THE WATCHERS

Assaults on privacy in America

by JONATHAN SHAW

Illustrations by DAVIDE BONAZZI

Do people behave differently when they think they are being watched? When former National Security Agency contractor Edward Snowden revealed the mass surveillance of American citizens in June 2013, the question suddenly grew in importance. Can the behavior of an entire population, even in a modern democracy, be changed by awareness of surveillance? And what are the effects of other kinds of privacy invasions?

Jon Penney was nearing the end of a fellowship at Harvard Law School's Berkman Klein Center for Internet & Society in 2013, and he realized that Snowden's disclosures presented an opportunity to study their effect on Americans' online behavior. During research at Oxford the following year, Penney documented a sudden decline in Wikipedia searches for certain terrorism-related keywords: *Al Qaeda, Hezbollah, dirty bomb, chemical weapon,* and *jihad,* for example. More than a year later, when the study ended, such searches were *still* declining. "Given the lack of evidence of people being prosecuted or punished" for accessing such information, Penney wrote in the *Berkeley Technology Law Review* (which published his research last June), he judged it unlikely that "actual fear of prosecution can fully explain the chilling effects suggested by the findings of this study." The better explanation, he wrote, is self-censorship.

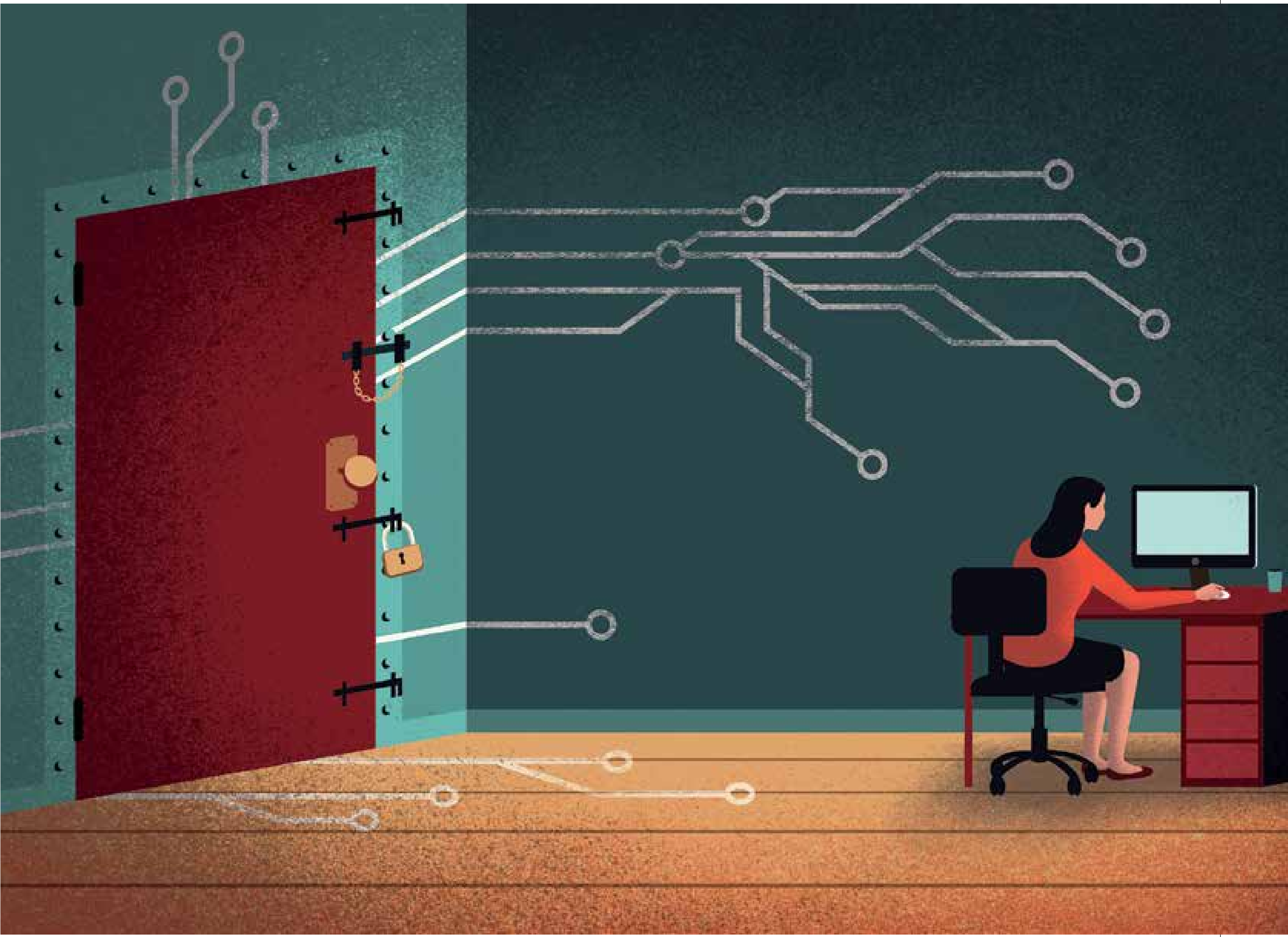
Penney's work is the sort of evidence for negative social effects that scholars (and courts of law) demand. If democratic self-governance relies on an informed citizenry, Penney wrote, then "surveillance-related chilling effects," by "deterring people from exercising their rights," including "…the freedom to read, think, and communicate privately," are "corrosive to political discourse."

