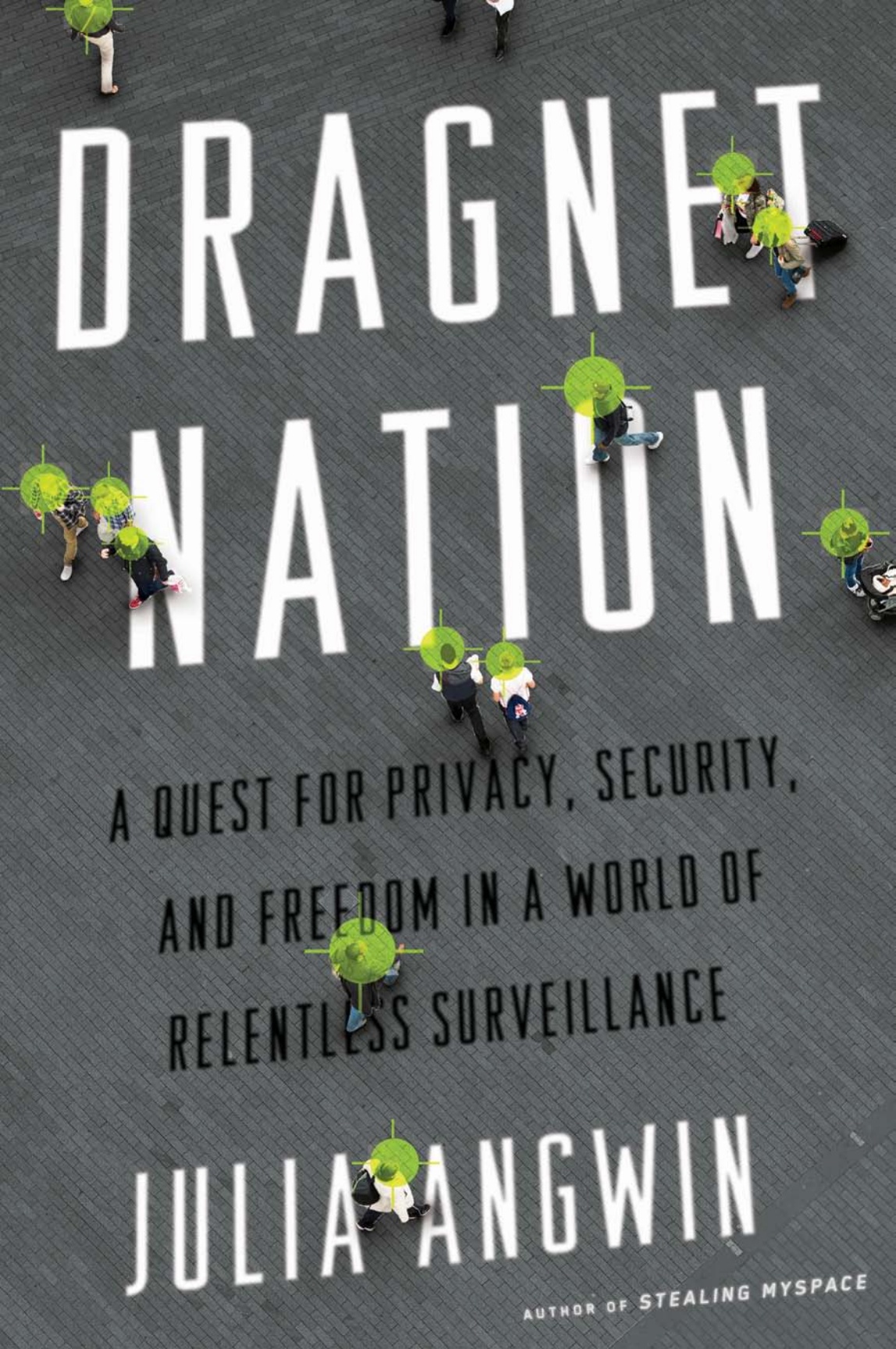
DRAGNET NATION
A QUEST FOR PRIVACY, SECURITY, AND FREEDOM IN A WORLD OF RELENTLESS SURVEILLANCE
JULIA ANGWIN
AUTHOR OF STEALING MYSPACE

Times Books
Henry Holt and Company, LLC
Publishers since 1866
175 Fifth Avenue
New York, New York 10010
www.henryholt.com

Distributed in Canada by Raincoast Book Distribution Limited

Library of Congress Cataloging-in-Publication Data

Angwin, Julia.
Dragnet nation : a quest for privacy, security, and freedom in a world of relentless surveillance / Julia Angwin. — First edition.
pages cm
Includes bibliographical references and index.
ISBN 978-0-8050-9807-5 (hardcover)—ISBN 978-0-8050-9808-2 (electronic)
1. Privacy, Right of. 2. Electronic surveillance. 3. National security—Moral and ethical aspects. 4. Information technology—Moral and ethical aspects. 5. Civil rights. I. Title.
JC596.A54 2014
323.44'8—dc23 2013042041

Henry Holt books are available for special promotions and premiums.
For details contact: Director, Special Markets.

