

CHAPTER 6

Big Data, Big Risk

**Our technological powers increase,
but the side effects and potential hazards also escalate.**

ALVIN TOFFLER

On the evening of November 26, 2008, a sixty-nine-year-old man checked into room 632 at the luxurious Taj Mahal Palace hotel in Mumbai, India. The guest, K. R. Ramamoorthy, was visiting from Bangalore on a routine business trip. Little did he know that his life was about to change forever.

At about 11:00 p.m., Ramamoorthy heard a brief commotion outside his door, then suddenly a knock. "Room service," a voice said. Ramamoorthy knew he had not ordered any food and sensed something was gravely wrong. He attempted a retreat to the bathroom, accidentally bumping into the door. The noise gave away his presence inside the hotel room. The response was swift: a hail of bullets came flying through the door, obliterating the lock separating the businessman from the world outside.

Two heavily armed men forced their way into Ramamoorthy's room, and in the blink of an eye he was beaten, stripped naked, and tied up in what would become the most terrifying night of his life. The men were from a Pakistani-based al-Qaeda-affiliated terrorist organization known as Lashkar-e-Taiba (LeT), and Ramamoorthy

had unfortunately found himself at the center of the deadly 2008 terrorist siege on the city of Mumbai.

"Who are you, and what are you doing here?" his LeT captors demanded of him. "I'm just an innocent schoolteacher," Ramamoorthy replied. Of course, the terrorists knew that no Indian schoolteacher could afford to stay in a suite at the city's most opulent hotel. The terrorists located their hostage's identification card on his bedside table and now had his true name, which they called in to their terrorist commanders on the satellite phone they had brought with them.

The LeT ops center receiving the call resembled any modern military command-and-control facility. From across the border in Pakistan, terrorist cell leaders tracked the progress of their attack on the people of Mumbai. They had carefully selected their targets, including two luxury hotels, a busy railway station, a Jewish community center, a popular tourist café, and even a women and children's hospital. On the ground in Mumbai, terrorist operatives ruthlessly threw hand grenades at innocent people as they sat eating in cafés and gunned down unarmed civilians waiting to catch trains on their way home from work.

As the attacks unfolded, LeT commanders in Pakistan used their war room to carefully monitor the BBC, Al Jazeera, CNN, and local Indian TV stations to learn as much as possible about the progress of their operatives and the response of the Indian government. Regrettably, the terrorists did not limit their information-gathering operations to broadcast media; they also mined the Internet and social media in real time, to deadly effect.

When the terrorists holding Ramamoorthy phoned in his name to their Pakistani base, the ops center deftly conducted an Internet search on their hostage. Moments later, they had his photograph. Then his place of work. They learned Ramamoorthy was not an innocent schoolteacher as he claimed when pleading for his life but rather the chairman of one of India's largest banks, ING Vysya. Based on the image they had found online, the terrorist commanders asked their operatives at the Taj Mahal Palace to compare the man before them with the photograph of the bank chairman located online:

Your hostage, is he heavyset?

Yes.

Is he bald in front?

Yes.

Does he wear glasses?

Yes.

"What shall we do with him?" asked Ramamoorthy's captors. Moments later, the terrorist war room gave its reply: Kill him.

In an instant, a simple Internet search was all the terrorists needed to decide the elderly man's fate. Though we may worry about advertisers and data brokers abusing our privacy settings on Facebook, the fact of the matter is that our openness can be used against us in ways worse than we had ever imagined. When we leak data, it's not just captured by corporations or governments. Criminals and terrorists have access to our social data as well, and they are leveraging it with killer precision. In today's world, a search engine can literally determine who shall live and who shall die.

The men who carried out that attack on Mumbai were armed with AK-47s and RDX explosives. Guns and bombs are nothing new in terrorist operations, but these LeT operatives represented a deeply disturbing new breed of terrorist. They had seen the future and leveraged modern information technologies every step of the way throughout their assault to locate additional victims and slaughter them.