"The fact that you *won't* do things, that you will self-censor, are the worst effects of pervasive surveillance," reiterates security expert Bruce Schneier, a fellow at the Berkman and in the cybersecurity program of the Kennedy School's Belfer Center for Government and International Affairs. "Governments, of course, know this. China bases its surveillance on this fact. It *wants* people to self-censor, because it knows it can't stop everybody. The idea is that if you don't know where the line is, and the penalty for crossing it is severe, you will stay far away from it. Basic human conditioning." The effectiveness of surveillance at preventing crime or terrorism can be debated, but "if your goal is to control a population," Schneier says, "mass surveillance is awesome."

That's a problem, he continues, because "privacy is necessary for human progress. A few years ago we approved gay marriage in all 50 states" (see "How Same-Sex Marriage Came to Be," March-April 2013, page 30). "That went from 'It'll never happen' to inevitable, with almost no intervening middle ground." But to get from immoral and illegal to both moral and legal, he explains, intervening steps are needed: "It's done by a few; it's a counterculture; it's mainstream in cities; young people don't care anymore; it's legal. And this is a long process that needs privacy to happen."

As a growing share of human interactions—social, political, and economic—are committed to the digital realm, privacy and security as values and as rights have risen in importance. When someone says, "My life is on my phone," it's meant almost literally: photos, passwords, texts, emails, music, address books, documents. It is not hard to imagine that the Declaration of Independence, redrafted for an information society, might well include "security and privacy," in addition to the familiar "life, liberty, and the pursuit of happiness," among its examples of "unalienable rights."

Although Snowden highlighted government surveillance, it may not be the worst problem. Corporations hold vast and growing troves of personal information that is often inadequately protected, its use largely unregulated. Since 2005, hackers have stolen hundreds of millions of credit-card numbers from major retailers such as Target, Home Depot, TJX, and eBay. In 2014, someone stole the keys to half a *billion* Yahoo accounts without being detected. And everyday threats to privacy are so commonplace that most people are numb to them. In exchange for free email, consumers allow companies such as Google to scan the content of their digital messages in order to deliver targeted ads. Users of social media, eager to keep in touch with a circle of friends, rarely read the standard agreement that governs the rights and use of what they post online. Smartphones know their owners' habits better than they themselves do: where and with whom they sleep, what time they wake up, whom they meet, and where they have been. People accept such tradeoffs in exchange for convenience. They don't really have a choice.



Bemis professor of international law and of computer science Jonathan Zittrain, faculty chair of the Berkman Klein Center, worries that the ubiquity of privacy threats has led to apathy. When a hacker released former Secretary of State Colin Powell's private assessments of the two leading presidential candidates prior to the recent election, "I was surprised at how little sympathy there was for his situation, how it was treated as any other document dump," Zittrain explains. "People have a hard time distinguishing, for instance, between government documents and *private* documents authored by people who were once government officials, [between] documents released under the Freedom of Information Act, and documents leaked by a whistleblower. It's all just seen as…'stuff is porous, and we can get it.'" As "the ability to hack is democratized," Zittrain worries that people have lost sight of the original value behind whistleblowing, which is to make powerful *institutions* publicly accountable. Now everyone is vulnerable. "Over time," he wrote recently, "continued leaks will lead people to keep their thoughts to themselves, or to furtively communicate unpopular views only in person." "That does not seem sustainable to me," he said in an interview, "and it doesn't seem healthy for a free society."