First Edition 2014
Designed by Meryl Sussman Levavi

Printed in the United States of America
10 9 8 7 6 5 4 3 2 1

CONTENTS

1

HACKED

Who is watching you?

This was once a question asked only by kings, presidents, and public figures trying to dodge the paparazzi and criminals trying to evade the law. The rest of us had few occasions to worry about being tracked.

But today the anxious question—"who's watching?"—is relevant to everyone regardless of his or her fame or criminal persuasion. Any of us can be watched at almost any time, whether it is by a Google Street View car taking a picture of our house, or an advertiser following us as we browse the Web, or the National Security Agency logging our phone calls.

Dragnets that scoop up information indiscriminately about everyone in their path used to be rare; police had to set up roadblocks, or retailers had to install and monitor video cameras. But technology has enabled a new era of supercharged dragnets that can gather vast amounts of personal data with little human effort. These dragnets are extending into ever more private corners of the world.

Consider the relationship of Sharon Gill and Bilal Ahmed, close friends who met on a private online social network called PatientLikeMe.com.

Sharon and Bilal couldn't be more different. Sharon is a forty-two-year-old single mother who lives in a small town in southern Arkansas. She ekes out a living trolling for treasures at yard sales and selling them

at a flea market. Bilal Ahmed, thirty-six years old, is a single, Rutgers-educated man who lives in a penthouse in Sydney, Australia. He runs a chain of convenience stores.

Although they have never met in person, they became close friends on a password-protected online forum for patients struggling with mental health issues. Sharon was trying to wean herself from antidepressant medications. Bilal had just lost his mother and was suffering from anxiety and depression.

From their far corners of the world, they were able to cheer each other up in their darkest hours. Sharon turned to Bilal because she felt she couldn't confide in her closest relatives and neighbors. "I live in a small town," Sharon told me. "I don't want to be judged on this mental illness."

But in 2010, Sharon and Bilal were horrified to discover they were being watched on their private social network.

It started with a break-in. On May 7, 2010, PatientsLikeMe noticed unusual activity on the "mood" forum where Sharon and Bilal hung out. A new member of the site, using sophisticated software, was attempting to "scrape," or copy, every single message off PatientsLikeMe's private online "Mood" and "Multiple Sclerosis" forums.

PatientsLikeMe managed to block and identify the intruder: it was the Nielsen Company, the New York media-research firm. Nielsen monitors online "buzz" for its clients, including major drug makers. On May 18, PatientsLikeMe sent a cease-and-desist letter to Nielsen and notified its members of the break-in. (Nielsen later said it would no longer break into private forums. "It's something that we decided is not acceptable," said Dave Hudson, the head of the Nielsen unit involved.)

But there was a twist. PatientsLikeMe used the opportunity to inform members of the fine print they may not have noticed when they signed up. The website was also selling data about its members to pharmaceutical and other companies.

The news was a double betrayal for Sharon and Bilal. Not only had an intruder been monitoring them, but so was the very place that they considered to be a safe space. It was as if someone filmed an Alcoholics Anonymous meeting and AA was mad because that film competed with its own business of videotaping meetings and selling the tapes. "I felt totally violated," Bilal said.

Even worse, none of it was necessarily illegal. Nielsen was operating

in a gray area of the law even as it violated the terms of service at PatientsLikeMe, but those terms are not always legally enforceable. And it was entirely legal for PatientsLikeMe to disclose to its members in its fine print that it would sweep up all their information and sell it.

This is the tragic flaw of "privacy" in the digital age. Privacy is often defined as freedom from unauthorized intrusion. But many of the things that *feel* like privacy violations are "authorized" in some fine print somewhere.

And yet, in many ways, we have not yet fully consented to these authorized intrusions. Even if it is legal for companies to scoop up information about people's mental health, is it socially acceptable?

Eavesdropping on Sharon and Bilal's conversations might be socially acceptable if they were drug dealers under court-approved surveillance. But is sweeping up their conversations as part of a huge dragnet to monitor online "buzz" socially acceptable?

Dragnets that indiscriminately sweep up personal data fall squarely into the gray area between what is legal and what is socially acceptable.

We are living in a Dragnet Nation—a world of indiscriminate tracking where institutions are stockpiling data about individuals at an unprecedented pace. The rise of indiscriminate tracking is powered by the same forces that have brought us the technology we love so much—powerful computing on our desktops, laptops, tablets, and smartphones.

Before computers were commonplace, it was expensive and difficult to track individuals. Governments kept records only of occasions, such as birth, marriage, property ownership, and death. Companies kept records when a customer bought something and filled out a warranty card or joined a loyalty club. But technology has made it cheap and easy for institutions of all kinds to keep records about almost every moment of our lives.

Consider just a few facts that have enabled the transformation. Computer processing power has doubled roughly every two years since the 1970s, enabling computers that were once the size of entire rooms to fit into a pants pocket. And recently, the cost to store data has plummeted from $18.95 for one gigabyte in 2005 to $1.68 in 2012. It is expected to cost under a dollar in a few years.