When the attackers set out to sea from Pakistan under cover of darkness, they wore night-vision goggles and navigated to Mumbai using GPS handsets. They carried BlackBerrys containing PDF files of the hotel floor plans and used Google Earth to explore 3-D models of target venues to determine optimal entry and exit points. During the melee, LeT assassins used satellite phones, GSM handsets, and Skype to coordinate with their Pakistan-based command center, which monitored broadcast news, the Internet, and social media to provide real-time tactical direction to its ground assault team.

When a bystander tweeted a photograph of police commandos rappelling from a helicopter onto the roof of the besieged Jew-

ish community building, the terrorist ops center intercepted the photograph, alerted its attackers, and directed them to a stairwell leading to the roof. The police, who had hoped to surprise the terrorists, instead found themselves ambushed inside the stairwell the moment they opened the door. When the BBC mentioned on air that witnesses had reported the terrorists were hiding in room 360 or 361, their war room phoned them immediately and told them to reposition themselves to avoid capture.

At every point during the siege, the LeT attackers exploited readily available technology to gain situational awareness and maintain tactical advantage over police and the government. They monitored the Internet and social media, gathered all available open-source data, and even mounted a sophisticated online counterintelligence operation to protect their operatives. Throughout their assault on Mumbai, the terrorists were so dependent on technology that numerous witnesses reported seeing LeT operatives shooting hostages with the guns in their right hands while simultaneously checking BlackBerry messages with their left.

Not only was technology crucial to the operational success of the siege, but as we learned in chapter 2, criminal abuse of technology also funded the attack. It was a Filipino hacking cell working on behalf of the al-Qaeda affiliate Jamaah Islamiyah that committed extensive cyber crime and online fraud to bankroll the LeT operation in India. The hackers funneled their millions in ill-gotten cyber gains back to their handlers in Saudi Arabia, who in turn laundered the funds and forwarded them to the Lashkar-e-Taiba team responsible for the brutal onslaught against the people of Mumbai.

In the end, it took police sixty-eight hours to end the siege on the city of Mumbai. Counterassault teams eventually killed nine of the terrorists and arrested the tenth. Shockingly, one of the innocents to survive the attack was K. R. Ramamoorthy. At the very moment the LeT command center had given the order to kill him, there was an explosion in the Taj Mahal Palace, which his attackers thought was the police closing in. As the terrorists ran to investigate, they gave Ramamoorthy the brief moment in time he needed to free himself and escape. Not so lucky were the 166 men, women, and children who lost their lives that day, as well as the hundreds more who were gravely wounded as a result of the carnage.

Let us pause for a moment to consider the implications of this terrorist assault. Ten men, armed not just with weapons but with technology, were able to bring a city of twelve million people, the fourth-largest metropolis on earth, to a complete standstill, in an event that was broadcast live around the world. The militants proved fully capable of collecting open-source intelligence mid-attack (traditional media, Internet, mobile, and social data) and using it for synchronous operational decision making. LeT simply processed the data the public was leaking and leveraged them in real time to kill more people and outmaneuver authorities. That was terrorism in the digital age circa 2008. What might terrorists do with the technologies available today? What will they do with the technologies of tomorrow? The lesson of Mumbai is that exponential change applies not just for good but for evil as well.

Data Is the New Oil

Data is constantly being generated by everything around us. Every digital process, sensor, mobile phone, GPS device, car engine, medical lab test, credit card transaction, hotel door lock, report card, and social media exchange produces data. Smart phones are turning human beings into human sensors, generating vast sums of information about us. As a result, children born today will live their entire lives in the shadow of a massive digital footprint, with some 92 percent of infants already having an online presence. From their parents' posting of their first in utero sonogram until the disconnection of their Internet-enabled pacemaker more than a hundred years later, every moment from birth to death will be digitally chronicled and preserved in the cloud in perpetuity. Our data creation cycle never sleeps, and in 2014 each and every minute of every day, we

- sent 204,166,667 e-mail messages
- queried Google's search engine 2 million times
- shared 684,000 pieces of content on Facebook
- sent out 100,000 tweets on Twitter
- downloaded 47,000 apps from the Apple App Store
- uploaded 48 hours of new video on YouTube

- posted 36,000 new photographs on Instagram
- texted 34 million messages on WhatsApp

Put another way, every ten minutes, we created as much information as did the first ten thousand generations of human beings. The cost of storing all these data is dropping exponentially as well. For instance, as of late 2014, a six-terabyte hard drive can be purchased on Amazon.com for just \$300 and store all of the music ever recorded anywhere in the world throughout history.

