted private investigator played by Hackman in Francis Ford Coppola's 1974 film *The Conversation*, and the work done by Edward Lyle, the disaffected, cynical former spy Hackman played in the 1998 Tony Scott film *Enemy of the State*, is more than a matter of tools.[12]

Caul uses audio and video surveillance to investigate private citizens, while Lyle deftly deploys the digital tools and techniques that have come to characterize our era of total surveillance. Before choosing to go "off the grid," Lyle did high-level work for either a government organization like the National Security Agency or a private contractor working for the NSA. (The exact truth is never fully revealed.) Lyle seems to be Caul twenty-four years later, with a new name and a deeper sense of nihilism but the same



aversion to sharing information with others. Caul's tools, analog and cumbersome, are remarkably effective at capturing the conversations and images of known people. He works on specific targets and is hired by private firms and individuals. He focuses on personal matters, not criminal or national security matters. Lyle, by contrast, introduces both Robert Clayton Dean (played by Will Smith) and filmgoers of the late 1990s to an invisible web sustained by the continuous mining and tracking of digital data. The team of geeky spies assigned to track Dean as he rushes through Washington, D.C., has at its disposal credit records, mobile phone signals, and hundreds of surveillance cameras positioned throughout the city.

Caul lives in a completely different information ecosystem from the one inhabited by Lyle. It's not that the government is more benign or restrained during the Nixon years, or that private firms have more noble motivations. And Caul certainly has the skill and equipment to track individuals and record their expressions in intimate detail. Like Lyle, he has the power to ruin lives through surveillance and revelation. But Caul cannot imagine anything beyond the precisely targeted surveillance of individuals.

Lyle, however, lives at the dawn of the Big Data era. In Lyle's information ecosystem, firms and states maintain massive databases that contain records of commercial transactions, movements, and expressions. There is a permeable membrane between data collected by private firms and data used by state security forces. And our electronic devices, as Dean learns the hard way, facilitate this constant and nearly total environment of discreet surveillance. Data collection is so cheap and easy that it's unnecessary to judge a priori what among the data might be important. Firms and states collect first and ask questions later.

*Enemy of the State* debuted in the United States the same year that two Stanford graduate students released a stripped-down site called Google that would help people search the World Wide Web with speed and precision, relaying on the data that users would provide through previous searches, links, and clicks. The film appeared three years before the attacks of September 11, 2001, which in turn precipitated a steady increase in state surveillance across the world. The film predated the USA PATRIOT Act by four years. It arrived four years before the U.S. government declared

its intention to gather and track massive amounts of commercial and communications data in a program it called Total Information Awareness. The film predated Facebook by seven years, the iPhone by nine years, and by fifteen years the revelations by Edward Snowden that the U.S. and U.K. governments were successfully tapping into and harvesting massive amounts of communication information on their own citizens as well as millions of innocent people around the world. So when viewed today, *Enemy of the State* seems almost comical, as its characters lack the basic awareness and acceptance that we would expect such sophisticated people to have about surveillance today.

## THE PROBLEM WITH PRIVACY

Caul's downfall in *The Conversation* results from a moment of weakness. He reveals the wrong details to the wrong person at the wrong time. His own vulnerability awakens his moral sense. Concerned not just for his own privacy, he now feels culpable for the damage he has done to others. In Caul's awakening we glimpse what Georgetown law professor Julie Cohen has called the move from a focus on individual autonomy to the "social value of privacy." Caul's concerns about even other people's individual privacy is inadequate. Theories founded on and bounded by liberal individualism consistently fail to account for how we actually live our lives in a networked world. After all, none of us actually live individual lives. We are embedded in social and cultural relationships, so we live among multiple social contexts. We make and remake ourselves dynamically as we move in time and among others, as our interests and allegiances change.[13]