The combination of massive computing power, smaller and smaller devices, and cheap storage has enabled a huge increase in indiscriminate tracking of personal data. The trackers are not all intruders, like Nielsen. The trackers also include many of the institutions that are supposed to be on our side, such as the government and the companies with which we do business.

Of course, the largest of the dragnets appear to be those operated by the U.S. government. In addition to its scooping up vast amounts of foreign communications, the National Security Agency is also scooping up Americans' phone calling records and Internet traffic, according to documents revealed in 2013 by the former NSA contractor Edward Snowden.

But the NSA is not alone (although it may be the most effective) in operating dragnets. Governments around the world—from Afghanistan to Zimbabwe—are snapping up surveillance technology, ranging from "massive intercept" equipment to tools that let them remotely hack into people's phones and computers. Even local and state governments in the United States are snapping up surveillance technology ranging from drones to automated license plate readers that allow them to keep tabs on citizens' movements in ways never before possible. Local police are increasingly tracking people using signals emitted by their cell phones.

Meanwhile, commercial dragnets are blossoming. AT&T and Verizon are selling information about the location of their cell phone customers, albeit without identifying them by name. Mall owners have started using technology to track shoppers based on the signals emitted by the cell phones in their pockets. Retailers such as Whole Foods have used digital signs that are actually facial recognition scanners. Some car dealerships are using a service from Dataium that lets them know which cars you have browsed online, if you have given them your e-mail address, before you arrive on the dealership lot.

Online, hundreds of advertisers and data brokers are watching as you browse the Web. Looking up "blood sugar" could tag you as a possible diabetic by companies that profile people based on their medical condition and then provide drug companies and insurers access to that information. Searching for a bra could trigger an instant bidding war among lingerie advertisers at one of the many online auction houses.

And new tracking technologies are just around the corner: companies are building facial recognition technology into phones and cameras,

technology to monitor your location is being embedded into vehicles, wireless "smart" meters that gauge the power usage of your home are being developed, and Google has developed Glass, tiny cameras embedded in eyeglasses that allow people to take photos and videos without lifting a finger.

Skeptics say: What's wrong with all of our data being collected by unseen watchers? Who is being harmed?

Admittedly, it can be difficult to demonstrate personal harm from a data breach. If Sharon or Bilal is denied a job or insurance, they may never know which piece of data caused the denial. People placed on the no-fly list are never informed about the data that contributed to the decision.

But, on a larger scale, the answer is simple: troves of personal data can and will be abused.

Consider one of the oldest and supposedly innocuous dragnets of all: the U.S. Census. The confidentiality of personal information collected by the census is protected by law, and yet census data have been repeatedly abused. During World War I, it was used to locate draft violators. During World War II, the Census Bureau provided the names and addresses of Japanese-American residents to the U.S. Secret Service. The information was used to round up Japanese residents and place them in internment camps. It was not until 2000 that the Census Bureau issued a formal apology for its behavior. And in 2002 and 2003, the Census Bureau provided statistical information about Arab-Americans to the Department of Homeland Security. After bad publicity, it revised its policies to require that top officials approve requests from other agencies for sensitive information such as race, ethnicity, religion, political affiliation, and sexual orientation.

The United States is not alone in abusing population statistics. Australia used population registration data to force the migration of aboriginal people at the turn of the twentieth century. In South Africa, the census was a key instrument of the state's "apartheid" system of racial segregation. During the Rwandan genocide of 1994, Tutsi victims were targeted with the help of ID cards that indicated their ethnicity. During the Holocaust, France, Poland, the Netherlands, Norway, and Germany used population data to locate Jews for extermination.

Personal data are often abused for political reasons. One of the most infamous cases was a program called COINTELPRO run by the Federal Bureau of Investigation in the late 1960s. The FBI's director, J. Edgar Hoover, set up the secret program to spy on "subversives" and then used the information to try to discredit and demoralize them. The FBI went as far as to send Martin Luther King Jr. a tape recording from surveillance of his hotel room that was meant to cause King to get separated from his wife—along with a note that King interpreted as a threat to release the recording unless King committed suicide.

Criminal hackers have also found that using personal data is the best way to breach an institution's defenses. Consider how Chinese hackers penetrated the sophisticated computer security pioneer RSA. The hackers trolled social media websites to obtain information about individual employees. They then sent those employees an e-mail titled "2011 Recruitment Plan." The e-mail looked legitimate enough that one employee retrieved it from the junk mail folder and opened it. That file installed spyware on the individual's machine, and from there the attackers gained remote control of multiple computers in the organization.

In short, they hacked people, not institutions.

Hacking people is not just for criminals. Marketers are following us around the Web in the hopes that they can obtain information that will let them "hack" us into buying their products. The NSA is scooping up all of our phone calls to establish patterns that it believes will let authorities "hack" a terrorist cell.

Here are some of the ways you may be already being hacked:

- You can always be found.
- You can be watched in your own home—or in the bathroom.
- You can no longer keep a secret.
- You can be impersonated.
- You can be trapped in a "hall of mirrors."
- You can be financially manipulated.
- You can be placed in a police lineup.

