THREE THE GOOGLIZATION OF US

UNIVERSAL SURVEILLANCE AND INFRASTRUCTURAL IMPERIALISM

In 2006, *Time* declared its Person of the Year to be you, me, and everyone who contributes content to new-media aggregators such as MySpace, Amazon, Facebook, YouTube, eBay, Flickr, blogs, and Google. The flagship publication of one of the most powerful media conglomerates in the world declared that flagship publications and powerful media conglomerates no longer choose where to hoist flags or exercise power. "It's about the many wresting power from the few and helping one another for nothing and how that will not only change the world, but also change the ways the world changes," Lev Grossman breathlessly wrote in *Time*. "And for seizing the reins of the global media, for founding and framing the new digital democracy, for working for nothing and beating the pros at their own game, Time's Person of the Year for 2006 is you."[1]

Almost every major marketing campaign these days is likewise framed as being about "you." "You" have freedom of choice. "You" can let yourself be profiled so that "you" receive solicitations only from companies that interest "you." "You" could customize "your" mobile phone with a ringtone. "You" go to the Nike Store to design your own shoes.

This emphasis on "you," however, is only a smokescreen for what is actually happening online. As I have stressed throughout this book, the Googlization of everything entails the harvesting, copying, aggregating, and ranking of information about and contributions made by each of us. This process exploits our profound need to connect and share, and our remarkable ability to create together—each person contributing a little bit to a poem, a song, a quilt, or a conversation. It is not about "you" at all. It should be about "us"—the Googlization of us.

Google, for instance, makes money because it harvests, copies, aggregates, and ranks billions of Web contributions by millions of authors who tacitly grant Google the right to capitalize, or "free ride," on their work. So in this process of aggregation, who are you? Who are you to Google? Who are you to Amazon? Are you the sum of your consumer preferences and MySpace personas? What is your contribution worth? Do "you" really deserve an award for allowing yourself to be rendered so flatly and cravenly? Do you deserve an award because Rupert Murdoch can make money capturing your creativity with his expensive toy, MySpace?

Because Google makes its money by using our profiles to present us with advertisements keyed to the words we search, precision is its goal. Google wants advertisers to trust that the people who see their paid placements are likely customers for the advertised products or services. These advertisers have little interest in broadcasting. That's a waste of money. The more Google knows about us, the more effective its advertising services can be. Understanding the nature of this profiling and targeting is the first step to understanding the Googlization of us.

How much does Google know about us? How much data does it keep, and how much does it discard? How long does it keep that information? And why?[2] Our blind faith in Google has allowed the company to claim that it gives users substantial control over how their actions and preferences are collected and used. Google pulls this off by telling the

truth: at any time, we may opt out of the system that Google uses to perfect its search engine and its revenue generation. But as long as control over our personal information and profiles is granted at the pleasure of Google and similar companies, such choices mean very little. There is simply no consistency, reciprocity, or accountability in the system. We must constantly monitor fast-changing "privacy policies." We must be willing to walk away from a valuable service if its practices cause us concern. The amount of work we must to do protect our dignity online is daunting. And in the end, policies matter less than design choices. With Google, the design of the system rigs it in favor of the interests of the company and against the interests of users.

Google complicates the ways we manage information about ourselves in three major ways. It collects information from us when we use its services; it copies and makes available trivial or harmful information about us that lies in disparate corners of the Internet; and it actively captures images of public spaces around the world, opening potentially embarrassing or private scenes to scrutiny by strangers—or, sometimes worse, by loved ones. In theory, Google always gives the victim of exposure the opportunity to remove troubling information from Google's collection. But the system is designed to favor maximum collection, maximum exposure, and the permanent availability of everything. One can only manage one's global electronic profile through Google if one understands how the system works—and that there is a system at all.[3] Google is a system of almost universal surveillance, yet it operates so quietly that at times it's hard to discern.

Google's privacy policy is not much help in this regard. In fact, it's pretty much a lack-of-privacy policy. For instance, the policy outlines what Google will collect from users—a reasonable, yet significant amount: IP (Internet Protocol) addresses (numbers assigned to a computer when it logs into an Internet service provider, which indicate the provider and the user's general location), search queries (which constitute a record of everything we care about, wonder about, or fantasize about), and information about Web browsers and preference settings (fairly trivial, but necessary to make Google work well). Google promises not to distribute this data—with two major exceptions. First, "We provide such

information to our subsidiaries, affiliated companies or other trusted businesses or persons for the purpose of processing personal information on our behalf." Second, "We have a good faith belief that access, use, preservation or disclosure of such information is reasonably necessary to (a) satisfy any applicable law, regulation, legal process or enforceable governmental request, (b) enforce applicable Terms of Service, including investigation of potential violations thereof, (c) detect, prevent, or otherwise address fraud, security or technical issues, or (d) protect against imminent harm to the rights, property or safety of Google, its users or the public as required or permitted by law."[4]

Google's privacy policy is a pledge from the company to us. It is binding in that if the company violated its policy, a user could sue Google in the United States for deceptive trade practices (though proving deception is always a difficult burden). However, Google changes its policy often and without warning. So today's policy—for all its strengths and weaknesses—might not be the policy tomorrow or next year. You might have engaged with Google and donated your data trail to it under the provisions of an early version of the policy, only to discover that Google changed the policy while you were not looking. The policy does pledge that "we will not reduce your rights under this Privacy Policy without your explicit consent, and we expect most such changes will be minor." But that is cold comfort, because the policy already gives Google substantial power over the data.

If you read the privacy policy carefully, it's clear that Google retains the right to make significant decisions about our data without regard for our interests. Google will not share information with other companies without user consent, but it asserts the right to provide such information to law enforcement or government agencies as it sees fit.

If another company were to acquire Google, the policy states, the company would inform users of the transfer of the data. But there is no promise that users would have a chance to purge their data from Google's system in time to avoid a less scrupulous company's acquisition of it. Although Google's commitments to fairness and transparency are sincere and important, they are only as durable as the company. If

Google's revenues slip or its management changes significantly, all the trust we place in the company today might be eroded.

To complicate matters more, each Google service has its own privacy policy. The index page for these policies contains a series of videos that outline the terms by which Google collects and retains data. One of the videos echoes the statement that Google retains personally identifiable information for only eighteen months after acquiring it. After eighteen months, information such as IP addresses is "anonymized" so that it's difficult to trace a search query to a particular user. However, that pledge is not made in the policy itself. Anonymization simply involves the removal of the last few digits of a user's IP address, and many cases of anonymization by information brokers have been exposed as ineffective at untethering people's identities from their habits.[5] The "cookies" left by many websites on users' computers contain information that could still be employed to identify a user.[6]

Although Google's public pronouncements about privacy and its general privacy statement fail to explain this point, Google actually has two classes of users, and consequently two distinct levels of data accumulation and processing. The larger, general Google user population simply uses the classic blank page with the search box in the center. Such general users leave limited data trails for Google to read and build services around. The second class might be called power users: those who have registered for Google services such as Gmail, Blogger, or iGoogle. Google has much richer and more detailed dossiers on these users. In exchange for access to this information, Google rightly claims that it serves these power users better than it serves general users. They get more subtle, personalized search results and a host of valuable services.

Google does empower users to control the information the company holds about them, but not in subtle or specific ways. Google's settings page offers a series of on-off switches that can prevent Google from placing cookies in a browser or from retaining a list of websites a user has visited. Power users can delete specific items from the list of website visits.

The default settings for all Google interfaces grant Google maximum access to information. Users must already be aware of and concerned

about the amount and nature of Google's data collection to seek out the page that offers all these choices.

Google's data-retention policies have come under significant scrutiny, especially in Europe. Most of the changes in its privacy policies in recent years have resulted from pressure by European policy officials. The United States government has offered consumers and citizens no help in these matters. In fact, it has acted to erode privacy. In 2006, the U.S. Department of Justice issued subpoenas to collect general information from the major search-engine companies in an effort to support its unsurprising contention that Internet users often search for pornography. The department wanted to use such data—which would not have been linked to any particular user, but instead would have offered generalized, statistical information about what users like to do online—in its legal defense of a law called the Child Online Protection Act. Of the major search companies, only Google resisted the subpoena, and then not to protect its users' privacy but to protect its trade secrets. Google's ability to analyze search queries for patterns is its greatest strength in the market. To give up such data could reduce the company's chief competitive advantage.[7] Google prevailed, and the government abandoned its efforts to collect such information.