The perception that the Information Age has put privacy and security at risk is widespread. Necessarily, the search for solutions is equally broad-based. In Washington, D.C., Marc Rotenberg '82, president and director of the Electronic Privacy and Information Center (EPIC), seeks legal solutions to privacy problems (see page 60). At Harvard, research into privacy and security is focused at the Berkman Klein Center; at the Paulson School of Engineering and Applied Sciences' Center for Research on Computation and Society; at the Kennedy School's cybersecurity program; at the Institute for Quantitative Social Science's (IQSS) Data Privacy Lab; and also within the schools of medicine and public health (and at the affiliated hospitals), where researchers seek to protect patient data so that it can be shared appropriately, particularly in the case of rare conditions. Solutions to privacy and security problems thus involve computer scientists and legal scholars, as well as experts in healthcare, government, and business.

SECURITY: "We Have Lost Control"

Assuring the privacy of information means making it secure. "I actually can't give you privacy unless you have security," Bruce Schneier points out: that involves protecting data through technological or legal means. Door locks, tall fences, and burglar alarms work well in the physical world. The problem, he explains, is that "in security, technology scales badly." If a burglar gets past a lock to rob a single house in a community of 100,000 people, that may be a tolerable risk. But anyone who finds a flaw in all *digital* locks could break into every home. "What happens," Schneier asks, "when systems become connected such that our risks are connected?"

Ordinary individuals, he points out, can do very little to mitigate this kind of systemic risk. Advice like don't have an email address, don't use your credit card, is "moronic. You can't be a fully functioning human being in the twenty-first century [like that.] So in a lot of ways, we have lost control."

In the past 15 years, entire corporations, even nations, have found their data and systems vulnerable to attack. The intrusion at the U.S. Office of Personnel and Management, disclosed in April 2015, was reportedly the most significant breach of federal networks to date: hackers, thought to be state-sponsored, took personal data for four million employees and political appointees, leading to the recall of American intelligence agents posted abroad. The 2016 digital break-in at the Democratic National Committee's headquarters was like a modern iteration of Watergate, but initiated by a foreign power seeking to interfere in the presidential election.

The stakes can become very high indeed. "Someone is learning to take down the Internet," wrote Schneier in September. He described how an unidentified entity had been probing the defenses of companies that provide critical Internet infrastructure, slowly ramping up repeated, carefully metered attacks, as if seeking to quantify precise points of failure. Although his best-selling book, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, has led to his reputation as a consumer-privacy-rights advocate, Schneier is also chief technology officer for Resilient, an IBM company that handles online incident response. He brings that security background to a new fellowship at the Kennedy School's Cyber Security Project. The project focuses on policy research into the U.S. military's operations in cyberspace; it puts "people with a technical background together with people with policy experience," in order to help inform debates in Washington, says project director Michael Sulmeyer, former director for plans and operations for cyber policy at the Department of Defense. "One of the biggest debates going forward will be the roles and missions for the military's 6,000-person force for cyberspace operations."

That Cyber Command is charged with protecting the Defense Department's weapons systems, millions of computing devices, and more than 15,000 data networks (say, in support of network operations for a battalion in Afghanistan fighting the Taliban). It also provides offensive cyber capabilities to commanders around the world in the event that hostilities break out (analogous to the access they have to air and sea power capabilities). And it is responsible for defending the nation—including aviation, financial, and power-transmission systems—against a significant cyberattack.

The structure of the Internet itself makes that defensive mission difficult. Eviatar Matania, the head of Israel's National Cyber Bureau, discussed that challenge last September at the Kennedy School. He noted that unlike the agricultural and industrial revolutions, the cyber revolution has both restructured society and created a space, “THE INCREASED INTERCONNECTIVITY OF THE WORLD WE ARE LIVING IN [HAS LED TO] A LEVEL OF VULNERABILITY THAT WE DON’T TRULY UNDERSTAND.”

“a new artificial domain.” Israel’s bureau was founded five years ago as a way to allow that small country to be “much bigger and stronger than in a physical domain,” Matania continued. But defending cyberspace is extremely difficult because it lacks both borders and distance. There are no clear boundaries between countries, and no clear divisions between corporate and government networks: “Everyone is connected to everyone.”

That implies that the defense mission is expansive. Admiral Michael Rogers, director of the NSA and head of U.S. Cyber Command, said during an October visit to the Kennedy School that the unit increasingly finds itself “helping defend systems across the broader U.S. government” and even “being called upon to…help within the private sector. These are big growth areas for us.”