This is not a comprehensive list. Rather, it is a snapshot in time of real-life events that are happening right now. In the future, we will likely read this list and laugh at all the things I failed to envision.

YOU CAN ALWAYS BE FOUND.

Your name, address, and other identifying details—even the location of your cell phone at any given time—are all stored in various databases that you cannot view or control. Stalkers and rogue employees have consistently found ways to abuse these databases.

In 1999, a deranged man named Liam Youens paid an online data broker called Docusearch to find the social security number, employment information, and home address of a woman he was obsessed with, Amy Boyer. A few days later, Youens drove to Boyer's workplace and fatally shot her as she left work. He then shot and killed himself.

Boyer's family sued the data broker, but the New Hampshire Supreme Court held that while the data broker had a duty to "exercise reasonable care" when selling personal data, it was also true that because information such as a work address "is readily observable by members of the public, the address cannot be private."

Boyer's parents got very little: in 2004, they settled with Docusearch for $85,000, having grown weary of years of legal battles. Docusearch is still in business and its website still advertises services including "reverse phone number search," "license plate # search," "find SSN by name," and "hidden bank account search."

Since then, the price of buying people's addresses has fallen from the nearly $200 that Youens paid to as low as 95 cents for a full report on an individual. Cyber-stalking cases have become so common that they rarely make news.

Consider just one example. In 2010, a Sacramento sheriff's deputy, Chu Vue, was convicted of murder after his brothers shot to death Steve Lo, who was having an affair with Vue's wife. During the trial it came out that Vue had searched law enforcement databases for Lo's name, had asked a colleague to look up Lo's license plate, and had searched for Lo's address using an online phone lookup service. Vue was sentenced to life without parole.

Even the most innocent data—such as airline travel records—can be abused. In 2007, a Commerce Department employee, Benjamin Robinson, was indicted for unlawfully accessing, more than 163 times, the government database that contains international airline travel reservation records. After a breakup with a woman, he accessed her files, as well

as those of her young son and husband. He left a message on her answering machine stating that he was going to check the files "to see if there is anything you lied about." He suggested that he might be able to get her deported. In 2009, Robinson pleaded guilty to unlawfully obtaining information from a protected computer, and he was sentenced to three years' probation.

And the day is not far off when real-time tracking will become routine. The United States already embeds radio-frequency identification (RFID) chips that can transmit data over a short range of about ten feet in passports, and schools and employers are starting to embed the chips in ID cards. In 2013, a federal judge in Texas denied a student's challenge to her school's requirement that she wear an RFID-enabled ID card. Some employers have even flirted with the idea of implanting the chips under their employees' skin, which prompted California to outlaw the practice in 2008.

Cell phone tracking has already become routine for police departments. In 2011, my colleague at the *Wall Street Journal* Scott Thurm and I submitted open records requests to the twenty largest state and local police departments in the United States. Eight agencies produced at least summary statistics suggesting that state and local agencies track thousands of cell phones in real time each year. It is as routine as "looking for fingerprint evidence or DNA evidence," said Gregg Rossman, a prosecutor in Broward County, Florida.

Inevitably, phone companies have started selling cell phone location data to a wider audience than just police. In 2013, Verizon said it would sell a new product called Precision Market Insights that would let businesses track cell phone users in particular locations.

One of Verizon's first customers is the Phoenix Suns basketball team, which wants to know where its fans live. Scott Horowitz, a team vice president, said: "This is the information that everyone has wanted that hasn't been available until now."

YOU CAN BE WATCHED IN YOUR OWN HOME—OR IN THE BATHROOM.

In 2009, fifteen-year-old high school student Blake Robbins was confronted by an assistant principal who claimed she had evidence that he was engaging in "improper behavior in his home." It turned out that his

school—Harriton High School, in an affluent suburban Philadelphia school district—had installed spying software on the Apple MacBook laptops that it issued to the school's twenty-three hundred students. The school's technicians had activated software on some of the laptops that could snap photos using the webcam, as well as take screen shots of the students' computers. Blake's webcam captured him holding pill-shaped objects. Blake and his family said they were Mike and Ike candies. The assistant principal believed they were drugs.

Blake's family sued the district for violating their son's privacy. The school said the software had been installed to allow technicians to locate the computers in case of theft. However, the school did not notify students of the software's existence, nor did it set up guidelines for when the technical staff could operate the cameras.

An internal investigation revealed that the cameras had been activated on more than forty laptops and captured more than sixty-five thousand images. Some students were photographed thousands of times, including when they were partially undressed and sleeping. A former student, Joshua Levin, said he was "shocked, humiliated, and severely emotionally distressed" when he viewed some of the eight thousand photos and screen shots captured by the camera on his laptop. Levin, Robbins, and one other student sued the school and won monetary settlements. The school board banned the school's use of cameras to surveil students.

We're used to the idea that surveillance cameras are everywhere. It is estimated that there are more than four thousand surveillance cameras installed in lower Manhattan. London is famous for its more than five hundred thousand security cameras.