Understandably, Google officials have practiced responses to questions about data retention and privacy. For instance, Google vice president Marissa Mayer explained to U.S. television host Charlie Rose in early 2009: "In all cases it's a trade-off, right, where you will give up some of your privacy in order to gain some functionality, and so we really need to make those trade-offs really clear to people, what information are we using and what's the benefit to them, and then ultimately leave it to user choice."[8] Mayer, who is very disciplined in her answers to questions about privacy, always offers statements very close to this. But Mayer and Google in general both misunderstand privacy. *Privacy* is not something that can be counted, divided, or "traded." It is not a substance or collection of data points. It's just a word that we clumsily use to stand in for a wide array of values and practices that influence how we manage our reputations in various contexts. There is no formula for assessing it: I can't give Google three of my privacy points in exchange

for 10 percent better service. More seriously, Mayer and Google fail to acknowledge the power of default settings in a regime ostensibly based on choice.

THE IRRELEVANCE OF CHOICE

In their 2007 book *Nudge: Improving Decisions about Health, Wealth, and Happiness*, the economist Richard Thaler and law professor Cass Sunstein describe a concept they call "choice architecture." Plainly put, the structure and order of the choices offered to us profoundly influence the decisions we make. So, for instance, the arrangement of foods in a school cafeteria can influence children to eat better. The positions of restrooms and break rooms can influence the creativity and communality of office staff. And, in the best-known example of how defaults can influence an ostensibly free choice, studies have demonstrated that when employer-based retirement plans in the United States required employees to opt in to them, more than 40 percent of employees either failed to enroll or contributed too little to get matching contributions from their employers. When the default was set to enroll employees automatically, while giving them an opportunity to opt out, enrollment reached 98 percent within six months. The default setting of automatic enrollment, Thaler and Sunstein explain, helped employees overcome the "inertia" caused by business, distraction, and forgetfulness.[9]

That choice architecture could have such an important effect on so many human behaviors without overt coercion or even elaborate incentives convinced Thaler and Sunstein that taking advantage of it can accomplish many important public-policy goals without significant cost to either the state or private firms. They call this approach "libertarian paternalism." If a system is designed to privilege a particular choice, they observe, people will tend to choose that option more than the alternatives, even though they have an entirely free choice. "There is no such thing as a 'neutral' design."[10]

It's clear that Google understands the power of choice architecture. It's in the company's interest to set all user-preference defaults to collect the

greatest quantity of usable data in the most contexts. By default, Google places a cookie in your Web browser to help the service remember who you are and what you have searched. By default, Google tracks your searches and clicks; it retains that data for a specified period and uses it to target advertisements and refine search results. Google gives us the power to switch off all these features. It even provides videos explaining how to do this.[11] But unless you act to change them, the company's default settings constitute your choices.

When Mayer and others at Google speak about the practices and policies governing their private-data collection and processing (otherwise known as privacy policies), they never discuss the power of defaults. They emphasize only the freedom and power that users have over their data. Celebrating freedom and user autonomy is one of the great rhetorical ploys of the global information economy. We are conditioned to believe that having more choices—empty though they may be—is the very essence of human freedom. But meaningful freedom implies real control over the conditions of one's life. Merely setting up a menu with switches does not serve the interests of any but the most adept, engaged, and well-informed.

Setting the defaults to maximize the benefits for the firm and hiding the switches beneath a series of pages are irresponsible, but we should not expect any firm to behave differently. If we want a different choice architecture in complex ecosystems such as the Web, we are going to have to rely on firms' acceding collectively to pressure from consumer groups or ask the state to regulate such defaults.

Google officials also don't acknowledge that completely opting out of Google's data-collection practices significantly degrades the user's experience. For those few Google users who click through the three pages it takes to find and adjust their privacy options, the cost of opting out becomes plain. If you do not allow Google to track your moves, you get less precise results to queries that would lead you to local restaurants and shops or sites catering to your interests. Google has to guess whether a search for "jaguar" is intended to generate information about the car or the cat. But if Google understands your interests, it can save you time when you shop. It can seem like it's almost reading your mind.

In addition, full citizenship in the Googleverse includes use of functions like Gmail and posting videos on YouTube, which require registration and allow Google to amass a much richer collection of data about your interests. Moreover, exploring such options can give you a pretty clear idea of the nature of the transaction between Google and its users; but for the vast majority of users, the fate of their personal data remains a mystery.

Opting out of any Google service puts the Web user at a disadvantage in relation to other users. The more Google integrates its services, and the more interesting and essential the services that Google offers, the more important Google use is for effective commerce, self-promotion, and cultural citizenship. So the broader Google's reach becomes—the more it Googlizes us—the more likely it is that even informed and critical Internet users will stay in the Google universe and allow Google to use their personal information. For Google, quantity yields quality. For us, resigning ourselves to the Google defaults enhances convenience, utility, and status. But at what cost?

THE PROBLEM WITH PRIVACY

Google is far from the most egregious offender in the world of personal data acquisition. Google promises (for now) not to sell your data to third parties, and it promises not to give it to agents of the state unless the agents of the state ask for it in a legal capacity. (The criteria for such requests are lax, however, and getting more lax around the world.) But Google is the master at using information in the service of revenue generation, and many of its actions and policies are illustrative of a much larger and deeper set of social and cultural problems.

In November 2007, Facebook, the social networking site most popular among university students and faculty, snuck in a surprise for its then-almost 60 million users (by 2010 it had 150 million users). With minimal warning, Facebook instituted what it called its Beacon program, which posted notes about users' Web purchases in the personal news feeds

on Facebook profiles. So if a user had purchased a gift for a friend on one of the Web commerce sites that were partners in the program, the purchase would be broadcast to all of that person's Facebook associates—most likely including the intended recipient of the gift. Facebook ruined a few surprises, but it had a bigger surprise in store for itself: a user rebellion. Within days, more than fifty thousand Facebook users signed up for a special Facebook group protesting the Beacon service and Facebook's decision to deny users the chance to opt out of it. The furor spread beyond Facebook. Major news media covered the story and quoted users who until then had been quite happy with Facebook but were now deeply alarmed at the inability to control Beacon or their Facebook profiles.[12]

This reaction caught Facebook executives by surprise. In 2006, when they had released the news feed itself as a way of letting people find out what their Facebook friends were up to, there had been a small protest. But within a few weeks, users got used to it and quieted down. Over time, users did not find news feeds too intrusive or troublesome, and they could turn off the service if they wished.

Facebook executives assumed that their users were not the sort who cared very much about personal privacy. After all, they readily posted photos from wild parties, lists of their favorite bands and books, and frank comments on others' profiles. All the while, Facebook executives were led to believe that young people today were some sort of new species who were used to online exposure of themselves and others, immersed in the details of celebrity lives via sites like PerezHilton.com and Gawker.com, obsessed with the eccentricities of reality television show contestants, and more than happy to post videos of themselves dancing goofily on YouTube.[13]

Then came the great Facebook revolt of 2010. By May of that year, users had alerted each other to the various ways that Facebook had abused their trust. Where once the service had allowed easy and trustworthy management of personal information (it was simple to choose who could and could not view particular elements of one's profile), it had slyly eliminated many of those controls. It had rendered much personal information openly available by default and made privacy settings

absurdly complicated to navigate and change. In addition, Facebook suffered some serious security lapses in early 2010. Soon a movement was born to urge friends to quit Facebook in protest. There is no way to tell how many people actually did quit, largely because Facebook would never release that number; moreover, completely deleting an account is very difficult. Facebook membership continued to grow worldwide throughout 2010, as did disgruntlement. Fundamentally, Facebook had become too valuable to people's lives to allow them to quit. The value, however, is in its membership, not in its platform. Facebook was only slightly chastened by the public anger.[14]

The cultural journalist Emily Nussbaum, writing in *New York* magazine in February 2007, stitched together some anecdotes about young people who have no qualms about baring their body parts and secrets on LiveJournal or YouTube. "Younger people, one could point out, are the only ones for whom it seems to have sunk in that the idea of a truly private life is already an illusion," Nussbaum wrote. "Every street in New York has a surveillance camera. Each time you swipe your debit card at Duane Reade or use your MetroCard, that transaction is tracked. Your employer owns your e-mails. The NSA owns your phone calls. Your life is being lived in public whether you choose to acknowledge it or not. So it may be time to consider the possibility that young people who behave as if privacy doesn't exist are actually the sane people, not the insane ones."[15]

Yet if young people don't care about privacy, why do they react angrily when Facebook broadcasts their purchases to hundreds of acquaintances? In fact, a study conducted by Eszter Hargittai of Northwestern University and danah boyd of Microsoft research demonstrated that young people in America have higher levels of awareness and concern about online privacy than older Americans do.[16] But still, isn't privacy a quaint notion in this era in which Google and Amazon—not to mention MI5, the U.S. National Security Agency, and the FBI—have substantial and detailed dossiers on all of us? Despite frequent warnings from nervous watchdogs and almost weekly stories about massive data leaks from Visa or AOL, we keep searching on Google, buying from Amazon, clicking through user agreements and "privacy" policies (that rarely if ever

actually protect privacy), and voting for leaders who gladly empower the government to spy on us.