But as the mission grows, vulnerabilities are becoming *more* complex, not less. The Internet of Things—chip-equipped, network-connected household items such as living-room televisions that can respond to commands to change the channel—present huge security (not to mention privacy) concerns. “The increased interconnectivity of the world we are living in,” explained Rogers, has led to “a level of vulnerability that we don’t truly understand.” The automobile, for example, used to be “a mechanical system with a one-way radio”; today it’s “a series of interconnected software applications and capabilities,” involving a host of remote connections that the driver doesn’t understand or even know about. “That offers both amazing capability, insight, and knowledge—data that could make the car safer, make decisions faster, and eventually lead to remotely piloted autonomous vehicles.” But “that car now has a whole lot of vulnerabilities that it never had before.”

OPENNESS: “We Have to be Extremely Skeptical”

It may seem logical for a centralized military organization to provide national cybersecurity and defend against cyber war. But Yochai Benkler points out how 9/11 led to war and “unjustified claims for extending surveillance powers, or extending detention and kidnapping powers, let alone torture.” The Berkman professor for entrepreneurial legal studies argues that “We have to be extremely skeptical of claims made in the name of national security in general, not because the people making them are bad people, but because the people making them…operate in a world where the only downside to failing to extend their power is that one day somebody will look at them and say, ‘Where were you when the world came down?’

“We should take with many grains of salt the claims of national security experts who see cyber war as the next domain,” he continues, “and operate in an environment where they want to control everything as much as possible in order to minimize risks, but come to their conclusions from a framework that…is relatively insulated from potential alternative viewpoints.”

Accordingly, Benkler advocates systems that allow personal data to remain in the hands of consumers—minimizing the privacy risks posed by governments, corporations, and hackers because personal information is not concentrated in a single place. (The technical term is “distributed network ecosystems based on open-source software.”) “Relying on a small number of high-end companies to provide security creates a single point of failure for hundreds of millions,” he says, referring to the 2014 theft of Yahoo user accounts. “If all those…people had decentralized email storage at home, and sign-on credentials that were not valid for diverse critical sites, collecting [that information] would be much harder.”

“It’s a challenge to get people to adopt safe habits,” he admits, “but it’s not impossible. You have to change users’ culture, and you have to design secure systems that are under the control of end users, not single companies.” The iPhone, secured with a PIN or a fingerprint, is an example of such encrypted, secure-by-default systems. Such devices aren’t hard to build—but, he says pointedly, “It’s hard to do so [within] a business model that depends on spying on your customers so you can sell them to advertisers.”

Furthermore, says Benkler, systems built in part with “free software developed by communities that don’t have the imperatives either of profit-making companies, or of dealing with the tensions between rights and the state of emergency, get better as their vulnerabilities are constantly probed, exposed, and then corrected in a constant, evolutionary, back and forth.” Such robustness is obviously desirable.

But it may not be as practicable as he hopes. Although the idea that users can enjoy more privacy and better security in a distributed computing environment is becoming more tangible as smartphones’ computing power rivals that of desktops, executing it consistently poses significant challenges. Ben Adida, a software engineer and architect and former fellow of Harvard’s Center for Research on Computation and Society, acknowledges this is “the vision that many security advocates, myself included, pushed for for a very long time.”

But now he thinks “we are far less secure” adopting that technological approach. (For a computer scientist’s perspective, and a description of a project to protect research data involving human subjects, see the online extra, “The Privacy Tools Project.”) Adida developed Helios, one of the first encrypted yet verifiable online voting systems; he’s now head of engineering at Clever, a startup that manages private student data for schools. Providing security to a range of companies has led him to discover how easy it is for small companies to err when implementing and defending the security of their systems, whether in cryptography, access control, network-level security, or in the internal audit processes used to ensure data is compartmentalized. A large company like Google, on the other hand, “does a really good job of making sure that only I can log in,” he explains. “They’ve added two-factor authentication, they have all sorts of heuristics to check whether a person is logging in from a different location than usual. There’s all sorts of work that they do to make sure that only the right people are accessing the right data.”