But as the cameras are getting smaller, they are traveling into our homes and intimate spaces, upending our definitions of public and private. Drones equipped with cameras have become cheap enough that they are becoming a nuisance. In May 2013, a Seattle woman complained on a local blog. A stranger had "set an aerial drone into flight over my yard and beside my house. . . . I initially mistook its noisy buzzing for a weed-whacker on this warm spring day." Her husband approached the man flying the drone, who declared that it was legal for him to fly it and that the drone was equipped with cameras. "We are extremely concerned, as he could very easily be a criminal who plans to break into our house or a peeping-tom," she said.

With all this cool technology, the bad guys are of course setting up their own camera dragnets. In 2013, the journalist Nate Anderson described a robust hacker community that trades tips and techniques for installing spyware on women's webcams. "They operate quite openly online, sharing the best techniques," he wrote. "Calling most of these guys 'hackers' does a real disservice to hackers everywhere; only minimal technical skill is now required."

In 2011, a Santa Ana man named Luis Mijangos was convicted of computer hacking and wiretapping after he was found to have installed malicious software that allowed him to control the webcams of more than one hundred computers. In one case, he gained control of a teenage girl's webcam and obtained naked photographs of her. He used the images to extort further nude images from his victims. During the sentencing, the judge said, "This was nothing short of a sustained effort to terrorize victims." Mijangos was sentenced to six years in prison.

And widespread camera dragnets are right around the corner. The arrival of wearable computers equipped with cameras, such as Google Glass, means that everything is fair game for filming. The *New York Times* columnist Nick Bilton was shocked when he attended a Google conference and saw attendees wearing their Google Glass cameras while using the urinals.

But Google Glass enthusiasts say that wearing cameras on their heads changes their life. "I will never live a day of my life from now on without it (or a competitor)," wrote the blogger Robert Scoble after trying out the glasses for two weeks. "It freaks some people out," he conceded, but he said, "It's new, that will go away once they are in the market."

YOU CAN NO LONGER KEEP A SECRET.

Bobbi Duncan, a twenty-two-year-old lesbian student at the University of Texas, Austin, tried to keep her sexual orientation secret from her family. But Facebook inadvertently outed her when the president of the Queer Chorus on campus added her to the choir's Facebook discussion group. Bobbi didn't know that a friend could add her to a group without her approval and that Facebook would then send a note to her entire list of friends—including her father—announcing that she'd joined.

Two days after receiving the notification that Bobbi had joined the

Queer Chorus, her father wrote on his Facebook page: "To all you queers. Go back to your holes and wait for GOD. Hell awaits you pervert. Good luck singing there."

When informed about the case, Facebook spokesman Andrew Noyes said that the "unfortunate experience reminds us that we must continue our work to empower and educate users about our robust privacy controls." His position seemed to put the blame on the victim for incorrectly flipping Facebook's dials and levers. But there was no dial or lever on Facebook that Bobbi could have set to prevent her being joined to the group without her permission.

"I blame Facebook," Bobbi said. "It shouldn't be somebody else's choice what people see of me."

As more personal data are swept up into various databases, it has become harder for any secrets to be kept—even by professional secret keepers. The most notable example is CIA director David Petraeus, who resigned after an unrelated FBI investigation uncovered e-mails that indicated he was conducting an extramarital affair. In 2012, former CIA analyst John Kiriakou was indicted for passing classified information to journalists, based in part on e-mail evidence. He pleaded guilty and was sentenced to thirty months in prison.

Even minor secrets are difficult to keep. People who download porn movies on their computers have been targeted by so-called copyright trolls who file mass lawsuits that allow them to obtain information about the identities of people who have downloaded copyrighted porn movies from file-sharing networks, with the intent of embarrassing the defendants into paying a quick settlement.

In July 2012, the U.S. Court of Appeals for the Fifth Circuit sanctioned one such plaintiff, an attorney for an adult movie producer, who had sued 670 downloaders based on their computer addresses and sought to obtain their identities without court approval. The court described the attorney's "violations as an attempt to repeat his strategy of suing anonymous Internet users for allegedly downloading pornography illegally, using the powers of the court to find their identity, then shaming or intimidating them into settling for thousands of dollars."

In May 2013, a California judge went even further, declaring that the copyright trolls had used a "nexus of antiquated copyright laws, paralyzing social stigma and unaffordable defense costs" to "plunder the citizenry."

YOU CAN BE IMPERSONATED.

Jaleesa Suell was taken away from her mother and placed in foster care when she was eight years old. She was placed in seven different foster homes before leaving the foster care system. When she turned twenty-one and was nearing graduation from George Washington University, she applied for a credit card. That's when she found out that a family member had stolen her identity, opened up a credit card in her name, and defaulted on the payments.

Without access to credit, Jaleesa couldn't get a car and worried she wouldn't be able to get an apartment after graduation. "I often find myself worried about if I was going to have a place to live the next day or have food, and I've worked so hard to ensure that that won't happen after, you know, I emancipated," she told participants in a workshop on identity theft in 2011. "But now I find myself in that exact situation, just for the simple fact that, like, I don't have a line of credit."