Broad assumptions about the apparent indifference to privacy share a basic misunderstanding of the issue. Too often we assume that a concern with privacy merely represents a desire to withhold information about personal conduct, such as sexual activity or drug use. But privacy is not just about personal choices, or some group of traits or behaviors we call "private" things. Nor are privacy concerns the same for every context in which we live and move. *Privacy* is an unfortunate term, because it carries no sense of its own customizability and contingency. When we complain about infringements of privacy, what we really demand is some measure of control over our reputations. Who should have the power to collect, cross-reference, publicize, or share information about us? If I choose to declare my romantic status or sexual orientation on Facebook, I may still consider that I am preserving my privacy because I assume I am managing the release of that information in a context I think I understand. *Privacy* refers to the terms of control over information, not the nature of the information we share.[16]

Through a combination of weak policies, poor public discussions, and some remarkable inventions, we cede more and more control over our reputations every day. And it's clear that people are being harmed by the actions that follow from widespread behavioral profiling, whether it's done by the Transportation Security Agency through its "no-fly list" or Capital One Bank through its no-escape, high-fee credit cards for those with poor credit ratings.

Jay Gatsby could not exist today. The digital ghost of Jay Gatz would follow him everywhere. There are no second acts, or second chances, in the digital age. Rehabilitation demands substantial autonomy and control over one's record. As long as our past indiscretions can be easily Googled by potential employers or U.S. security agents, our social, intellectual, and actual mobility is limited.[17]

We learn early on that there are public matters and private matters, and that we manage information differently inside our homes and outside them. Yet that distinction fails to capture the true complexity of the privacy tangle. Because it's so hard to define and describe what

we mean by privacy and because it so often seems futile to resist mass surveillance, we need better terms, models, metaphors, and strategies for controlling our personal information. Here's one way to begin to think more effectively about the issue.

We each have at least five major "privacy interfaces," or domains, through which we negotiate what is known about us.[18] Each of these interfaces offers varying levels of control and surveillance.

The first privacy interface is what I call "person to peer." Early on, we develop the skills necessary to manage what our friends and families know of our predilections, preferences, and histories. A boy growing up gay in a homophobic family learns to exert control over others' knowledge of his sexual orientation. A teenager smoking marijuana in her bedroom learns to hide the evidence. If we cheat on our partners, we practice lying. These are all privacy strategies for the most personal spheres.

The second interface is one I call "person to power." There is always some information we wish to keep from our teachers, parents, employers, or prison guards because it could be used to manipulate us or expose us to harsh punishment. The common teenage call "Stay out of my room!" exemplifies the frustration of learning to manage this essential interface. Later in life, an employee may find it prudent to conceal a serious medical condition from her employer to prevent being dismissed to protect the company's insurance costs.

The third privacy interface is "person to firm." In this interface, we decide whether we wish to answer the checkout person at Babies "R" Us when she asks us (almost always at a moment when we are feeling weak and frustrated) for a home phone number. We gladly accept what we think are free services, such as discount cards at supermarkets and bookstores, that actually operate as record-keeping account tokens. The clerk at the store almost never explains this other side of the bargain.

The fourth interface is the most important because the consequences of error and abuse are so high: "person to state." Through the census, tax forms, drivers' license records, and myriad other bureaucratic functions, the state records traces of our movements and activities. The mysterious and problem-riddled "no-fly list" that bars people from boarding

commercial flights in the United States for unaccountable reasons is the best example. Because the state has a monopoly on legitimate violence, imprisonment, and deportation, the cost of being falsely caught in a dragnet warrants concern, no matter how unlikely it seems.

The fifth privacy interface is poorly understood and has only recently gained notice, although Nathaniel Hawthorne explained it well in *The Scarlet Letter.* It's what I call "person to public." At this interface, which is now located largely online, people have found their lives exposed, their names and faces ridiculed, and their well-being harmed immeasurably by the rapid proliferation of images, the asocial nature of much ostensibly "social" Web behavior, and the permanence of the digital record. Whereas in our real social lives we have learned to manage our reputations, the online environments in which we work and play have broken down the barriers that separate the different social contexts in which we move. On Facebook, MySpace, or YouTube, a coworker may be an online friend, fan, or critic. A supervisor could be a stalker. A parent could be a lurker. A prospective lover could use the same online dating service as a former lover. In real life, we may be able to keep relationships separate, to switch masks and manage what people know (or think they know) about us. But most online environments are intentionally engineered to serve our professional, educational, and personal desires simultaneously. These contexts or interfaces blend, and legal distinctions between public and private no longer hold up.[19] We are just beginning to figure out how to manage our reputations online, but as long as the companies that host these environments benefit directly from the confusion, the task will not be easy.

In *The Future of Reputation,* the law professor Daniel Solove relates the sad story of the "Star Wars Kid." In November 2002, a Canadian teenager used a school camera to record himself acting like a character from *Star Wars,* wielding a golf-ball retriever as a light saber. Some months later, other students at his school discovered the recording and posted it on a file-sharing network. Within days, the image of a geeky teen playing at *Star Wars* became the hit of the Internet. Thousands—perhaps millions—downloaded the video. Soon, many downloaders used their computers to enhance the video, adding costumes, special effects, and

even opponents for the young man to slay. Hundreds of versions still haunt the Web. Many Web sites hosted nasty comments about the boy's weight and appearance. Soon his name and high school became public knowledge. By the time YouTube debuted in 2005, the "Star Wars Kid" was a miserable and unwilling star of user-generated culture. He had to quit school. The real-world harassment drove his family to move to a new town. The very nature of digital images, the Internet, and Google made it impossible for the young man to erase the record of one afternoon of harmless fantasy. But it was not the technology that was at fault, Solove reminds us. It was our willingness to ridicule others publicly and our ease at appealing to free-speech principles to justify the spreading of everything everywhere, exposing and hurting the innocent along the way.[20]

No one made any money from this or the other events that Solove describes, and the state is neutral toward such incidents, so we can't blame market forces or security overreactions. But our appetite for public humiliation of others (undeserved or otherwise) should trouble us deeply. Like Hester Prynne in *The Scarlet Letter,* any one of us may be unable to escape the traces of our mistakes. We are no longer in control of our public personas, because so many of our fellow citizens carry with them instruments of surveillance and exposure such as cameras and video recorders. An advocate of Internet creativity and its potential to contribute to democratic culture, Solove treads lightly around any idea that might stifle creative experimentation. But even those of us who celebrate this cultural "mashup" moment would be delinquent if we ignored the real harms that Solove exposes.

The sociologist James Rule, in *Privacy in Peril,* emphasizes one point that is either muted in or absent from most other discussions about privacy and surveillance: data collected by one institution is easily transferred, mined, used, and abused by others. Companies such as ChoicePoint buy our supermarket and bookstore shopping records and sell them to direct-mail marketers, political parties, and even the federal government. These data-mining companies also collect state records such as voter registration forms, deeds, car titles, and liens in order to sell consumer profiles to direct-marketing firms. As a result of this

cross-referencing of so many data points, ChoicePoint knows me better than my parents do—which explains why the catalogs that arrive at my home better reflect my tastes than the ties my father gives me each birthday. Each data point, each consumer choice, says something about you. If you purchase several prepaid cell phones and a whole lot of hummus, you might be profiled as a potential jihadist. If you use your American Express Platinum card to buy a latte from Starbucks the same day that you purchase a new biography of Alexander Hamilton from Barnes and Noble in an affluent Atlanta ZIP code, you might be identified as a potential donor to a Republican election campaign.[21]

The privacy laws of the 1970s, for which Rule can claim some credit after his 1974 book *Private Lives and Public Surveillance,* sought to guarantee some measure of transparency in state data retention. Individuals should be entitled to know what the federal government knew about them and thus be able to correct errors. And there were to be strong limits on how government agencies shared such data.[22] As Rule explains in *Privacy in Peril,* such commonsense guidelines were eroded almost as soon as they became law. And in recent years, following pressure from the great enemy of public transparency and accountability, former vice president Dick Cheney, they have been pushed off the public agenda altogether. It's as if Watergate, the Church Committee report (which in 1975 exposed massive government surveillance of U.S. citizens and other illegal abuses of power by the CIA), and the revelations of FBI infiltration of antiwar protest groups never happened.[23]

Mass surveillance has been a fact of life since the eighteenth century. There is nothing new about the bureaucratic imperative to record and manipulate data on citizens and consumers. Digital tools just make it easier to collect, merge, and sell databases. Every incentive in a market economy pushes firms to collect more and better data on us. Every incentive in a state bureaucracy encourages massive surveillance. Small changes, such as the adoption of better privacy policies by companies like Google and Amazon, are not going to make much difference in the long run. So the only remedy is widespread political action in the public interest, much as we had in the 1970s. Passivity in the face of these threats to dignity and personal security will only invite the deployment of more

unaccountable technologies of surveillance. The challenge is too large and the risks too great.