This vast growth in the world's information infrastructure has been dubbed the big-data revolution. The promise of big data is that long-standing complex problems become quantifiable and thus empirically solvable. Consider medicine. As all patient data are cataloged in electronic medical records, it becomes easier for doctors to mine these data sets to identify the most effective treatments, spot deadly drug interactions, and even predict the onset of disease before physical symptoms begin to emerge. Untold lives could be saved.

Across all industries, whether retail, transportation, or pharmaceuticals, there will be tremendous economic value realized as a result of big data, so much so that the World Economic Forum recently dubbed data "the new oil." There is a new-age gold rush afoot in which hundreds of companies such as IBM, Oracle, SAS, Microsoft, SAP, EMC, HP, and Dell are aggressively organizing to maximize their profits from the big-data phenomenon. And if data are the new oil, the modern currency of a digital world, then those in possession of the greatest amounts will have enormous power and influence. Just as the first oil barons, such as John D. Rockefeller and J. Paul Getty, ruled their era, so too will those who possess the largest amounts of data in today's world, as Mark Zuckerberg and Eric Schmidt have demonstrated. Companies such as Facebook, Google, and Acxiom are creating the largest data sets about human behavior ever accumulated in history and can leverage this information for their own purposes, whatever they might be, whether profit, surveillance, medical research, political repression, or blackmail.

But if data are the new oil, then like other long-established natural resources, they must be safeguarded. We don't leave 100 million

barrels of oil unprotected, and yet for the most part that is exactly what we do with the vast majority of data created. The protection of our digital information is nowhere near the levels it should be. The 100 million barrels of oil are protected by guards, fences, guns, video cameras, and sensors in the ground and along the pipelines. But what about the 100 million credit cards and customer records stored by retailers such as Target? They, as we have seen, are stored in inherently insecure and poorly defended databases. When you aggregate such vast troves of valuable data and fail to protect them, what do you think is going to happen? Our ability to capture and store information is greatly outpacing our ability to understand it or its implications. Though the business costs of storing the world's information may be driving toward zero, the social costs may be much higher, posing huge future liabilities for society and our world.

History here can be instructive. Willie Sutton, the famous American bank robber, stole nearly \$2 million over his multi-decade career in crime, which began in the 1920s. After his capture by the FBI, a reporter asked Sutton, "Hey, Willie, why do you rob banks?" His answer, oft repeated, was, "Because that is where the money is." Though Sutton could have robbed two million people of a dollar each, he chose a more logical and time-efficient approach, deciding instead to rob the currency aggregators (banks). Thus is it any surprise that criminals are going after Target, Sony, and other data aggregators when the rewards are so high and the risks so low? In today's world, data are where the money is.

Taking a cue from Gordon Moore and his eponymous law, I too decided a dictum was in order to describe the risks associated with the growing mountains of data produced. Thus I present Goodman's law:

The more data you produce and store, the more organized crime is happy to consume.

Eventually, your personal details will fall into the hands of criminal cartels, competitors, and even foreign governments. While big data may be the new oil, our personal data are more like weapons-grade plutonium—dangerous, long lasting, and once they are leaked, there's no getting them back.

Even the federal government is realizing it too can fall victim to this problem. Just look at the 2010 WikiLeaks debacle and

the hundreds of thousands of classified diplomatic cables Private Chelsea (Bradley) Manning was able to steal while working as an army intelligence analyst in Iraq. Of course just a few years later the world would meet Edward Snowden, who used his skills and access as an NSA system administrator to steal millions of highly classified files from America and its allies and share them with journalists for publication online. Some have called this type of mass information theft and disclosure the "civil disobedience of the information age." But if Manning and Snowden could (after purportedly thorough background investigations) amass and steal such vast volumes of sensitive data from the federal government, what might they do if they were working for Target, Citibank, or Apple? The exponential growth in corporate data means that trade secrets, engineering designs, technical know-how, customer lists, employee salary tables, pricing strategies, suppliers, and any other information stored on a digital device can leak. Today, any company, large or small, can have a Snowden in its midst with notable implications for its data security, privacy, and long-term economic viability.