Sadly, foster children like Jaleesa are among the most common victims of the crime known as identity theft. I prefer to call the crime "impersonation," because no one can really steal your identity. Jaleesa is still herself. Someone has simply impersonated her for financial gain.

In response to the rising problem of impersonation among foster children, President Barack Obama signed a law in 2011 that contained a provision requiring the credit-reporting companies to provide foster children with a free credit report annually after they turn sixteen years old for as long as they remain in the system.

But the underlying problem of impersonation continues to rise. Complaints of identity theft increased by nearly one-third in 2012—up to 369 million from 279 million a year earlier—after remaining fairly steady for the previous five years, according to statistics compiled by the Federal Trade Commission.

Credit card fraud used to be the most common complaint, according to Steve Toporoff, the FTC attorney who coordinates the agency's identity protection program. These days, he said, tax fraud is the top complaint. "We also see new forms of fraud, such as medical fraud, in which people use identity information to obtain health treatment," he said. It's harder for people to catch tax and medical fraud, as they do not have access to their files as easily as they do with credit reports.

In 2013, two Florida women were convicted of defrauding the government in a scheme in which they submitted nearly two thousand fraudulent tax returns to the IRS seeking $11 million in refunds. The Department of the Treasury paid out nearly $3.5 million. One of the women, Alci Bonannee, filed many of the fraudulent returns using personal information purchased from a hospital nurse. The hospital, Baptist Health South Florida, stated that 834 patient records had been accessed. An IRS agent, Tony Gonzalez, told a local TV station that "the bad guys that are able to get these social security numbers are buying them from employees that work at these hospitals and these medical centers which are sold up to $150 each."

Identity information is not only being stolen, it is also being lost all the time, for reasons ranging from carelessness to hacking. Public reports of data breaches have been steadily on the rise since 2009, and jumped by a dramatic 43 percent in 2012, according to the Open Security Foundation's DataLossDB website.

And companies are rarely penalized for losing customer data. A test case is playing out as a result of the repeated hacks of the Wyndham hotel chain. In 2008, hackers broke into the computer network of the Wyndham hotel in Phoenix. Through that network, the hackers gained access to the credit card accounts of more than five hundred thousand customers at all forty-one Wyndham hotels and transferred the information to Russia. The hackers allegedly racked up more than $10.6 million in fraudulent charges.

But even after that breach, Wyndham failed to secure its computer network. The following year, it was hacked twice, losing another fifty thousand and sixty-nine thousand customer credit cards, respectively. In 2012, the Federal Trade Commission sued Wyndham, alleging that its failure to secure its network was deceptive and unfair to customers.

Wyndham fought back. It claimed the FTC was unfairly penalizing the company for being the victim of a crime. It called the FTC's case "the Internet equivalent of punishing the local furniture store because it was robbed and its files raided." The FTC responded in a legal filing that "a more accurate analogy would be that Wyndham was a local furniture store that left copies of its customers' credit and debit card information lying on the counter, failed to lock the doors of the store at night, and was shocked to find in the morning that someone had stolen the information."

YOU CAN BE TRAPPED IN A "HALL OF MIRRORS."

Companies that monitor people's Web-surfing behavior say their actions are innocuous: they only want to show ads for shoes to people who have recently looked at shoes, or to show political news to people who prefer political news. I call this type of mass customization a "hall of mirrors."

Sometimes the hall of mirrors is helpful. I don't particularly mind seeing an ad that reminds me to purchase a product I was just looking at. But the hall of mirrors can also veer into disturbing territory.

Consider this: searching for a traditionally black-sounding name such as "Trevon Jones" is 25 percent more likely to generate ads suggesting an arrest record—such as "Trevon Jones Arrested?"—than a search for a traditionally white-sounding name like "Kristen Sparrow," according to a January 2013 study by Harvard professor Latanya Sweeney. Sweeney found this advertising disparity even for names in which people with the white-sounding name did have a criminal record and people with the black-sounding name did not have a criminal record.

Data about people's Web-surfing behavior is also increasingly used to provide so-called customized content. For instance, Google uses information from past searches and browsing habits to provide different search results to different people—even when they conduct identical search requests. Sometimes those extrapolations can be useful, such as when Google suggests a restaurant near where you live instead of across the country. But sometimes they are intrusive.

In the months leading up to the November 2012 presidential election, Google took its guesses into the political realm in a controversial way. Searchers who looked up Barack Obama saw news about the president threaded into their future searches on other topics. Searchers who looked up Mitt Romney did not see news about the Republican presidential candidate included in subsequent searches.

Google said that the disparity was simply the result of the mathematical formula it was using to predict users' queries. Google's technologists viewed their effort as helping us figure out the answer to our needs before we know we have those needs. But it is worth noting that if a newspaper did the same thing—inserted Obama news into articles about toothpaste for certain readers—it would be roundly called out as biased and intrusive. Similarly, a newspaper would be called out if it placed only gay ads in the

papers of subscribers it deemed to be gay, or diabetes treatment ads in the papers of subscribers it guessed had the disease.