Like Benkler, Adida agrees that centralized data is too easily accessed by law enforcement, but says that for now, “We need to rethink how to defend that data through a combination of legal and technical means.” Technically, that might mean discarding chats more than few months old, for example; and legally, resisting official requests for user data in court. He advocates “evolution in the law, too.” The Fourth Amendment guarantees the “right of the people

> “PRIVACY TURNS OUT TO BE AN EXTRAORDINARILY POWERFUL AND COMPREHENSIVE HUMAN-RIGHTS CLAIM, PARTICULARLY IN THE DIGITAL AGE, BECAUSE SO MUCH ABOUT US IS BASED ON OUR DATA.”

to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures…,” but historically, that has been interpreted to mean that obtaining data held by a *third* party doesn’t require a search warrant. That means personal documents stored in Google’s cloud, for example, are exposed. Adida says he nevertheless keeps “extremely private data hosted by a third party because that is the right operational thing to do. Everybody hosting their own stuff just doesn’t make any sense”—but he hopes that someday, if the government wants access to that information, it “would require a warrant, just as if they were knocking down someone’s door.”

CONFIDENTIALITY:
“Privacy Is about Accountability”

In the here and now, using encryption, firewalls, and passwords is one way to keep information secret. But secrecy is just “a very small slice” of what privacy is about, says Marc Rotenberg of EPIC. Through “creative advocacy, litigation, and public engagement,” the Washington, D.C.-based nonprofit aims to shape policy and advance the legal framework for safeguarding personal liberty. Rotenberg, an attorney and adjunct professor at Georgetown University Law Center, has won cases before the Supreme Court, filed numerous amicus briefs, testified before Congress, and given awards to leading privacy advocates across the political spectrum.

“Privacy is about accountability,” he says. “It’s about the fairness of decisionmaking. It’s about holding large government actors and private companies accountable for their decisionmaking. It turns out to be an extraordinarily powerful and comprehensive human-rights claim, particularly in the digital age, because so much about us is based on our data.”

Getting a loan or health insurance, or gaining admission to a certain school, are all data-driven determinations, Rotenberg points out. He asks how those data are being used. What personal information does an organization consider relevant? Are people pulled out of line at an airport because of their nationality, their religion, or because of a book purchased on Amazon? Given all the ways in which personal information drives decisions, Rotenberg says, secrecy “almost isn’t even relevant to the discussion. Because paradoxically, what *we keep secret* is almost certainly what we *don’t* need privacy law for. We need privacy law for everything else: for the things that we don’t have the physical ability to control. When you give sensitive test information to your doctor, for example, it’s no longer in your control. The credit card company has all your transactional records. What are you going to do? Nothing. *That’s* when we start to ask questions about what type of safeguards are in place to protect our personal information held by others.”

“I see privacy as closely tied to the strength of democratic governance,” he continues. Recalling the first time he read the NSA’s foreign intelligence surveillance court order demanding that Verizon turn over all customer telephone-call records (perhaps the most significant of Snowden’s revelations), Rotenberg says, “I looked at that order, ‘Provide all records, because all records are relevant,’ and actually thought it was satirical, a joke from *The Onion*, or an exercise attached to a privacy-law exam asking students to draft an unlawful court order.…And then I realized it was a real order—that the NSA thought it had the authority to collect all domestic telephone records on all U.S. telephone customers.”

EPIC brought a petition to the Supreme Court arguing that the Foreign Intelligence Surveillance Court had exceeded its legal authority, and a broad coalition of legal experts and former members of Congress joined the campaign. But the Court did not rule on the merits of the petition. “That was after the Solicitor General twice sought extensions,” Rotenberg explains, “which gave the foreign intelligence surveillance court enough time to issue an opinion justifying the program. We call that just-in-time lawmaking.” The EPIC petition nevertheless marked the beginning of a broad bipartisan coalition to pass legislation, the USA Freedom Act of 2015, ending the NSA’s bulk collection of such information.

Such battles almost never stay won, says Rotenberg. “The Europeans were very upset, obviously, about the U.S. surveillance activities that Snowden had documented, but then you had the terrible tragedy of *Charlie Hebdo*, and suddenly the French government created new surveillance authorities that go beyond what the U.S. does.”

“When governments make these decisions,” he reflects, “it is almost as if they’re saying, ‘We can’t afford as much democracy, we can’t afford as much openness, we can’t afford to trust our citizens as much, we need to engage in more surveillance, we need less judicial review and less accountability.’” But privacy, he says, is not a trade-off: “I’ve been in Washington long enough to know that when someone says, ‘We need to strike the right balance,’ it means they probably don’t know what they’re talking about. A sacrifice of privacy is also a sacrifice of democracy.”