We can see that privacy is not merely those aspects of our lives that we withhold from others. Privacy is more than the autonomy we exercise over our own information. The word more accurately describes the ways we manage our various reputations within and among various contexts. Those contexts might include school, church, the public sphere, a place of employment, or a family. Each of these contexts shifts and overlaps with others. Borders change. Contexts blend. So configuring a "self" in the twenty-first century is a lot more work than it used to be. The fluidity is liberating,



especially for those who seek niches supportive of marginalized identities. But it can be a terrifying and vertiginous liberty—sometimes exhausting and even potentially dangerous.[14]

Contexts in a digitally networked world—a world that Lyle eschews in *The Enemy of the State*—are constantly intersecting and overlapping, like blobs of paraffin in a lava lamp. Our work sphere bleeds into our family sphere too easily, challenging our personal ability to manage our reputations and control the manners of disclosure. Our public contexts blend as commercial data firms collect and then sell our profiles to political parties and campaigns. Facebook brings all of our acquaintances together into one confusing collection of otherwise unrelated profiles that we are forced to deal with without the help of rank or distinction. Friends are just friends. So are lovers, bosses, acquaintances, and high school teachers.

## THE CRYPTOPTICON

In the current commercial, political, and regulatory environment, institutions have powerful incentives to collect, save, and analyze every trace of human activity. But there have long been potential payoffs for tracing and tracking subjects (consumers, citizens, criminals, users). To explain the relatively recent turn to Big Data as a tool of choice, scholars and analysts tend to emphasize the availability of appropriate technologies. These include huge server farms, algorithms designed to quickly reveal patterns within otherwise meaningless pools of data, greater bandwidth and faster processing capacities, and so on. But this technocentric analysis misses or downplays the role of significant changes in the global political economy and dominant ideologies since 1980. When securities markets and consultants praise "efficiency" above all other values, when states place "security" above all other public needs, and when mass-market advertising reaps at best murky returns for each dollar spent, the incentives to target, trace, and sift grow in power.

There is little in the current regulatory or market environment that would discourage the use of Big Data. Because it offers clear public benefits, such as, for instance, quicker and broader epidemiological assessments, it

would seem foolish to dispense with Big Data and its technological systems and practices. But we should understand the costs as well as the benefits—and not allow its rapid rise and widespread adoption to blind us to the need for critical public and political discussions of its use and abuse. In his influential book from the 1970s, *Discipline and Punish*, Michel Foucault adopted the concept of the Panopticon—Jeremy Bentham's never-realized design for a circular prison with a central watchtower, from which the behavior of inmates could be observed at all times—to describe the programs and techniques used by the modern state to monitor, supervise, and ultimately modify the behavior of its citizens. To Foucault, the Panopticon was embedded in the practices, structures, and institutions of modern society, from government bureaucracies to schools to hospitals and asylums and to the assorted regimes of health, well-being, and citizenship they variously inscribed upon their subjects. Such systems of surveillance left "no need for arms, physical violence, material constraints," as Foucault once said. "All that was needed was 'a gaze,' an endlessly inspecting gaze, which each individual would end up internalizing, thus becoming his or her own constant supervisor. A superb formula: Power exercised continuously and for what turns out to be a minimal cost." The gaze, the theory goes, works as well as iron bars to control the behavior of most people.[15]

Those who write about privacy and surveillance often invoke the Panopticon to argue that the great harm of mass surveillance is social control. Yet the Panopticon does not describe our current predicament. First, mass surveillance does not inhibit behavior: people will act weirdly and willfully regardless of the number of cameras pointed at them. The thousands of surveillance cameras in London and New York City do not deter the eccentric and avant-garde. Today, the example of reality television suggests that there may even be a positive correlation between the number of cameras and observers pointed at subjects and their willingness to act strangely and relinquish all pretensions of dignity. There is no empirical reason to believe that awareness of surveillance limits the imagination or cows creativity in a market economy in an open, non-totalitarian state.