"STREET VIEW" AND THE UNIVERSALIZATION OF SURVEILLANCE

Although there is indeed nothing new about the incentives for the state and businesses to keep tabs on private individuals, Google, with its Street View service in Google Maps, now enables individuals to undertake forms of surveillance of each other that have never been possible before. Our first reactions to seeing other people's streets and neighborhoods on our screens are hyperbolic. Once the service has been in place for a while, however, it generates broad interest and some utility. It also causes much anxiety without causing demonstrable harm. Only in a handful of places has Google been urged or forced to alter Street View significantly.

Google Street View allows users of Google Maps to take a 360-degree view, at ground level, of streets and intersections in many cities in (as of 2009) the Netherlands, France, Italy, Spain, Australia, New Zealand, and Japan, in addition to the United States and the United Kingdom. Google captures these images by sending automobiles known as Googlemobiles (Vauxhall Astras in the United Kingdom; Chevrolet Cobalts in the United States; Toyota Priuses in Japan), with special cameras mounted on their roofs, to drive along every street in a city.[24] Launched first in May 2007 in New York, San Francisco, and a handful of other large U.S. cities, Google Street View now covers thousands of small towns across the United States—even Charlottesville, Virginia (population 50,000). At first, American users flocked to the service to check for a record of their own lives, and perhaps to discover embarrassing or revealing aspects that Google might disclose. Many commentators declared the service to be too invasive for comfort.[25]

Generally, Google introduces a service in a standard way in all locations. If it generates attention or complaints, Google might tailor some policies for a specific locality. But the defaults Google sets for itself are consistent, if not constant. Responding to the initial criticisms of Street View, Google defended the service by saying—as it always does—that if anyone reported an image to be troubling, embarrassing, or revealing of personal information such as faces or vehicle license plates, Google would be happy to remove or smudge the image. But, as usual, the defaults were set for maximum exposure.

Critical suspicion of Google Street View faded after a few weeks. Over time, as no horror stories emerged, American Google users became accustomed to the new function and started coming up with creative ways to employ it. Google accurately gauged the sensibilities toward privacy and publicity of users in the United States, where practicality has a way of sweeping away any number of nebulous concerns.

As I studied the reaction in the spring of 2009, I wondered to what interesting uses my fellow Americans had put Google Street View in the two years since its launch. I solicited some input via Twitter, Facebook, and my blog. Overwhelmingly, my respondents (mostly technologically adept and highly educated) reported using Street View to scout out potential homes. Some used it to assess the prospects for parking in a busy area. Others wrote that they often remembered where a restaurant was, but could not remember its name or precise address, so they used Street View to locate it and recommend it to friends.[26]

A few of my responders had particularly interesting applications for Street View. David de la Peña, an architect based in Davis, California, uses Street View daily in his work:

> [Google Street View] is a very useful tool that I use regularly on community design and streetscape projects. It saves me from the drudgery of taking hundreds of photographs of a site, and the user interface is more intuitive than flipping through, say, 100 photographs of a street. For community design projects, it allows designers to see a neighborhood scene more or less from eye-level perspective. When we see a neighborhood from this experiential level, rather than from an aerial photograph, we have a better shot at creating more livable environments. The eye-level views also allow us to verify elements of a streetscape that just aren't apparent from a plan or an aerial photo, such as architectural character, yard and porch layouts, and tree types. For streetscape projects, the eye-level views give a very realistic view of a street's character, which are comprised of building facades; types and

varieties of street trees; locations of street lights and power poles; and arrangements of drive lanes, bicycle lanes, parking and sidewalks.

I started using it as soon as it was available. I immediately saw it as a useful tool to be added to my toolbox. Before [Google Street View], we relied primarily upon aerial photographs, MS Live 3D aerials, and photos we would take ourselves. Of course, none of these replaces on-the-ground research. I have been using [Google Street View], for example, on a project near Sacramento that is located 30 minutes from my office. We are trying to locate a new community center and park within a low-income neighborhood on foreclosed fourplexes that the city owns. GSV gave me a better sense than any other visual tool about the feel of each of the potential sites. Today I visited the sites to confirm our intuitions and to take more photographs. While walking the neighborhood, I was approached by eight different neighbors asking what I was doing. People naturally get suspicious when you're taking pictures of their homes, but if you're open to talking with them, other doors will open. I met a few single mothers who had great suggestions for locating a tot lot, and an on-site building manager who had suggestions for how the city deals with code compliance. These chance encounters gave me more information than any visual tool could, and more important, they helped me to establish as sense of trust.[27]

Cory Doctorow, an author, blogger, and activist, told me that he had used Google Street View to describe in detail a scene in San Francisco when he was writing his successful young-adult novel *Little Brother*. Here is the scene from his novel: "I picked up the WiFi signal with my phone's wifinder about three blocks up O'Farrell, just before Hyde Street, in front of a dodgy 'Asian Massage Parlor' with a red blinking CLOSED sign in the window. The network's name was HarajukuFM, so we knew we had the right spot."[28]

Doctorow wrote to me that he had written much of the novel while living in Los Angeles, but had done a lot of globe-trotting during that time, as well. "I think I was writing from Heathrow that day, or possibly Croatia. I know O'Farrell [Street] pretty well, but it had been a few years. I zoomed up and down the street with [Google Street View] for a few seconds until I had refreshed my memory, then wrote."[29]

One objection to Street View in the United States came from Aaron and Christine Boring, a couple living in Pittsburgh, Pennsylvania.

Concerned that Street View included clear images of their driveway and house, which was sited far back from the street, the couple sued Google in April 2008 seeking $25,000 in damages and alleging Google had in effect trespassed on their property through the power of its lenses. The judge in the case dismissed their claims in February 2009 because the couple had not taken the simple step of requesting that Google remove the offending images. In other words, as far as the court was concerned, as soon as the Borings had discovered the images of their property, they could have acted in a low-cost way to alleviate the conflict. However, that decision did not take account of how long the images had been public or how many people might have seen them.[30]

Today Google Street View, perhaps the most pervasive example of the Googlization of us, barely causes a gasp in the United States. That was not the case in Canada, parts of Europe, or in Japan.

In late spring 2009, Google was planning to extend Street View to Canadian cities. Canada has much stronger data-privacy laws than the United States does, and its people are far less likely to acquiesce in the aims of rich American companies. Along with much of Western Europe, Canada upholds a general prohibition on the photography of people without their permission, with special exceptions for journalism and art. As early as 2007, Google announced that it would tailor Street View to conform to Canadian law by blurring faces and license plates—as if that were a special concession for Canada.[31] In fact, faces and license plates were blurred in street views of the United States and the rest of the world as well. By April 2009, just before the Canadian launch of Street View, Google still claimed that its imperfect, machine-driven blurring technology would comply with Canadian law.[32]

The problem with the blurring process, in addition to a small rate of complete failure, is that a face is not the only feature that defines one's identity. For example, I used to live near the corner of Bleecker Street and LaGuardia Place in New York City. Every day I walked a white dog with brown spots. I drove a black car. And I am more than two meters tall, bald, and heavy. Any shot of me on Google Street View in that neighborhood would be instantly recognizable to hundreds of people who know me even casually. If one of those images seemed to implicate

me in, for example, the activities of one of the many illegal gambling establishments within ten blocks of my apartment, my personal and professional reputation could be harmed severely. Canadian privacy advocates articulated the same concerns about the blurring technology in the weeks leading up to the launch of Google Street View, but their arguments did not sway either the company or the Canadian government.