Does technology immunize Google from something that would not otherwise be socially acceptable? Or is Martin Abrams, a leading privacy expert, right to call this type of behavior restrictive "boxing," where "my vision of what is possible is limited by the box" in which I am placed?

YOU CAN BE FINANCIALLY MANIPULATED.

As companies gather more digital data about potential customers, they have the ability to use that information to charge different prices to different users or steer different users to different offers.

Ryan Calo, a law professor at the University of Washington, calls this the "mass production of bias," in which companies use personal data to exploit people's vulnerability. For example, companies can chip away at consumers' willpower until they finally give in to making a purchase. Or a computer algorithm can set prices for each individual at exactly the price that is the most he or she is willing to pay for a given product or service.

The credit card companies have started using some of these techniques. In 2010, my colleagues at the *Wall Street Journal* and I discovered that Capital One was showing different credit cards (with different rates) to different website visitors, based on its guesses about their income and geographic location. The result was that when Thomas Burney, a Colorado building contractor, visited Capital One's website, he was greeted with offers for a card for people with excellent credit, the "Capital One Platinum Prestige." By comparison, when Carrie Isaac, a young mother from Colorado Springs, visited the website, she was shown a card described as being for people with "average" credit.

The reason was buried in the computer code. Contained in the 3,748 lines of code that passed between Thomas's computer and Capital One's website were the credit card company's guesses about his income level ("upper-mid"), education ("college graduate"), and his town ("avon"). Capital One had assessed Carrie as having only "midscale" income with "some college" education. A Capital One spokeswoman told us, "Like every marketer, online and off-line, we're making an educated guess about what we think consumers will like and they are free to choose another product of their liking."

By 2012, when my team again tested for market manipulation, the techniques had become more widespread and increasingly sophisticated. We found that credit card companies were still offering different cards to different users. Discover was showing a prominent offer for the "it" card to computers connecting from cities including Denver, Kansas City, and Dallas, but not to people connecting from Scranton, Pennsylvania; Kingsport, Tennessee; and Los Angeles.

But we also found that websites were varying prices based on their guesses about where users were located. In our tests, Lowe's was selling a refrigerator for $449 to users in Chicago, Los Angeles, and Ashburn, Virginia. But it cost $499 in seven other test cities. Similarly, a 250-foot spool of electrical wiring was displayed at six different prices on Home Depot's website depending on the user's location: $70.80 in Ashtabula, Ohio; $72.45 in Erie, Pennsylvania; $75.98 in Olean, New York; and $77.87 in Monticello, New York. Both Lowe's and Home Depot said the variations were an attempt to match online prices to the closest store.

We found the most comprehensive price differences on the website of the office supply giant Staples, which appears to use data about visitors to guess where they live. It then displays different prices to different users based on its estimate of their geographic location. The end result: when Trude Frizzell logged on to Staples.com from her work computer in Bergheim, Texas, she saw a Swingline stapler listed for sale for $14.29. Just a few miles away, in Bourne, Kim Wamble saw the same stapler listed on the same website for $15.79. The difference was not due to shipping costs, which are calculated after purchasing the item. Rather, the prices seem to reflect how far Staples believes the user lives from a competitor's store. Staples confirmed that it varies prices by a number of factors but declined to be specific.

It's not illegal to charge different prices to different users, as long it is not based on race or other sensitive information that could constitute redlining. But offering price variations to different users can result in unfair results that are unintended. Our tests of the Staples website showed that areas with higher average income were more likely to receive discounted prices than lower-income areas. "I think it's very discriminatory," said Kim.

The worst types of financial manipulation exploit the poor, the old, or the uneducated. Consider the so-called sucker lists that data brokers com-

pile of people who are old, in financial distress, or vulnerable in some other way to certain types of marketing pitches. Sucker lists are often sold to unscrupulous marketers who pitch fraudulent products.

In October 2012, the Federal Trade Commission fined one of the nation's largest data brokers, Equifax, and its customers a total of $1.6 million for abusing personal data by selling lists of people who were late in paying their most recent mortgage bills to fraudulent marketers. The lists were marketed with names like "Save Me From Foreclosure" and "Debt Regret." One of the buyers was a particularly seedy Southern California boiler room operation that allegedly bilked more than $2.3 million from at least fifteen hundred home owners who paid fees ranging from $1,000 to $5,000 for loan modifications that almost never materialized. Many of those home owners eventually lost their homes.

When I asked an official at the Direct Marketing Association whether there are any lists its members won't sell, such as "seniors with Alzheimer's who like sweepstakes," she sent me the organization's ethical guidelines, which prohibit the sale of lists that are "disparaging." Otherwise, it's fair game, apparently.

YOU CAN BE PLACED IN A POLICE LINEUP.

On April 5, 2011, John Gass picked up his mail in Needham, Massachusetts, and was surprised to find a letter stating that his driver's license had been revoked. "I was just blindsided," John said.

John is a municipal worker—he repairs boilers for the town of Needham. Without a driver's license, he could not do his job. He called the Massachusetts Registry of Motor Vehicles and was instructed to appear at a hearing and bring documentation of his identity. They wouldn't tell him why his license was revoked.