Just one compromised e-mail account on Facebook, Google, or Apple can give hackers access to years of your e-mail messages, calendar appointments, instant messages, photographs, phone calls, purchase histories on Amazon, bank and brokerage accounts, and documents in Dropbox or on Google Drive. It is important to note, however, that the data losses we imagine today will pale in comparison with what becomes possible tomorrow. In this world, our ability to aggregate all information created by both man and machine and store it in perpetuity is far exceeding our understanding of the concomitant risks.

Bad Stewards, Good Victims, or Both?

What I did in my youth is hundreds of times easier today.

Technology breeds crime.

FRANK W. ABAGNALE

**When Sony, Target, and T.J. Maxx were hacked, whose fault was it?
Were these firms innocent victims of ingeniously inventive cyber**

attacks perpetrated by sophisticated transnational organized crime groups? Or were they deeply lax with their security precautions, remiss in implementing the most basic of protections for the hundreds of millions of accounts entrusted to them? The answer lies between the two extremes. Not only are retailers doing an ineffective job of protecting their customer data, but so too are legions of Internet start-ups and the behemoths of social media. When you volunteer your data to Facebook, Google, LinkedIn, and others, you need to be aware not only of the numerous privacy ramifications of doing so but of the criminal implications as well. These firms are routinely hacked, and the data taken are yours. How often does this happen? Way more than you might ever imagine.

Facebook's own security department has shockingly acknowledged that over 600,000 accounts are compromised every day. Did you get that? Not 600,000 accounts per year or even per month, but per day. That's one account every 140 milliseconds (a blink of an eye is 300 milliseconds). These data can be used for identity theft, criminal impersonation, tax fraud, health insurance scams, and a host of other criminal offenses. Consider the tremendous volumes of personal data you share on Facebook, and now think what organized criminals might be able to do with them. Mother's maiden name, check. Place of birth, check. Date of birth, check. Photographs of your kids, check.

Compromising your Facebook account is not the end goal; it's just the beginning. Because 75 percent of people use the same password for multiple Internet sites and 30 percent use the same login information for all their online activities, once your Facebook account password is compromised, it can potentially be used to access your bank, credit card, and e-mail accounts. In addition, third-party companies are increasingly allowing you to use your Facebook log-on credentials as your passport to the rest of the digital world. While using your Facebook account to shop, listen to music, and play games is greatly convenient, once that single sign-on is compromised, so too are all the other services.

Many social media companies have been breached, including LinkedIn (6.5 million accounts), Snapchat (4.6 million account names and phone numbers), Google, Twitter, and Yahoo! Transnational organized crime groups are responsible for carrying out

a full 85 percent of these data breaches, and their goal is to exploit the greatest amount of data possible, with the highest value in the cyber underground. Sometimes organized crime groups don't even need to hack into a computer system; it's already wide open. Just as predators on the plains of the Serengeti won't pass up an already dead animal as a free meal, so too are hackers happy to take advantage of any free data bounty that comes their way. Such was the case, for example, when the mega cloud storage data company Dropbox accidentally turned off the need for any account password whatsoever across its entire network back in 2011. As a result, any person could read any file posted on the Dropbox network.

You might think that if your social media or Internet accounts were compromised in such a manner and you suffered harm, such as identity theft or tens of thousands of dollars stolen from your bank account as a result of somebody else's negligence, you might have recourse to sue those who put your information at risk. Of course, you do not. You waived all of those rights when you clicked "I have read and agree to the terms of service," a caveat that holds these companies completely harmless for such breaches. And Facebook makes it clear:

We try to keep Facebook up, bug-free, and safe, but you use it at your own risk. We are providing Facebook as is without any express or implied warranties . . . We do not guarantee that Facebook will always be safe, secure or error-free . . . [Y]ou release us, our directors, officers, employees, and agents from any claims and damages, known and unknown, arising out of or in any way connected with any claim you have.