In May 2009, a data-privacy official in the city of Hamburg, Germany, threatened to fine Google over Street View unless the city received a written guarantee that the service would conform with German privacy laws—specifically, the prohibition against the publication of images of people or their property without their explicit consent. Other German cities also protested Street View. Residents of the city of Kiel had put stickers on their front doors demanding that Google not photograph their homes—a nonelectronic way of opting out of Street View.[33] The city of Molfsee forbade Google vehicles from trawling the streets in 2008.[34] And in May 2010 German privacy officials criticized Google for collecting the addresses of unsecured wireless routers throughout Germany with the same cars that the company uses to create Street View. Law-enforcement officials around the world, including the United States, started investigations of Google's data-surveillance practices.[35]

In May 2009 Greece banned Street View on the grounds that Google did not have an adequate plan for notifying residents of town and cities that Google cars would be coming through. Greek authorities also wanted details about the data-storage and protection measures Google would use for the images. In reaction to the Greek decisions, a Google spokesperson uttered the standard mantra to the *Times* of London: "Google takes privacy very seriously, and that's why we have put in place a number of features, including the blurring of faces and license plates, to ensure that Street View will respect local norms when it launches in Greece."[36]

The tension over local norms revealed itself through the reaction in Japan when Street View was launched in 2008. A group of lawyers and professors called the Campaign against a Surveillance Society staged a protest against the service, but these initial objections did not deter

the company or generate government reaction.[37] Once Japanese Web users found the standard array of embarrassing images on the service, however, concern about it started to build.[38]

One search-engine professional, Osamu Higuchi, posted an open letter to Google staff in Japan on his blog in August 2008. The letter urged Google staff to explain to their partners in the United States that Street View demonstrates a lack of understanding of some important aspects of daily life in Japan. Osamu urged Google to remove largely residential roads from Street View. "The residential roads of Japan's urban areas are part of people's living space, and it is impolite to photograph other people's living spaces," wrote Osamu. He pointed out that in the United States, the boundary between private space and public space is the property line that abuts a public road. "For people living in Japan, though, the situation is quite the opposite," wrote Osamu. "The residential street in front of a house, the so-called 'alleyway,' feels more like a part of one's own living space, like part of the yard." Osamu explained that private citizens care for, personalize, and decorate these narrow public streets as if they were part of their own land. "When we walk along an alleyway like that, we don't stare at and scrutinize the houses along the way," Osamu wrote. The population density of urban Japan demands a strong sense of mutual discretion, he argued. One does not peep into people's limited and exposed living spaces.

The main problem with Street View, Osamu explained, is the asymmetry of the gaze. A person walking down the street peering into residents' yards would be watched right back by offended residents, who would consider calling the police to report such dangerous and antisocial behavior. But with Google Street View, the residents can't see or know who is peeping.[39] Osamu's pleas and concerns were shared by enough others in Japan that, by May 2009, Google announced it would reshoot its Street View images of Japanese cities with the cameras mounted lower, to avoid peering over hedges and fences.[40]

Certainly, the physical and social geography of Japan and its accompanying notions of privacy are aspects of its culture that Google's engineers and corporate leaders might understandably have failed to grasp. But Osamu's analysis of the asymmetry of the gaze explains much

of the more general, global aversion to Street View. Only in a handful of places do Google's defaults run afoul of local laws; in most of the world, the utility of Street View has so far trumped poorly articulated concerns about asymmetry or lack of reciprocity. But everywhere in the world, at least some people find Street View a little bit creepy; some, as in Japan, are deeply offended by it.

The reaction in Britain in 2009 echoed the American reaction from 2007—but with a few significant amplifications and ironies. On the day it unveiled Street View, Google had its busiest day ever in the United Kingdom, with a 41 percent increase in traffic.[41] Google already controlled more than 90 percent of the Web search traffic in the United Kingdom.[42]

Many of the problems that first day were fairly predictable: a few embarrassing scenes were caught on camera; a few sensitive images had to be deleted on request. And the *Independent* newspaper misquoted a Google engineer as saying that Google's technology catches and blurs "99.9" percent of faces and license plates automatically. That turned out to be "a figure of speech," as a Google spokesperson told the *Independent* later. "The technique is not totally perfect. The idea is not to blur every single face, only those that can be clearly identified."[43]

In fact, enough identifying details were preserved in British Street View images to cause a public backlash. Thousands of people requested that Google remove specific images of their homes and businesses, including the former prime minister Tony Blair. A former criminal wrote a column in the *Sun* claiming that Street View would be a gift to criminals. Bloggers quickly found and copied embarrassing images, including a man vomiting outside a pub and another leaving an adult video store. The ensuing fury exceeded all reactions in the United States two years before. And although Google acted quickly to remove these troubling images, they were preserved in other parts of the Web—and easily discoverable via Google Image Search.[44]

The most dramatic reaction to Google Street View came from residents of an affluent village in Cambridgeshire called Broughton. When one of the village residents spotted the Googlemobile, with a camera perched on its roof, slowly cruising his neighborhood, he raced into the street to

block it, called the police, and started calling for neighbors to join him. Dozens formed a human chain to prevent the Google car from continuing. The residents of Broughton claimed that the presence of their homes on Google Street View would invite the attention of burglars (though they offered no evidence that a burglar has actually ever used Google Street View to plan a crime or that such information would be more useful to burglars than simply walking the neighborhood themselves). The move to block the Google car from the streets of Broughton generated significant worldwide attention, but it also provoked a blowback. Soon, Google Street View defenders started a campaign to drive the streets of Broughton, taking photographs and posting them on the social photography site Flickr.[45]

Ultimately, neither Broughton nor Google suffered substantial or long-term damage from these high-profile incidents. If anything, the news coverage and peer-to-peer buzz about Street View enhanced Google's presence in Britain. In other words, the very panic that journalists, politicians, activists, or angry citizens generate at the imposition of something as strange and unnerving as Street View creates a tremendous amount of interest in the service, as well as voyeuristic curiosity about what it shows. Google officials can then boast of the increase in usage as evidence of public acceptance, rather than evidence of wariness and concern about the service.

Wherever Street View has been launched, a company spokesperson has repeated that "privacy is very important to Google" without ever defining exactly what the company means by privacy or addressing what a culture considers private or sacrosanct. The company always reiterates that individuals may opt out and request that an image be removed; it does not, however, explain that such a request takes at least three steps of effort and that several hours, or even days, may elapse before the offending images disappear from Google Street View.

In March 2009, just days after the launch of Google Street View in the United Kingdom, Google had to remove an image of a naked toddler who was playing in a garden square in North London.[46] Although Google's policy operated as the company promised, the public exposure could

still have subjected this child or his parents to ridicule and shame. Street View had been up for at least forty-eight hours by the time the image of the child was discovered and Google alerted. There is no way to tell how many people saw or made copies of the image in that period. It's likely that friends and neighbors of that child could identify him from such an image, even if it his face were blurred, simply from the setting or from the images of adults in the area.

Moreover, not everyone featured in an embarrassing image is likely to find it within forty-eight hours of its appearance on the Internet. Not everyone uses Google Maps or Street View. Not every neighborhood is filled with computer users. To defeat Google's default settings, you have to be looking out for yourself, your property, your family, and your neighborhood. As always, the technologically proficient and aware suffer little harm and gain greatly from the convenience of Google Street View. Those who are not proficient, perhaps by choice but perhaps because of age, disability, or lack of means, are much more vulnerable under such a system. Because of this and other high-profile incidents, by April 2010 the United Kingdom's information commissioner, Christopher Graham, had called for Google to flip its defaults and grant privacy protection first, rather than placing the burden on the individual to opt out. "It is unacceptable," Graham wrote to Eric Schmidt, "to roll out a product that unilaterally renders personal information public, with the intention of repairing problems later as they arise."[47]

A few days after the Broughton incident, I had a long conversation with Peter Barron, head of communication and public affairs for Google in the United Kingdom, Ireland, Belgium, the Netherlands, and Luxembourg. "This was actually a fantastically successful launch" in the United Kingdom, Barron told me over a Skype connection.