In the mid 1990s, *The New York Times* quoted Rotenberg saying that the protection of privacy in the Information Age would be like the protection of the environment in the Industrial Age—“which is to say it’s so much a part of the nature of economic production today, you don’t solve it, you have to manage it.” Many people predicted the end of privacy. But Rotenberg believes people don’t understand the full consequences: “Among other things, you would lose your democratic state if everyone said, ‘Why do we care if the government knows everything about us? Who needs a private phone call? Who needs a building with walls? Why should data be accurate?’ Everything collapses. And we know what that world looks like: that’s what [Jeremy] Bentham described as the Panopticon”—designed so an observer can watch everything, but without being seen. “When you’re under constant surveillance,” says Rotenberg, “you’re in a prison.”

On the corporate front, EPIC brought the complaint that forced Snapchat, the photo-sharing service, to fulfill its promise to delete images. When Google tried to move all Gmail users onto Buzz, its social-media platform, EPIC complained to the Federal Trade Commission (FTC), and established a significant precedent for Internet privacy. When WhatsApp announced that it would share users' secure-message data with Facebook (which had recently acquired the company), EPIC intervened. Likewise, when Facebook started changing user privacy settings after consumers had set them, EPIC brought the matter to the FTC, which stopped the practice. Most recently, EPIC has been active in the discussion over how student data are collected and used.

EPIC may seem the proverbial finger in the dike, barely holding back the flood. But Rotenberg says he is "actually a bit of an optimist about all of this," citing the Supreme Court's "remarkable 9-0 opinion, written by Chief Justice Roberts, that says the search of a cell phone following an arrest requires a warrant"—a case in which EPIC's extensive brief was cited. Rotenberg calls the 2014 decision "a strong statement about privacy in the modern age. And the fact that it was a unanimous court, I think, was remarkable."

EPIC also studies diverse privacy laws to advance legal protections. A project begun in 2015 to identify states with the best privacy laws examines data security and breaches, drone surveillance, police body cameras, and student privacy, to name a few. EPIC considers Massachusetts's 2007 data-protection law one of the best in the country; California has crafted very good data-breach-notification regulations. Farther afield, Rotenberg admires the European Court of Justice's decision on the "right to be forgotten," which involved personal bankruptcy records that had been published in a newspaper 10 years earlier. The Spanish plaintiff asked both the newspaper and Google to remove the records. Spain's privacy agency decided not to touch the newspaper, but ordered Google to remove the record from search results—drawing "a very thoughtful line" between the protected free expression of news organizations and the commercial operations of data brokers, who commodify personal information.

DISCRIMINATION: "Algorithmic Accountability"

Rotenberg has recently begun advocating for laws that would require companies to disclose how algorithms use personal data—for hiring, credit determinations, or online advertising. As businesses demand more information from people, he thinks companies should reveal how they make decisions. Businesses regard their algorithms as intellectual property, but Rotenberg argues that their rights "extend as far as my personal data….And if that creates a problem for them, don't collect my data." The algorithms act invisibly and without accountability. Rotenberg says the solution is straightforward: "There should be algorithmic accountability. We should be able to open the code."

One computer scientist, famous for her work on privacy technology and re-identification of anonymous subjects in large data sets, approaches this problem as a technologist, seeking to expose the inner workings of algorithms in ways that make them susceptible to *existing* laws (see "Exposed," September-October 2009, page 38).

Google seemed to think professor of government and technology in residence Latanya Sweeney might have an arrest record. A simple search for the name of this African-American computer scientist, now faculty dean of Currier House, yielded ads implying that she had a criminal past. When former Reuters reporter Adam Tanner, now an Institute for Quantitative Social Science (IQSS) fellow, suggested that resulted from her "black-sounding name," Sweeney at first resisted his explanation. Then she discovered that a search for "Latanya" turned up images of black women, and a search for "Tanya" turned up images of whites. She decided to dig deeper.

Because she runs Harvard's Data Privacy Lab, based in IQSS, Sweeney has resources to find out what makes an algorithm tick. Using lists of first names given more often to black babies than to white ones, she Googled the names of real people from Internet addresses around the country, capturing 100,000 ad impressions. For some names, ads implied the existence of an arrest record as much as 80 percent of the time, even when there was none. "Blacks are a protected group. Employment is a protected setting," she notes. If an employer Googles an applicant's name and ads pop up implying that there is an arrest record, she says, that is enough to trigger a federal discrimination investigation.