Obviously, coercive state violence still exists, and at times metastasizes. The Stasi in Cold War–era East Germany knew how to exploit the widespread awareness of surveillance to heighten the fear and submissiveness of the general public. But the environment shaped by the Stasi is not the environment in which most of us now live. Unless the Panopticon is as visible, ubiquitous, and intentionally menacing as agencies such as the Stasi made it, it cannot influence behavior in the ways Bentham and Foucault assumed.[16]



In Europe, North America, and much of the rest of the world, governments and businesses achieve their ends in almost the opposite way from that of the Panopticon: not through the subjection of the individual to the gaze of a single, centralized authority, but through the surveillance of the individual by all (in theory, though at least in fact by many). I call this the Cryptopticon: an inscrutable information ecosystem of massive corporate and state surveillance.[17]

Unlike Bentham's Panopticon, the Cryptopticon is not supposed to be obvious. Its scale, its ubiquity, and even its very existence are supposed to be hidden from clear view. So while a CCTV camera mounted over a counter at a convenience store openly warns shoppers to behave or risk being caught, the Cryptopticon relies on browser cookies, data streams retained by telecommunication firms, satellite imagery, global positioning system traces, covert voice surveillance, store discount cards, e-book readers, and mobile applications. Each of these techniques masks its real purpose: to gather or provide data and to track the behavior of millions of people with stunning precision. Beguilingly, though, each technique offers something valuable and convenient—often "for free."[18]

Unlike Bentham's prisoners, we don't—perhaps can't—know all the ways in which we are being watched or profiled. So we don't regulate our behavior under the gaze of surveillance. Instead, we seem not to care. The workings of the Cryptopticon are cryptic, hidden, scrambled, and mysterious. One can never be sure who is watching whom and for what purpose. Surveillance is so pervasive and much of it so seemingly benign ("for your safety and security") that it's almost impossible for the object of surveillance to assess how she is manipulated or threatened by powerful institutions gathering and using the record of surveillance. The threat is not that expression or experimentation will be quashed or disciplined, as they supposedly would be under the Panopticon. The threat is that subjects will become so

inured to and comfortable with the networked status quo that they will gladly sort themselves into "niches" that enable effective profiling and behavioral prediction. The Cryptopticon is intimately linked to Big Data. And the dynamic relationship between the two concepts underlines the need to understand both in relation to commerce, the state, and society more generally.

Facebook, Google, and Amazon want us to relax and be ourselves. They have an interest in exploiting niche markets that our consumer choices have generated. These companies are devoted to tracking our eccentricities because they understand that the ways we set ourselves apart from others are the things about which we are most passionate. Our passions, predilections, fancies, and fetishes drive and shape our discretionary spending; they are what make us easy targets for precise marketing. Market segmentation is vital to today's commerce. In order for marketers and vendors to target messages and products to us, they must know our eccentricities—what makes us distinctive, or, at least, to which small interest groups we belong. Forging a mass audience or market is a waste of time and money unless you are selling soap—and a very generic soap at that.[19]

Even modern liberal states such as those of North America and Western Europe want us to be ourselves. They count on subversive and potentially dangerous people to reveal themselves through their habits and social connections, not to slink away and hide in the dark. Repressing dissent and subversion does not eliminate potentially dangerous types. The Stasi lost control over the East German people despite the enormous scale of its operations and the long-lasting damage that inflicted on both the observers and the observed. In the liberal state of the twenty-first century, domination does not demand social or cultural conformity. The state, like every private firm that employs a sophisticated method of marketing, wants us to express ourselves—to choose—because mere expression of difference is usually unthreatening, yet remarkably useful to the powerful.

Florian Henckel von Donnersmarck's brilliant 2007 film *The Lives of Others* demonstrates the corrosive power of constant state surveillance. The protagonist, a playwright loyal to the East German government, enjoys all the perks of stardom, such as it is in a society not overwhelmed with material



glitter. Many of his intellectual and artistic friends, however, have strayed from the uncomfortable embrace of the state. Still, he naively trusts that his political loyalty will continue to protect him. When a romantic entanglement places his girlfriend, and then him, under high-level surveillance, his confidence unravels and the depravity of the state becomes clear. The film concludes with a glimpse of the 1991 version of Big Data. The playwright, now trying to reconstruct his life in the wake of the unification of Germany, visits the new archive in Berlin that allows citizens to examine the files that the Stasi collected. This moment leaves viewers with a powerful sense of how detailed, destructive, and all-encompassing state surveillance could be in even an era of non-networked analog media forms.[20]