> We had record numbers of people visiting Google Maps. Many, many millions of people used and enjoyed and found the product extremely useful. We had a very small number of complaints—complaints in the hundreds—about the fact that people's houses were up or maybe their faces weren't blurred. We explained to people that these images could be removed if you wanted that and this was carried out very, very quickly, usually within an hour or two. . . . The truth is, we expected a degree of controversy. In many countries where Street View has launched, there is a degree of controversy within the first few weeks. There is an element of the shock of the new. People aren't used to Street View and perhaps feel a bit uncomfortable with it in the beginning. But after a couple of weeks it tends to die down.[48]

INFRASTRUCTURAL IMPERIALISM

Barron was correct about the ebb of panic and concern about Google Street View after a few weeks. British newspapers moved on to other issues. The public began to use Google Maps and Street View to find its way around London. Barron emphasized that there was a substantial difference between the ways urban and rural areas of the United Kingdom reacted to Google Street View. "People in the cities are very used to having themselves publicly photographed, and in the countryside less so," Barron told me. That's certainly true in the United Kingdom, with the heaviest surveillance of any liberal and industrialized state in the world. Video cameras are posted on almost every street corner in the major cities of the United Kingdom.[49] The BBC estimates that there are as many as 4.2 million surveillance cameras—both public and private—operating in Britain. That's about one for every fourteen people.[50] After decades of terrorism at the hands of Irish Republican Army members, and more recently Islamic radicals, the people of the United Kingdom have grown to accept high levels of surveillance in their cities, even though such a lattice of lenses has not contributed to any measurable decrease in crime or increase in security.[51] There has certainly been a cost, however. Privacy International ranks the United Kingdom as the worst democracy at protecting individual privacy. (Again, the group is fuzzy on its definition of privacy.) The United Kingdom ranks with Malaysia and China in terms of the levels and reach of state surveillance.[52]

It's puzzling why people in the United Kingdom, who are so used to assuming their image is being captured on camera, reacted so viscerally to the idea of an American corporation taking static photographs in which most people are difficult to identify, and making those photographs available to anyone with a computer. The negative reactions in

Germany and Japan are more readily understandable. After the invasive and destructive state surveillance that Germans experienced during the Nazi era and in Soviet-dominated East Germany, one can understand the wariness with which German citizens consider Google's initiatives. And the density of Japanese cities explains the Japanese aversion to Street View. The people of the United Kingdom, by contrast, have consistently elected leaders who support expanding technologies of surveillance rather than limiting them. And Britain after Margaret Thatcher, John Major, Tony Blair, and Gordon Brown is hardly an anticorporate or anti-American culture. So it's possible that the reaction to Google Street View was a reflection of the sensationalism endemic to British journalism rather than a deeper cultural issue. Or perhaps some people in the United Kingdom have had enough of living under constant state and commercial scrutiny.[53] Maybe a few of them chose to make a stand against an obvious and less powerful offender than their own state and corporate bureaucracy.

After examining this array of reactions to Street View and Google's unvarying approach to its introduction in diverse cultural, political, and historical contexts, I wondered whether Google operated with a universalizing ideology. Did the company consider local differences and concerns? I didn't see any evidence of it in the Street View saga.

Google's CEO, Eric Schmidt, has commented that he sees few, if any important cultural differences among Google users around the world. In a conversation at Princeton University with the computer scientist Ed Felten in May 2009, Schmidt said, "The most common question I get about Google is 'How is it different everywhere else?' and I am sorry to tell you that it's not. People still care about Britney Spears in these other countries. It's really very disturbing." Schmidt said his experience analyzing Google users' habits around the world had convinced him that "people are the same everywhere." Schmidt went on to give the standard Google line that the company respects local laws (as, of course, it must). But his universalist statements are consistent with much of the company's behavior.[54]

The tension between universalism and particularism in the age of rapid globalization is well documented. It's clear after decades of argument that ideologies such as market fundamentalism, liberalism (with its imperative for free speech), techno-fundamentalism, and free trade are no longer simply "Western"—if they ever were.[55] It's too simple (and ahistorical) to tag such ideologies as merely imperialistic. But it is true that they are universalizing. They carry strong assumptions that people everywhere have the same needs, values, and desires—even if they don't yet know it themselves.

Cultural imperialism has become a useless cliché. The academic cultural-imperialism thesis is in severe need of revision. Once dominant among leftist critics in the 1970s and 1980s, it has been supplanted and modified by the rise of cultural studies.[56] Yet it still resonates in public discourse about the global North and the global South and in some anxious corners of academia.[57] While those who complain about cultural imperialism cite the ubiquity of KFC in Cairo and McDonald's in Manila, anxious cultural protectionists in the United States quiver at the sound of Spanish spoken in public or mosques opening in Ohio. Some American nationalists argue that cultural imperialism would be good for the world, because Americans have so much figured out.[58] Others dodge its complications by celebrating "creolization" at all costs, while ignoring real and serious imbalances in the political economy of culture.[59]

Although the evidence for cultural imperialism is powerful only when selectively examined, the evidence for the recent emergence of what we might call "infrastructural imperialism" is much stronger. There are imbalances of power in global flows of culture, but they are not what traditional cultural-imperialism theorists claim them to be.

If there is a dominant form of cultural imperialism, it concerns the pipelines and protocols of culture, not its products—the formats of distribution of information and the terms of access and use.[60] It is not exactly content-neutral, but it is less necessarily content-specific than theorists of cultural imperialism assume. The texts, signs, and messages that flow through global communications networks do not carry a clear and unambiguous celebration of ideas and ideologies we might lazily label Western, such as consumerism, individualism, and secularism.[61] These commercial pipelines may instead carry texts that overtly criticize

and threaten the tenets of global capitalism, such as albums by the leftist rock band Rage against the Machine, films by Michael Moore, and books by Naomi Klein. Time Warner does not care if the data inscribed on the compact discs it sells simulates the voice of Madonna or of Ali Farka Touré. What flows from North to South does not matter as much as how it flows, how much revenue the flows generate, and who uses and reuses them. In this way, the Googlization of us has profound consequences. It's not so much the ubiquity of Google's brand that is troubling, dangerous, or even interesting: it's that Google's defaults and ways of doing spread and structure ways of seeking, finding, exploring, buying, and presenting that influence (though they do not control) habits of thought and action. These default settings, these nudges, are expressions of an ideology.[62]

Because Barron had watched closely as Google introduced a number of high-profile services to several European countries, I asked him how Google navigates cultural differences and whether he was concerned that Google's universalist tendencies would cause trouble in places that do not embrace either the technocratic imperative or a cultural commitment to free expression.

"Google starts from a position that we seek to make information available to the widest number of people," Barron explained to me. "Google is built on free expression. In the United States, that has been embraced enthusiastically. Elsewhere, there are different cultural norms, different laws, and different customs. We are committed to abiding by the laws of the countries that we operate in, but also taking into account local norms and local customs."[63]

This was the standard line. So I asked Barron for an example of how Google had tailored its practices to conform to a local concern. He had a good one at hand. "Over the last year, we had some problems with gang-related videos, with boys brandishing weapons and making general threats on these videos." Under YouTube's established guidelines, these videos would not have been considered violations, Barron said. But "because of the nature of the concern in the UK, YouTube decided to alter their guidelines for the UK to cover gang-related videos."

In this case, and that of the decision to reshoot the entire nation of Japan for Google Street View, Google altered its operations in response to reactions in particular environments. This is good practice, even if, as in Japan, it took a year for the company to concede the point. Google has found this approach to globalization workable in almost every context in which it operates. The vast majority of those who use Google find services such as Street View more beneficial to them than harmful. The few who might be offended by the standard and universal policies of Google are of little importance to the company. After all, we are not Google's customers: we are its products. Google can afford to alienate a few thousand of us, because for most of those who are connected to the cosmopolitan global culture of the Internet, living without Google is not tenable. For every person who complains about Street View, millions more find it useful.

THE GOOGLIZED SUBJECT

This universalization of surveillance via infrastructural imperialism, and its general acceptance, merits critical attention. However, most work surveying the troubling implications of mass surveillance has fundamentally misrepresented its nature. It assumes that surveillance of the kind that Google makes possible is analogous to the theory of social control described by Michel Foucault as the Panopticon. But this trope has exhausted its utility. The original Panopticon, conceived by Jeremy Bentham, was a design for a circular prison with a central watchtower, in which all the inmates would behave because they would assume that they were being observed at all times. Foucault argued that state programs to monitor and record our comings and goings create imaginary prisons that lead citizens to limit what they do out of fear of being observed by those in power. The gaze, the theory goes, works as well as iron bars to control the behavior of most people.[64] Those who write about privacy and surveillance usually can't help invoking the Panopticon to argue that the great harm of mass surveillance is social control.[65]

However, the Panopticon model does not suffice to describe our current predicaments. First, mass surveillance does not inhibit behavior: people may act weird 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. Long before closed-circuit cameras, cities were places to be seen, not to disappear. Today, reality television suggests that there may be a positive relationship 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 under a nontotalitarian state.

Certainly the Stasi in East Germany exploited the controlling power generated by widespread awareness of surveillance and the potential for brutal punishment for thought crimes.[66] But that is not the environment in which most of us now live. And unless the Panopticon is as visible and ubiquitous as agencies like the Stasi, it cannot influence behavior as Bentham and Foucault assumed it would.