Her work showed, Sweeney says, that these unforeseen consequences can be studied and the results used "to empower the government structures we already have for oversight." Rather than demanding new laws that focus on new technologies, she used science to expose the workings of technology, so

(please turn to page 82)

(continued from page 61)

existing law could be applied.

Armed with this tool for “algorithmic accountability,” Sweeney took a year’s sabbatical in 2014 to work as chief technology officer at the FTC. The commission had lacked pertinent technological expertise to investigate the issue; Sweeney’s presence persuaded the chairwoman to hire additional technologists.

While at the commission, Sweeney studied the practices of advertisers targeting the sites of sororities, fraternities, and other student groups, including Omega Psi Phi, a black fraternity celebrating its centennial. Ads routed to its website included options for graduate education and for travel—and one that implied the need for a criminal lawyer. Credit-card ads included only the lowest-ranked cards, whereas Sweeney found that the sites of similar fraternal student organizations turned up ads for American Express Blue. How, she wondered, did that decisionmaking occur in a supposedly neutral algorithm? “If, through their practices, technology companies are dominating the online experience” and shaping people’s experiences of the Internet, she says, “then it’s *those* practices that have to be addressed, or at least connected to…societal norms. Just because Google or Facebook implement business practices and technology together in a package in a certain way doesn’t mean that’s the *only* way. The technology…and the business practices didn’t have to be that way. And that has to be unpacked.”

COMMERCE: “Surveillance Capitalism”

Shoshanna zuboff, the Wilson professor of business administration emerita, would agree. She thinks about the information landscape in economic terms and says that there is even more at stake than privacy. Zuboff says that corporate use of personal data has set society on a path to a new form of capitalism that departs from earlier norms of market democracy.

She draws an analogy from the perfection of the assembly line: Ford engineers’ discovery a century ago, after years of trial and error, that they had created “a logic of high-volume, low-unit cost, which really had never existed before with all the pieces aligned.” Today, many corporations follow a similar trajectory by packaging personal data and behavioral information and selling it to advertisers: what she calls “surveillance capitalism.”

“Google was ground zero,” Zuboff begins. At first, information was used to benefit end users, to improve searches, just as Apple and Amazon use their customers’ data largely to customize those individuals’ online experiences. Google’s founders once said they weren’t interested in advertising. But Google “didn’t have a product to sell,” she explains, and as the 2001 dot.com bubble fell into crisis, the company was under pressure to transform investment into earnings. “They didn’t start by saying, ‘Well, we can make a lot of money assaulting privacy,’” she continues. Instead, “trial and error and experimentation and adapting their capabilities in new directions” led them to sell ads based on personal information about users. Like the tinkerers at Ford, Google engineers discovered “a way of using their capabilities in the context of search to do something utterly different from anything they had imagined when they started out.” Instead of using the personal data to benefit the *sources* of that information, they commodified it, using what they knew about people to match them with paying advertisers. As the advertising money flowed into Google, it became a “powerful feedback loop of almost instantaneous success in these new markets.”

“Those feedback loops become drivers themselves,” Zuboff explains. “This is how the logic of accumulation develops…and ultimately flourishes and becomes institutionalized. That it has costs, and that the costs fall on society, on individuals, on the values and principles of the liberal order for which human beings have struggled and sacrificed much over millennia—*that*,” she says pointedly, “is off the balance sheet.”

Privacy values in this context become externalities, like pollution or climate change, “for which surveillance capitalists are not accountable.” In fact, Zuboff believes, “Principles of individual self-determination are *impediments* to this economic juggernaut; they have to be vanquished. They are friction.” The resulting battles will be political. They will be fought in legislatures and in the courts, she says. (See EPIC’s cases, above.) Meanwhile, surveillance capitalists have learned to use all necessary means to defend their claims, she says: “through rhetoric, persuasion, threat, seduction, deceit, fraud, and outright theft. They will fight in whatever way they must for this economic machine to

"IN SURVEILLANCE CAPITALISM, RIGHTS ARE TAKEN FROM US WITHOUT OUR KNOWLEDGE, UNDERSTANDING, OR CONSENT, AND USED TO CREATE PRODUCTS DESIGNED TO PREDICT OUR BEHAVIOR."

keep growing." Consumer-citizens feel the assault, but for the surveillance capitalists, their creation is like "a living organism now, that has to grow."