By the way, it is not just organized crime groups that are going after the massive data repositories you've created with Google, Yahoo!, and Facebook; it is governments, foreign and domestic, as well. For example, in January 2010 Google went public with news of a massive attack across its network and blamed the attack on the Chinese government. Google reported that Chinese authorities were going after the Gmail accounts of activists in the United States, Asia, and Europe who had raised concerns about China's

human rights practices. Also targeted in the incident were trade secrets and Google's source code—the very software that runs Google and its products.

Though Google admitted being attacked, the exact extent and nature of what was taken were closely guarded company secrets. Later, however, it was revealed that hackers tied to China's People's Liberation Army (PLA) took the source code for Google's global password management system. The theft of Google's source code could readily have provided the Chinese persistent access to the passwords of millions of Google's customers worldwide and have allowed the PLA to remain hidden within Google's systems on a long-term basis. Have you changed your Google password since 2010? If not, the PLA may have a copy of it. Whether Internet and social data companies are bad stewards of our data, highly targeted victims, or a little bit of both, the fact of the matter is that any data we entrust to the sites and companies could leak to criminals, terrorists, and others.

Data Brokers Are Poor Stewards of Your Data Too

One of the problems with having shadowy and poorly regulated data brokerages amass huge volumes of information on us is that these companies can readily be hacked as well. When firms such as Acxiom store trillions of records on each of us, those records will be targeted by organized crime because, as Willie Sutton reminds us, that's where the money is. This theft of large-scale data sets from data brokers has been going on for many years, and back in 2002–3 more than 1.6 billion customer records were stolen from Acxiom and its clients. According to court documents, the hacker responsible for the theft, Scott Levine, was able to download more than eight gigabytes of Acxiom files, making it one of the largest ever intrusion cases involving the theft of personal data.

More recently, in 2013, the data broker Experian mistakenly sold the personal data of nearly two-thirds of all Americans to an organized crime group in Vietnam. The epic fraud meant that the Social Security numbers of 200 million Americans were now available to the thieves around the world. The data sets obtained were

known as "fullz" in the criminal underground because they contain the full set of information required for criminals to apply for credit cards and take out loans in the names of their victims. The massive breach of security occurred because Experian failed to do due diligence on the Vietnamese hacking organization, which had established a front company posing as a U.S. private investigation firm in order to purchase the data for its crime commission. Get that? Experian sold 200 million user data files to an ID theft ring. The data were eventually put up for sale on dozens of hacker ring-sites, including SuperSet.info and FindGet.me, selling for just sixteen to twenty-five cents a record, with payment accepted via untraceable online currencies such as Liberty Reserve and WebMoney. Experian learned of the compromise and its complicity in the affair only after it was contacted by the Secret Service, which discovered the information for sale on the hacker Web sites.

And why on earth would a purportedly reputable firm sell the data without doing due diligence? The answer, as usual, lies in the money. Data brokers make money when they sell data, not when they protect it. In the course of the investigation, it was uncovered that criminals had accessed the Vietnamese data set at least 3.1 million times before it was taken down—but of course by then, the damage had been done.

Given the ready availability of data on any one of us, organized crime groups have now even started their own data brokerages and front companies providing illicitly obtained information on any particular target of interest. An example of this was seen when Russian hackers created a Web site known as Exposed.su to demonstrate their hacking prowess to their fellow criminally inclined buying public—bona fides, if you will. Boasting of their ability to get data on anybody, the hackers freely hosted credit files on a wide number of public figures in politics, law enforcement, and entertainment.

To obtain their ill-gotten goods, the thieves subverted the security systems at Equifax's AnnualCreditReport.com Web site and obtained the full credit reports of all those targeted. Those who fell prey to the attack included a who's who of celebrities, among them Ashton Kutcher, Kim Kardashian, Jay-Z, Bill Gates, Beyoncé,

Robert De Niro, Lady Gaga, and Sean Combs. Also breached were the credit reports of a number of extremely high-profile government figures such as First Lady Michelle Obama, Vice President Joe Biden, former president George Bush, the FBI director Robert Mueller, the CIA director John Brennan, and Attorney General Eric Holder, as well as the LAPD chief Charlie Beck.