Companies such as Google and Facebook put Big Data collection and analysis at the heart of their revenue-generating functions, always described by company officials as enhancements to the "user experience."[21] The line between state and commercial surveillance hardly matters anymore, as state security services regularly receive significant data sets on people's movement and habits just by asking for or by licensing the data on the open market.[22] Data collected by one institution are easily transferred, mined, used, and abused by another. So one company might purchase consumer data from a supermarket or big-box retailer and then sell them to direct-mail marketers, political parties, and even local law enforcement. Data firms also collect state records such as voter registrations, deeds, car titles, and liens to sell consumer profiles to direct-marketing firms.[23]

Given the many possible abuses of Big Data, including the long-term tarnishing of personal and professional reputations, citizens need to be fully aware of the flows of information between private firms, governments, and any other institutions that might have an interest in using such data.

## SOCIETY

In Michelangelo Antonioni's 1966 film *Blow-Up,* a photographer secretly photographs a couple embracing in a London park. The woman, furious when she notices what the photographer is up to, chases him down. "This is a public place," she says to the man. "Everyone has the right to be left in

peace." It is an odd bit of dialogue, at least to American ears. The standard American assumptions about private and public spaces are that everyone has a right to be left in peace in private, but not in public. The seeming incongruity compels most American viewers to interrogate the idea of being "left in peace," and under what conditions someone should be. Because privacy law in the United States has for so long depended on the distinction drawn in the constitutional prohibition on "unwarranted search and seizure," we assume that there are private spaces and public spaces and that our norms and expectations of what is appropriate to each must fall within those demarcations. Privacy ends at the threshold.

Almost fifty years after the release of Antonioni's film, the flimsiness of the American conception of privacy is easier to see. The distinction between private and public spaces is no longer relevant. We might have had privacy when our thoughts and personal information were recorded in papers that we stored at home. But now so much of our essential data sits on servers far from our computers, in a place we nonchalantly and naively call "the cloud." American law does not protect this information from the prying eyes of the state because we have placed it with "third parties." In doing so, we have withdrawn it from the realm of private. As Justice Sonia Sotomayor wrote in her concurring opinion in *United States v. Jones* in 2012, "I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on." The case was about the warrantless surveillance of a suspect who was driving around with a global positioning system sensor placed beneath his car. The police argued that they were merely tracking his movements in public. The Court, and Sotomayor in particular, did not find that a persuasive response.

The scene from *Blow-Up*, with its very un-American notion that privacy is not necessarily a spatial matter in all contexts, leads us to recognize that social relations rely on a web of trust. Respecting privacy is high among these norms that facilitate social relations.[24] The unnamed photographer in *Blow-Up* does not work for the state. He does not work for a commercial firm. And it's unclear from the testimony or action of his subject, played



by Vanessa Redgrave, what she fears the photographer might use the photograph for. The film teaches us, long before millions of people walked the streets with powerful cameras in their pockets, that one of the greatest threats to personal dignity comes not from large firms or powerful governments. It comes from millions of individuals armed at all times and in all places with audio, video, and photographic recording devices. Fellow members of society have the means, if they are so inclined, to expose, harass, and vilify their neighbors either to satisfy a sense of vigilante justice or simply to amuse themselves. Soon we may have access to "always-on" surveillance technologies such as Google Glass that will not only record all of our public and private interactions in both public and private but also share the images and sounds with Google—thus making them available to businesses and governments as well.[25]

When *Blow-Up* was released, the lone man with a camera in a park capturing images of strangers was an anomaly. Now such behavior is so common that it's unremarkable and even the norm. The new normal deserves remark and reconsideration, not least because it is so ethically and legally fraught. We so precipitously entered the age of (potentially) near-total and continuous mutual surveillance that we failed to weigh our individual consumer desires and personal predilections against the need for certain norms to uphold the common good.[26]