But more important, the forces at work in Europe, North America, and much of the rest of the world are the opposite of a Panopticon: they involve not the subjection of the individual to the gaze of a single, centralized authority, but the surveillance of the individual, potentially by all, always by many. We have a "cryptopticon" (for lack of a better word). Unlike Bentham's prisoners, we don't know all the ways in which we are being watched or profiled—we simply know that we are. And we don't regulate our behavior under the gaze of surveillance: instead, we don't seem to care.

In fact, that's just how those doing most of today's surveillance want it. ChoicePoint, 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 the mass are the things about which we are most passionate. Our passions, predilections, fancies, and fetishes are what we are likely to spend our surplus cash on and thus make

us easy targets for precise marketing. For example, almost everybody kind of likes Fleetwood Mac's 1977 album *Rumours*, so the fact that I bought it long ago says nothing special about me. But I am one of the few people who really digs their earlier, bluesy *Then Play On*. That says something about me that might be useful to marketers. As Joseph Turow explained in *Niche Envy*, and *Wired* editor Chris Anderson describes in *The Long Tail*, 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.[67]

Even the modern liberal state, like those of North America and Western Europe, wants us to be ourselves. It wants subversive and potentially dangerous people to reveal themselves through their habits and social connections, not to slink away and hide in the dark.[68] Repressing dissent and subversion does not eliminate them: the Stasi lost its efforts to control the East German people despite the enormous scale of its operations and the long-lasting damage it inflicted on both the observers and the observed. In the twenty-first-century liberal state, 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 both harmless and remarkably useful to the powerful.

Living so long under the dominance of market fundamentalism and techno-fundamentalism, we have come to accept the concept of choice and the exhortation of both the Isley Brothers and Madonna, "Express yourself," as essential to living a good life. So comforted are we by offers of "options" and "settings" made by commercial systems such as Facebook and Google that we neglect the larger issues. We weave these services so firmly and quickly into the fabrics of our daily social and intellectual lives that we neglect to consider what dependence might cost us. And many of us who are technically sophisticated can tread confidently through the hazards of these systems, forgetting that the

vast majority of people using them are not aware of their pitfalls or the techniques by which users can master them. Settings only help you if you know enough to care about them. Defaults matter all the time. Google's great trick is to make everyone feel satisfied with the possibility of choice, without actually exercising it to change the system's default settings. But as I show in the next chapter, for people living in illiberal political contexts, different vulnerabilities exist.

about Google from an e-mail list called Red Rock Eater, written and edited by Phil Agre, a professor of information studies at UCLA. Like many Web geeks of the late 1990s, I read Agre's newsletter religiously. If he liked Google, chances were good that I would as well.

Unlike everything else on the Web at that time, Google lacked clutter. It was simple, fast, and effective. Before Google essentially solved the problem of managing and filtering the Web for us, we relied on the pages we liked and trusted to provide links to other pages we might like and trust. But Google was aggregating all of that linking and clicking, making it a general process of ranking and linking. It was brilliant.

And then, within hours of using Google for the first time, I started thinking through the consequences of Google becoming the institution that governs the Web. I had no idea how quickly that notion would grow into an obsession.

While composing this book I often used my blog, Googlization of Everything, to solicit feedback and comments from Web users. Back in July 2008 I posted a simple query: "Do you remember the first time you used Google? When was it? How did you hear about Google? What was your first impression?" The response was overwhelming: 216 people posted their stories to my blog, and 36 more posted comments to BoingBoing, the most popular blog in the world, after it linked to my query.

From the website developer and critic Waldo Jaquith:

> It's difficult to properly emphasize how truly terrible search engines were in 1998. AltaVista and HotBot were as good as it got, and that's saying very little. Results were basically sorted randomly. Choosing a search engine was really based on faith more than anything else. . . . And then along came Google.

From the author Clay Shirky:

> Late 90s—I'd been the CTO of a web shop in Manhattan, and we'd always spend a lot of time with new clients on the "nav bar issue"—what was the best set of links to put in the home page navigation? . . . we spent a *lot* of time studying Yahoo's front-page taxonomy—the whole Web, broken down into 14 top-level categories. And then I saw Google, which had no taxonomy at all. just search. I . . . switched immediately, as many of us did in those days, but I didn't realize what a big deal it was until 2000. I was at a geek dinner of two dozen people, hosted by Tim O'Reilly, on a completely different subject. . . . At that dinner, Tim said "I know this doesn't have anything to do with the matter at hand, but out of curiosity, how many people here use Google?" Every hand went up.

From library consultant Karen Coyle:

> I was chatting with the brother of one of the Google founders. He told me that his brother was working on a new search engine that would be better than anything ever seen before. I tried to argue that it would still be limited by the reality of the full-text search. I probably looked at Google when it was first made available, and I was pretty un-impressed. Just more keyword searching. Today I use it constantly, but I'm very aware of the fact that it works quite well for nouns and proper nouns (people, companies, named things), and less well for concepts. . . . . I think of it as a giant phone book for the Internet, not as a classification of knowledge.

Many of the people who responded to my query were information or Web professionals. They were certainly the earliest to embrace Google and recognize its value. They quickly spread the word to their immediate friends and family. From there, it grew to span the world within five years. We were so thrilled to find so much, so easily, that we hardly stopped to ask questions. We became true believers.

CHAPTER 3. THE GOOGLIZATION OF US

1. Lev Grossman, "Time's Person of the Year: You," *Time*, December 13, 2006.
2. See Robert L. Mitchell, "What Google Knows about You," *Computer World*, May 11, 2009.
3. Michael Zimmer, "Privacy on Planet Google: Using the Theory of Contextual Integrity to Clarify the Privacy Threats of Google's Quest for the Perfect Search Engine," *Journal of Business and Technology Law* 3 (2008): 109.
4. "Privacy Policy: Google Privacy Center," Google.com, www.google.com/privacypolicy.html, accessed March 11, 2009.
5. Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," *SSRN eLibrary*, August 13, 2009, http://papers.ssrn.com.
6. "Privacy Policy," Google.com. March 11, 2009.
7. Arshad Mohammed, "Google Refuses Demand for Search Information," *Washington Post*, January 20, 2006.
8. *Charlie Rose Show*, 2009, available at http://video.google.com.
9. Richard Thaler and Cass Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness* (New Haven, CT: Yale University Press, 2008), 109.
10. Ibid., 3.
11. *Google Search Privacy: Plain and Simple*, 2007, www.youtube.com.
12. Louise Story and Brad Stone, "Facebook Retreats on On-Line Tracking," *New York Times*, November 30, 2007.
13. Warren St. John, "When Information Becomes T.M.I.," *New York Times*, September 10, 2006.

14. Jenna Wortham, "Facebook Glitch Brings New Privacy Worries," *New York Times*, May 5, 2010; Laura M. Holson, "Tell-All Generation Learns to Keep Things Offline," *New York Times*, May 8, 2010.

15. Emily Nussbaum, "Say Everything: Kids, the Internet, and the End of Privacy: The Greatest Generation Gap since Rock and Roll," *New York*, February 12, 2007.

16. dana boyd and Eszter Hargittai, "Facebook Privacy Settings: Who Cares?" *First Monday* 15, no. 8 (2010), www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3086/2589.

16. Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford, CA: Stanford Law Books, 2010).

17. Michael Zimmer, "The Quest for the Perfect Search Engine: Values, Technical Design, and the Flow of Personal Information in Spheres of Mobility," PhD diss., New York University, 2007.

18. I am basing the notion of privacy interfaces on the work of the foremost philosopher of privacy and ethics in online environments, Helen Nissenbaum. See her most influential work on the subject, "Privacy as Contextual Integrity," *Washington Law Review* 79, no. 1 (2004): 101–39. Also see Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford, CA: Stanford Law Books, 2010).

19. Helen Nissenbaum, "Protecting Privacy in an Information Age: The Problem of Privacy in Public," *Law and Philosophy* 17, no. 5 (1998): 559–96.

20. Daniel Solove, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* (New Haven, CT: Yale University Press, 2007). Solove's earlier book, *The Digital Person: Technology and Privacy in the Information Age*, set the standard for explaining what is at stake in online data collection and analysis. In it, Solove walks us through the construction of "digital dossiers" in the "person to firm" and "person to state" interfaces and outlines the potentials for abuse. *The Digital Person* is significant because it came out long enough after September 11, 2001, to take into account the U.S. government's notorious Total Information Awareness program and other efforts at behavioral profiling. It supplemented the best previous book of social and media theory applied to massive digital data collection and private-sector surveillance, Oscar Gandy's *The Panoptic Sort*. But 2004 was a long time ago in matters of government surveillance. Solove could not have predicted the revelation in 2005 that the NSA was monitoring American phone calls through an illegal secret program that relied on the cooperation of the major telecommunication companies.