Once the Exposed.su hacker crew obtained the complete credit reports on those listed above, they posted them in full online in PDF format. There for all the world to see were the Social Security numbers of the victims, their dates of birth, every address they had ever used, personal phone numbers, legal judgments against them, and other personally revealing information such as how many hundreds of thousands of dollars they charged every month on their American Express black cards or how many millions they owed on their mortgages. The credit reports of those affected were viewed nearly one million times before the sites were eventually taken down.

As noted in the last chapter, large data brokers create highly segmented lists of clustered individuals such as "Caucasian, high school educated, rural, family oriented, and interested in hunting, fishing and watching NASCAR." Now it appears as if certain data brokers are also creating lists that are of direct benefit to organized crime groups, who will pay top dollar for such criminal leads. Scammers are a lucrative fountain of revenue for data brokers, and as such the data industry is happy to create lists that cater to criminal customers as well. Though data brokers would disagree or disavow any responsibility for what happens with the lists, clusters of individuals such as "'gullible' pensioners who 'want to believe their luck can change'" are nothing more than an invitation to defraud senior citizens of their life savings.

For data brokers such as ChoicePoint, Experian, and Equifax, the economic incentives are gravely misaligned from a public risk and security perspective. This is particularly true in the age of big data, when organized criminals now find themselves in the knowledge management business. They are an efficient, effective, and industrious force in the world of big data, and the more we create, the more they are happy to consume.

Social Networking Ills

Social media are great fodder for identity theft, as all the information criminals need to pursue you is freely available online, whether it's your date of birth or your mother's maiden name on your Facebook account. You may be thinking, "Criminals can't see that information . . . I've blocked it in my privacy settings." If only the system worked as advertised. There are many reasons why any information you post to Facebook leaks. First, as noted above, when Facebook updates its ToS, it will often reset your desired privacy settings back to the least private options available, making these data available to anybody, especially its advertisers. Second, with 600,000 Facebook accounts compromised daily, it's only a matter of time before criminals get around to you. Last, given that social data are now "where the money is," criminals have created specialized tools, in the form of targeted viruses and Trojans, to take over your Facebook and other social media accounts without your permission.

At least 40 percent of social media users have been exposed to one form of malware, and more than 20 percent of us have had our e-mail or social networking account compromised or taken over by a third party without our permission. Bad guys trick users into clicking on links in posts and messages that purport to come from friends or colleagues using a technique known as social engineering. Criminals take advantage of the trust we extend to those in our social network by masquerading electronically as these trusted parties, invariably tricking users to click on a link that will ultimately infect a computer with a virus, Trojan, or worm. Moreover, organized crime groups are extremely quick to react to breaking news, which they use to dupe innocent users to click on as a means of infecting them. Whether it was the earthquake in Haiti, Justin Bieber's arrest, or Miley Cyrus in the nude, the headlines are too good to ignore and thus people click on them. When Malaysia Airlines Flight MH370 went missing over the Indian Ocean, scammers were ready to go with fake photographs of the plane and purported videos showing "MH370 found at sea, shocking video just released by CNN." The messages spread like wildfire over social media to a curious public eager for answers, not realizing they had

just infected their machines with viruses. Sometimes curiosity really does kill the cat.

One of the best-known pieces of social media malware was known as Koobface (a variation of "Facebook"), which targeted Facebook users around the world. The malicious social media worm spread by tricking users to click on a Facebook link with an impossibly compelling headline such as "OMG—I just saw this naked video of you!" Who wouldn't click on such a message? Unfortunately, one curious click can lead to a flurry of malware. Once infected, the Koobface worm steals any available log-in credentials it can find on your machine, including those for your Facebook, Skype, Yahoo! Messenger, and Gmail accounts. Koobface can also force your computer to take part in denial-of-service attacks against third parties and hijack your Web search returns and clicks to take you to untrusted Web sites. The malware was designed and disseminated by a hacking group in St. Petersburg, Russia, and though the criminals responsible were individually identified and even publicly named, Russian authorities have refused to extradite them to face trial for their crimes.