The need for informed debate about the norms, practices, and regulations that would govern how we should treat each other is clearly urgent. Many strong incentives (the desire for ease, efficiency, connection, pleasure) militate in favor of people's tacitly accepting the status quo of maximum surveillance by as many people as possible. And the devices that make this new normal possible are so attractive in so many ways that to criticize them or their users is to encounter a powerful resistance.[27]

How young people manage their reputations within various contexts has been a subject of much poorly conducted debate in recent years. Privacy is as much a matter of social norms as law or technology. Should we, as the pundits warn, assume "privacy is dead" because young people seem to share all sorts of details via social media without regard for traditions of reticence and modesty? In fact, the rest of us might do better to emulate the

sophisticated strategies many young Americans actively deploy to protect themselves and engage socially. The studies that danah boyd undertook for her essential book *It's Complicated: The Social Lives of Networked Teens* demonstrate that young people learn early on how to mask the meanings of their social network engagements by developing codes that are impenetrable for parents and others in authority. Just as important, young people are far more likely to manipulate privacy settings on social network services than are their older "friends" (i.e., relatives, teachers, and coaches).[28]

We are beginning to understand the ramifications of rapid change in our information ecosystem. Scholars in such disconnected areas as computer science, science and technology studies, library and information studies, communication, marketing, political science, media studies, and the philosophy of science have been picking away from different angles at the problems and opportunities that Big Data presents. Our thinking about "privacy" and "surveillance" is still overdetermined by American legal history and by the long shadow of Michel Foucault. Focusing on how Facebook uses us might help.[29]

## THE ZUCKERBERG DOCTRINE

All of this promiscuous connectivity and data collection does not pose a problem in Mark Zuckerberg's view. He believes that the very process of connectivity is good for us. If some connectivity is good, then more must be better. Facebook employees tend not to use words such as "privacy" when discussing their company's services. There is good reason for this. The term itself is too heavy. It carries too many meanings and can only seem to be the opposite of what Facebook wants to build. After all, privacy implies a denial of communication, a restriction on movement and gaze. Privacy seems to be the opposite of connectivity. As Zuckerberg wrote in a 2010 op-ed in the *Washington Post*, "If people share more, the world will become more open and connected. And a world that's more open and connected is a better world." Facebook has repeatedly and regularly introduced features such as the News Feed, photo albums, and the Beacon program (which alerted one's Friends of purchases) that generated immediate blowback because



of privacy concerns. Each time (except with Beacon, which Facebook closed down) Facebook just persisted until its users capitulated and grew comfortable with the new features—or just grew tired of complaining and protesting.[30]

So Facebook's playbook has seemed to be to slowly and steadily acclimate users to a system of surveillance and distribution that if introduced all at once might seem appalling. Facebook has been training us to accept its core principles as matters of habit and practice. Meanwhile, Facebook emphasizes that it gives users "control" over what they share and with whom, even as it steadily erodes resistance to systems and features that remove control from users. And Zuckerberg keeps telling us what he wants us to want. As Zuckerberg told *Time* in 2010, "What people want isn't complete privacy. It isn't that they want secrecy. It's that they want control over what they share and what they don't." He never defines "complete privacy." Facebook documents and Zuckerberg's statements leave "privacy" undefined. Whatever it means to Facebook and Zuckerberg, it's something to be resisted, not protected. It's something to overcome, not something to strengthen. Zuckerberg has decided it is not in our interest. And he has steadily built a system that moves us to accept his vision of a better, more connected, more watched world.[31]

By emphasizing user "control" Zuckerberg is not completely misguided. The essence of privacy is the combination of autonomy and dignity. Privacy is not a substance we can trade away. It's not a state of being that either exists or does not exist. And it can't "die," as too many people have declared. Privacy is a power we exercise—or hope to exercise—when we see fit. It exists when we have control over how information about us is used in various contexts. Early in life we figure out that our social lives are made up of intersecting circles of family, friends, acquaintances, and the people and institutions that exercise power over us. So as children we quickly learn how to manage our reputations among these various contexts. We learn, often the hard way, that some things we can say to our friends we should not say to our parents. Things that we reveal to clergy we should not share with siblings. Teachers and coaches have special knowledge about us that if released to our peers might humiliate us. So we manage who knows what

about us. We develop bonds of trust among the people and institutions in our lives. When someone abrogates that trust we suffer. That process of management of reputation among various contexts is what we usually call privacy.[32]