When John showed up for his hearing, he learned that the RMV had begun using facial recognition software to search for identity fraud. The software compared license photos to identify people who might have applied for multiple licenses under different aliases. The software had flagged him and another man, Edward Perry of Rehoboth, Massachusetts, as having similar photos and had required them to prove their identities.

John was a victim of what I call the "police lineup"—dragnets that allow

the police to treat everyone as a suspect. This overturns our traditional view that our legal system treats us as "innocent until proven guilty."

The most obvious example of this is airport body scanners. The scanners conduct the most intrusive of searches—allowing the viewer to peer beneath a person's clothes—without any suspicion that the person being scanned is a criminal. In fact, the burden is on the individual being scanned to "prove" his or her innocence, by passing through the scanner without displaying any suspicious items. These dragnets can be Kafkaesque. Consider the no-fly list. People placed on the list are not told how they got on the list, nor can they argue against the decision.

John Gass luckily was given a chance to plead his case. But it was an absurd case. He was presented with a photo of himself from thirteen years ago.

"It doesn't look like you," the officer said.

"Of course it doesn't," John said. "It's thirteen years later. I was a hundred pounds lighter."

John presented his passport and his birth certificate, and his license was reinstated. But the officers wouldn't give him any paperwork to prove that it was reinstated. He wanted a piece of paper to show his boss that he was okay to drive again. "It was kind of like a bad dream," John said.

Angry at his treatment and his lost income, John filed a lawsuit against the RMV, claiming that he had been denied his constitutionally protected right to due process. The RMV argued that he had been given a window of opportunity to dispute the revocation because the letter had been mailed on March 24 and the license wasn't revoked until April 1. John didn't pick up his mail until April 5.

The Suffolk County Superior Court granted the RMV's motion to dismiss. Gass appealed, but the appellate court also ruled against him. "Although Gass's pique at having to defend his identity is understandable, it does not follow that his case raises larger legal questions that appellate courts must resolve at this time," the court stated.

John felt betrayed by the whole process. He now is very careful around state police because he worries that he won't be treated fairly. "There are no checks and balances," he said. "It is only natural humans are going to make mistakes. But there is absolutely no oversight.

"I do think we are trading our liberties for security," he said.

These stories illustrate a simple truth: information is power. Anyone who holds a vast amount of information about us has power over us.

At first, the information age promised to empower individuals with access to previously hidden information. We could comparison shop across the world for the best price, for the best bit of knowledge, for people who shared our views.

But now the balance of power is shifting and large institutions—both governments and corporations—are gaining the upper hand in the information wars, by tracking vast quantities of information about mundane aspects of our lives.

Now we are learning that people who hold our data can subject us to embarrassment, or drain our pocketbooks, or accuse us of criminal behavior. This knowledge could, in turn, create a culture of fear.

Consider Sharon and Bilal. Once they learned they were being monitored on PatientsLikeMe, Sharon and Bilal retreated from the Internet.

Bilal deleted his posts from the forum. He took down the drug dosage history that he had uploaded onto the site and stored it in an Excel file on his computer. Sharon stopped using the Internet altogether and doesn't allow her son to use it without supervision.

They started talking on the phone, but they missed the online connections they had forged on PatientsLikeMe. "I haven't found a replacement," Sharon said. Bilal agreed: "The people on PLM really know how it feels."

But neither of them could tolerate the fear of surveillance. Sharon said she just couldn't live with the uncertainty of "not knowing if every keystroke I'm making is going to some other company," she said. Bilal added, "I just feel that the trust was broken."

Sharon and Bilal's experience is a reminder that for all its technological pyrotechnics, the glory of the digital age has always been profoundly human. Technology allows us to find people who share our inner thoughts, to realize we're not alone. But technology also allows others to spy on us, causing us to pull back from digital intimacy.

When people ask me why I care about privacy, I always return to the simple thought that I want there to be safe, private spaces in the world for Sharon and Bilal, for myself, for my children, for everybody. I want there to be room in the digital world for letters sealed with hot wax. Must we

always be writing postcards that can—and will—be read by anyone along the way?

Do we want to live in a world where we are always at risk of being hacked? A world where we can always be found, we can't keep secrets, we can be watched even in our own homes, we can be impersonated, we can be trapped in a hall of mirrors, we can be financially manipulated and put in a police lineup? This book is my attempt to answer that question in two parts.

In the opening chapters, I explore why indiscriminate surveillance matters. To do that, I examine the legal and technical origins of our Dragnet Nation, the uses and abuses of surveillance, and its impact on individuals and society.

In the chapters that follow, I examine whether there is any hope of building an alternative world, where we can enjoy the fruits of technology without fear of being hacked. I test various strategies for evading dragnets, ranging from using a burner phone to establishing fake identities.

I hope that my exploration will help the conversation about privacy evolve beyond the simple anxiety of "Who's watching me?" into a more nuanced discussion of "Why does it matter?" and, ultimately, to a productive conversation about what we can do about it.