Of course these days, social media attack tools have become streamlined, and one need not even be a master hacker to steal information. For example, Firesheep is a simple Firefox browser plug-in that anyone could download to take over the Facebook session of others on the same network and hijack their Facebook accounts. With this, for example, if you checked your Facebook account at a local Starbucks while sharing the network with twenty-five other people in the coffee shop, and if one of them was running Firesheep, the hacker could use the plug-in to log in as you on your own Facebook account. Easy as pie. Once logged in, the crook could see all your personal information, change your account settings, and post anything he or she wanted on your wall or in messages to other users. This technique is sometimes known as session hijacking or "sidejacking" and is ridiculously easy to execute.

Criminals are also targeting users on social media sites via third-party apps and online games, attacks that grant them access to your bank account and can ruin your credit. This was a lesson Lisa Lockwood of Baltimore, Maryland, learned the hard way when the information her seventeen-year-old son had provided

a Facebook gaming app came back to bite them both. The game offered the teen extra gaming points in exchange for filling out an account application that asked for his Social Security number. Without thinking, and with visions of more points to "level up" dancing in his head, the teen completed the application, never realizing his Social Security number was about to be used by criminals to complete seven separate car loan applications on his behalf in a matter of days. It was only when the boy's mother received a telephone call from a local Subaru-Volkswagen dealer inquiring about her son's credit application for a new car that she learned of the incident.

Illicit Data: The Lifeblood of Identity Theft

The explosion of data has led to the creation of a brand-new industry for transnational organized crime groups, and mass identity theft is the result. According to the Congressional Research Service, identity fraud cost Americans nearly \$21 billion in 2012, and more than 13.1 million Americans are reportedly victims of identity fraud annually. That works out to about one American every two seconds. Furthermore, the theft of this personally identifiable information is a gateway crime that leads to any number of other criminal offenses such as financial fraud, insurance fraud, tax fraud, welfare fraud, illegal immigration, and even terrorist finance. Exponential growth in data is leading to exponential growth in online crime.

Children are the fastest-growing group of victims of identity theft. They are particularly vulnerable because they don't have early-warning systems built in as do adults. If somebody fraudulently charged \$500 or \$1,000 to your credit card, you would likely notice it on your next billing statement, but children don't get credit card statements. Thieves who pilfer their identities can use them for eighteen years, and only when these young adults apply for credit themselves, such as college student loans, do they learn that their credit history has been destroyed by information thieves. In the United States alone, 500,000 children are victims of

identity theft annually. According to a study of 40,000 children by Carnegie Mellon University's CyLab, kids are shockingly fifty-one times more likely to be victims of identity theft than adults. From toddlers to teenagers, young people are readily targeted because their credit histories are nonexistent and thus a tabula rasa for organized crime groups. Parents don't find out about the crimes and identity thefts until years and years later, when suddenly they are confronted by aggressive bill collectors attempting to collect on their children's unpaid debts. Given the extent to which children and young adults live their lives online, and the aggressive ways in which data brokers and large companies are pursuing them, it is perhaps to be expected that they would face significant threats from identity thieves. If only these financial woes were their biggest problem. As we shall see, the data we all leak can lead to physical dangers as well.

Stalkers, Bullies, and Exes—Oh My!

The volumes of data about you sloshing around online are useful not only for identity thieves but for legions of other criminals as well. Old-world crimes are increasingly enabled by newer technologies, and big data allow traditional criminals to target you with ever-greater precision. Through our persistent 24/7 online lifestyles, we are reachable at all times, even by those who we wish could not reach us. What is odd about this phenomenon is that often we, through our voluntary provision of information or via data leaks, are making it easier for stalkers, harassers, and criminals to find us.

Take, for example, the case of cyber bullying. Though bullying has always been a problem in schools, the Internet provides cyber bullies with instant access to their victims, not just in the school yard, but everywhere, at all times. The threats come online, via e-mail, on social media, on mobiles, and even via messaging apps and games. According to the National Crime Prevention Council, nearly half of all teens are affected by cyber bullying. For young people facing the persistent harassment, it seems as if there

is no escape; as a result, a full 20 percent of middle school students admitted to "seriously thinking about attempting suicide" because of online bullying.