Facebook scrambles our social contexts. If we don't actively partition our collection of hundreds or thousands of Friends and segregate those subcollections, we soon find our contexts melding. A joke meant for friends from university years reaches an employer and degrades our status at work. A political comment meant for a tight circle of peers who have engaged in an ongoing argument gets recast when it shows up in the News Feed of a neighbor. What's entertaining in one context can be embarrassing in another. Facebook offers us rough tools to manage our contexts, but it defines our contexts awkwardly and unhelpfully. So our social contexts quickly collapse. Over time, we give up trying to work so hard at it. Either we accept the social consequences or we temper our expressions under the assumption that the wrong people could read our posts at any time.[33]

By emphasizing "user control," Facebook puts the burden on us to manage the collapse of social contexts that Facebook itself creates. This is the standard position of Facebook, Google, and other Silicon Valley companies that monitor our behavior and record our transactions. They defend their policies by reminding us we may help ourselves if we see fit to do so. We may change the settings on each service to limit the surveillance. While installing the default settings in their favor, they claim they empower us by giving us choices. This spirit of "self-help" teaches us over time that privacy is a personal matter, not a social or political one. The burden Facebook places on us is to protect *ourselves*—not those less aware of how Facebook works or of the consequences of privacy violations, not those more vulnerable, and certainly not the entire ecosystem. Protecting privacy is an environmental problem that Facebook treats as a matter of individual responsibility.

Facebook also treats privacy as an engineering problem that can only be solved using the labor and foresight of its users. As a response to revenge porn, Facebook launched an experiment in late 2017 in Australia. Users who feared they might become victims of revenge porn were encouraged to



send nude photos of themselves to Facebook. Facebook employees would examine those images and feed them into a computer to create a unique digital signature for each image. An algorithm deploying artificial intelligence could scan and match the offending images with those others upload to Facebook. Facebook would store the images for a short period (Facebook did not declare how short that period would be) before deleting the original image but retaining the fingerprint. The fingerprinting method, known as "hashing," allows the algorithm to match the original image with an altered version of the image—a move many revenge porn perpetrators make to try to limit the scanning power of photo-hosting sites. Major technology companies use similar processes—a combination of human judgment and algorithmic screening—to identify child pornography.[34]

Because Facebook is so huge, and because the volume of photograph uploads is so massive—more than 350 million each day—there might be no more effective way to address the threat of revenge porn. But that's the problem. Facebook cannot hire and train enough people to do this work preemptively. Plus, looking at thousands of images per day of all the horrible things people do to each other is among the worst jobs in the world. Machine learning is only as effective as the "training data" that go into it—in other words, nude photos. As long as Facebook maintains private groups and allows for the promiscuous and instant uploading of images it must rely on users themselves to police the site. It's not in Facebook's interest to shut down groups or to delay the availability of all photographs for a few hours while computers and people scan them. The "user experience" of most trumps the health and safety of some. The risk and burden lie on us, while the benefits go to Facebook.[35]

This Australian revenge porn experiment highlights the central problem with Facebook's approach to the dark and cruel things people do to each other. Those who have been victimized or fear being victimized by revenge porn are often traumatized. Yet the company is willing to ask those very victims to engage in the most intimate ways with a system that they have no reason to trust and people they will never meet or know. That seems like too large a burden to place on those who have already paid too high a price for these ubiquitous systems of surveillance.[36]

The tension between the ethical demands to protect people from harassment and exploitation and the urge to keep the "user experience" seamless and convenient exists because everything Facebook does is based on the urge to harvest our attention and use it for two purposes: to give us more of what we tell Facebook we want and to help advertisers precisely match their pleas for commerce with those who might be interested in those goods and services. Facebook has mastered the attention economy. It can't operate any other way. Our privacy and dignity ultimately do not matter in the attention economy. They are inconvenient and disposable.