"Privacy," according to Zuboff, "is having the right to decide how you want to live, what you want to share, and what you choose to expose to the risks of transparency. In surveillance capitalism, those rights are taken from us without our knowledge, understanding, or consent, and used to create products designed to predict our behavior." These products are then sold into new markets that she calls "behavioral futures markets." At each stage, "our lives are further exposed to others without our consent." In losing decision rights, we lose privacy, as well as autonomy and self-determination. Such rights don't vanish, she points out. "We lose them to someone else. Google is an example of a company that amasses 'decision rights' that once belonged to us. Decision rights are fundamentally political. So these are concentrations of political power, in institutions that we have not authorized. We didn't elect them, we didn't vote for them, we didn't sanction this transfer of rights and power."

Targeted ads—about which consumers already express concern—are the beginning of a much more ambitious program of modifying and influencing behavior toward profitable ends, Zuboff argues. "No one ever said mass production was only for automobiles, and surveillance capitalism isn't only for advertisers." There are many other companies and industries, she says, that want to participate in the new behavioral futures markets. Early examples include sectors such as insurance, retail, and health.

Behavioral futures markets develop in stages, she explains. Predictive analytics is a familiar use of data in which patterns are identified in order to predict whether somebody might be pregnant, or getting married, or has just lost a loved one. (The technique is already being used to place police officers in locations where crime is more likely to occur.) Zuboff notes that Google Maps, to take another example, recently introduced a feature that suggests a destination based on what it knows about users before they've even indicated where they're going. "Maybe it picked up from an email that you've recently moved and need to get tools for the workshop," Zuboff explains, "so it suggests a hardware store that you can go to. Would you think that hardware store is an innocent recipient of Google's largess?"

The stakes are getting higher. She points to the wildly popular game Pokémon Go, which rewards players with virtual experiences. "I can send you to the dry cleaner, I can send you to the car mechanic, I can send you to the restaurant—anywhere I want to with this reward system. All these entities pay to play in the new marketplace for behavior." Even before the game launched in Japan, McDonald's had paid to designate its 3,000 restaurants as destinations (called "gyms") within the game. The game's developer is Niantic, formerly a lab within Google run by John Hanke, who also led Google's geolocation services. (The core mapping technology was funded by the CIA's venture-capital arm.) Having mapped a virtual world onto the physical one with Google Maps and Google Earth, use of smartphone location services closes the loop, populating that cyber domain with people in the physical world.

At the moment, the project is "allowing the public to get exposed to this kind of interaction, and become habituated to it," says Zuboff. Pokémon players have fun, without realizing that it is also another form of social and economic control.

"I think it's very important to connect the dots," she explains, "and see that all of this makes sense when we frame it as a new form of capitalism that has particular requirements in order to be successful. Technology is never a thing in itself. It is always designed and deployed to reflect the aims and needs of a particular economic order. Suddenly, we can see that these ventures are part of a cohesive, internally consistent, and coherent economic logic. And when we can do that, then I think as a society we are far better positioned to increase and expand our advocacy and reform efforts, [to figure out how] to successfully tether information-based capitalism to pro-social and pro-democratic values and principles," rather than solely serving third-party economic interests. "The challenge of surveillance capitalism becomes part of the larger historical project of harnessing capitalism to society."

Surveillance capitalism, driven by the profit motive, "has been able to gather to itself concentrations of knowledge and power that exceed anything imaginable even a few years ago," she says. "One of its consequences is the deletion of privacy. But if we fight this only on the grounds of privacy, we're bound to meet with constant frustration and limited success. This is an economic logic that *must* delete privacy in order to be successful." This is why, despite the "brilliant and heroic scholarship" that has come out of Berkman, and despite the "brilliant and heroic advocacy that has come from many quarters in the United States, including Marc Rotenberg and his amazing team at EPIC,...this thing keeps growing."

History may suggest better ways to respond, she says. "We have experience in taming capitalism, and binding it to pro-social and pro-democratic principles. In the late nineteenth century, the Gilded Age, there was no protection for labor, and capital had complete freedom to do whatever it wanted to do with resources, with people, with communities, producing extreme economic and social inequality along the way." The twentieth century "was a long journey to correct that imbalance." The social challenge now, she says, is to insist on a new social contract, with its own twenty-first century legislative and regulatory innovations, that harnesses information capitalism to democratic values and norms. This begins, she believes, with deepening social understanding and awareness. "We have to create the political context in which privacy can be successfully defended, protected, and affirmed as a human right. Then we'd have a context in which the privacy battles can be won." ⛉

Jonathan Shaw '89 is managing editor of this magazine.