21. James Rule, *Privacy in Peril* (Oxford: Oxford University Press, 2007).

22. James Rule, *Private Lives and Public Surveillance: Social Control in the Computer Age* (New York: Schocken Books, 1974).

23. Ibid.

24. In May 2008, Google announced it would deploy special tricycles to extend Street View to roads and alleys in which cars would have trouble navigating. The tricycle experiment began in Italy but was soon used throughout Europe. See Google, "Trike with a View," Press Centre, May 18, 2009, www.google.co.uk/intl/en/press/pressrel/20090518_street_view_trike.html.

25. Elinor Mills, "Are Google's Moves Creeping You Out?" *CNET News*, June 12, 2007.

26. Siva Vaidhyanathan, "Ever Use Google Street View for Something Important?" Googlizationofeverything, blog, March 29, 2009, www.googlizationofeverything.com.

27. Ibid.

28. Cory Doctorow, *Little Brother* (New York: Tor Teen, 2008).

29. Cory Doctorow, quoted in Vaidhyanathan, "Ever Use Google Street View?"

30. Jemima Kiss, "Google Wins Street View Privacy Case," *Guardian*, February 19, 2009.

31. "Google Eyes Canada Rollout of Discreet Street View," Reuters, September 24, 2007, http://uk.reuters.com; "Google's Street View Blurred by Canadian Privacy Concerns," CanWest News Service, www.canada.com.

32. Tamsyn Burgmann, "Google to Blur Faces in Canadian Street View," *Star* (Toronto), April 5, 2009. One Conservative member of Parliament, Pierre Poilievre of Ontario, switched positions on Street View. At first he questioned the propriety and utility of the service. Less than a week later he wrote an op-ed piece advocating the service and complaining that Canadian law seemed to impede it. See Michael Geist, "Poilievre Changes His Tune on Privacy and Google Street View," Michael Geist, April 2, 2009, www.michaelgeist.ca/content/view/3797/125/. See also Vito Pilieci, "MP wants Google Boss to Explain Street Cameras," *Ottawa Citizen*, March 30, 2009; Pierre Poilievre, "Pierre: Updating the Law to Deal with Google," *National Post*, April 2, 2009.

33. Kevin J. O'Brien, "Google Threatened with Sanctions over Photo Mapping Service in Germany," *New York Times*, May 20, 2009.

34. "Hamburg Threatens Google Street View Ban," *Local: Germany's News in English*, May 18, 2009, www.thelocal.de.

35. Kevin J. O'Brien, "New Questions over Google's Street View in Germany," *New York Times*, April 29, 2010.

36. Mike Harvey, "Greece Bans Google Street View," *TimesOnline*, May 13, 2009, http://technology.timesonline.co.uk.

37. "Japanese Group Asks Google to Stop Map Service," Reuters, December 19, 2008.

38. James, "More Sensational News from Japan about the Dangers of Google Street View," *Japan Probe*, January 11, 2009.

39. Chris Salzberg and Higuchi Osamu, "Japan: Letter to Google about Street View," Global Voices Online, August 8, 2008, http://globalvoicesonline.org.

40. Stephen Kamizura; "Google Forced to Retake All Street View Images in Japan," *DailyTech*, May 18, 2009, www.dailytech.com; "Google to Reshoot Street Views of Japanese Cities," *Japan Today*, May 14, 2009, www.japantoday.com.

41. Jo Adetunji, "Google Hit by Privacy Protests over Its Tour of British Cities," *Guardian*, March 21, 2009.

42. Alex Chitu, "Google's Market Share in Your Country," Google Operating System: Unofficial News and Tips about Google, blog, March 13, 2009, http://googlesystem.blogspot.com.

43. Jane Merrick, "Google Street View Forced to Remove Images," *Independent*, March 22, 2009.

44. Ibid.; Urmee Khan, "Google Removes Picture of Naked Child from Street View," *Daily Telegraph*, March 22, 2009; "Public Urged to Report Google Street View Fears," *Independent*, March 21, 2009.

45. Andy Dolan and Eddie Wrenn, "Watch Out Broughton! Street View Fans Plan to Descend on 'Privacy' Village for Photo Fest," *Daily Mail*, April 4, 2009.

46. Khan, "Google Removes Picture."

47. Paul Harris, "Watchdog Calls for Tighter Google Privacy Controls," *Guardian*, April 20, 2010.

48. Peter Barron, personal communication, April 21, 2009.

49. Jeffrey Rosen, *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age* (New York: Random House, 2004); B. Yesil, "Watching Ourselves," *Cultural Studies* 20, no. 4 (2006): 400–416.

50. "Britain Is 'Surveillance Society,'" BBC News, November 2, 2006, http://news.bbc.co.uk.

51. "Report Says CCTV Is Overrated," *Guardian*, June 28, 2002; Alan Travis, "Police and CCTV: Pictures Too Poor, Cameras in Wrong Place," *Guardian*, October 20, 2007.

52. "Britain Is 'Surveillance Society.'"

53. Sarah Lyall, "Britons Weary of Surveillance in Minor Cases," *New York Times*, October 25, 2009.

54. Eric Schmidt, presentation at Princeton Colloquium on Public and International Affairs, 2009, video available at www.youtube.com.

55. Amartya Sen, *Development as Freedom* (Oxford: Oxford University Press, 2001); Amartya Sen, *Identity and Violence: The Illusion Of Destiny* (New York: W.W. Norton, 2007).

56. Herbert Schiller, *Communication and Cultural Domination* (White Plains, N.Y.: M.E. Sharpe, 1976). John Tomlinson, *Cultural Imperialism: A Critical Introduction* (Baltimore, MD: Johns Hopkins University Press, 1991).

57. Steven Feld, "A Sweet Lullaby for World Music," *Public Culture* 12, no. 1 (January 1, 2000): 145–71.

58. David Rothkopf, "Praise of Cultural Imperialism?" *Foreign Policy*, no. 107 (1997): 38–53.

59. Tyler Cowen, *Creative Destruction* (Princeton, NJ: Princeton University Press, 2002).

60. Siva Vaidhyanathan, "Remote Control: The Rise of Electronic Cultural Policy," *Annals of the American Academy of Political and Social Science* 597 (January 2005): 122–33; Siva Vaidhyanathan, *The Anarchist in the Library: How the Clash between Freedom and Control Is Hacking the Real World and Crashing the System* (New York: Basic Books, 2004).

61. Edward Herman and Robert McChesney, *The Global Media: The New Missionaries of Corporate Capitalism* (London: Continuum, 2001).

62. John Thompson, *Ideology and Modern Culture: Critical Social Theory in the Era of Mass Communication* (Stanford, CA: Stanford University Press, 1990).

63. Peter Barron, personal communication, April 21, 2009.

64. Michel Foucault, *Discipline and Punish: The Birth of the Prison* (New York: Pantheon Books, 1977).

65. See, for example, Oscar H. Gandy, *The Panoptic Sort: A Political Economy of Personal Information* (Boulder, CO: Westview Press, 1993); David Lyon, *Theorizing Surveillance: The Panopticon and Beyond* (Cullompton, U.K.: Willan Publishing, 2006); Satu Repo and Canadian Centre for Policy Alternatives, *Teacher Surveillance: The New Panopticon* (Ottawa: Canadian Centre for Policy Alternatives, 2005); Mark Andrejevic, *iSpy: Surveillance and Power in the Interactive Era* (Lawrence: University Press of Kansas, 2007). For a refreshing approach to studying surveillance without the Panopticon model, see Kevin Haggerty, "Tear Down the Walls: On Demolishing the Panopticon," in Lyon, *Theorizing Surveillance*.

66. B. Brower, review of Sonia Combe, *Une société sous surveillance: Les intellectuels et la Stasi*, in *Totalitarian Movements and Political Religions* 2 (2001): 88–92; Gary Bruce, "The Prelude to Nationwide Surveillance in East Germany: Stasi Operations and Threat Perceptions, 1945–1953," *Journal of Cold War Studies* 5, no. 2 (May 1, 2003): 3–31; Sonia Combe, *Une société sous surveillance: Les intellectuels et la Stasi* (Paris: Albin Michel, 1999).

67. Chris Anderson, *The Long Tail: Why the Future of Business Is Selling Less of More* (New York: Hyperion, 2006).

68. Eric Lichtblau, *Bush's Law: The Remaking of American Justice* (New York: Pantheon Books, 2008).