Children are not the only ones victimized by cyber bullying; cyber stalking is increasingly affecting the adult population as well. In fact, the ever-expanding flows of data about us and our persistent online presence have helped to transform the Internet into a fertile ground for a new breed of criminal known as the cyber stalker. These offenders use the Internet as "their weapon to harass, threaten and intimidate their prey." Cyber stalkers do this by sending unwanted e-mails, text messages, postings, and tweets and by spreading rumors about the victim online. Using the data that each of us leaks every day or that are commonly available via data brokers, cyber stalkers can easily obtain detailed information about their victims, including their home and work addresses and phone numbers. Often these details are used by cyber stalkers to confront their victims in person.

Facebook has been of particular use to stalkers. With each of us having hundreds of friends, many of whom we've never met, it would be wise to more carefully consider who was actually sending those friend requests. Christopher Dannevig used Facebook to find his victim, Nona Belomesoff, an eighteen-year-old woman from Sydney, Australia, and meticulously studied her profile before contacting her. It was Belomesoff's frequent posting about her love of animals on her Facebook page that gave her stalker the idea of how to persuade her to meet him. Using the social media data the young woman was innocently leaking, Dannevig created a fake profile under the name "James Green" and claimed he worked as an HR recruiter for a well-known local animal rescue group. The woman's stalker used the very details she had posted to con her. After creating the fake profile, Dannevig contacted Belomesoff and exchanged a series of messages, eventually befriending her and gaining her trust. Shortly thereafter, he announced there was a job opening at the animal rescue charity for which she would be a perfect fit. Belomesoff agreed to meet him for an interview, and her stalker offered to drive the young woman to the animal shelter located in a secluded area just outside Sydney. Thrilled at the prospect of having found a paying position working with the

animals she loved, she agreed to travel with the man. It was there, in the deserted outskirts of Sydney, that Dannevig strangled and murdered the girl.

Though the threat from strangers using our data to find and stalk us is real, it pales in comparison to the perils we face as a result of domestic violence and harm by those with whom we once shared an intimate relationship. Facebook makes it easy to keep tabs on a former boyfriend, girlfriend, or spouse out of a normal, though unhealthy, level of prurient curiosity. New friends, life updates, changes in relationship status, travel locations, and vacation plans are all of great interest to former partners. The phenomenon is so common that "Facebook stalking" has even entered the common lexicon.

But for some, the data we leak fuel much more than curiosity on the part of our ex-partners. In those relationships that involved domestic violence in the real world, 45 percent of victims admitted that their abusers followed and attacked them online as well, causing many to suffer from PTSD. Social data can also provide details as to their locations, and because abusers often go to great lengths to find their victims, an innocent tweet, check-in, or status update could be as effectively dangerous as a bullet. For instance, Paul Bristol flew from Trinidad to England to stab his ex-girlfriend to death after seeing a post of a photograph with her new boyfriend on Facebook.

Another challenge in the world of big data is that the information we share and intend to keep private leaks out to others. Often we are betrayed by those with whom we have entrusted the most intimate details of our lives, particularly with the photographs we have shared. Sexting, or the sharing of sexually explicit SMS photographs via mobile phones, is a growing phenomenon, and some 67 percent of college-aged students have admitted to engaging in the practice. Unfortunately, photographs shared in such a manner do not just disappear, and these data detritus, like all other forms, often come back to bite their originators in unexpected ways.

Web sites such as MyEx.com allow the jilted to share photographs of their ex-lovers on a single Web site. There are more than seven hundred pages of photographs of naked men and women, with paragraphs of complaints about those in the photos—terrible

lover, cheated on me with my sister, small penis! Another wildly popular site, IsAnyoneUp.com, was created by twenty-four-year-old Hunter Moore as a data repository for anyone to submit naked photographs of their exes and enemies and was visited by a quarter of a million people daily. The phenomenon has become so popular it now has its own name: revenge porn. Moore's site by design listed next to each photograph links to the person's Facebook or Twitter account, her full name, and hometown and made this information fully indexical and retrievable in Google so that it would show up in an innocent search by a third party looking for that person. Every naked photograph was accompanied by a comments section that allowed members of the public, and Moore himself, to comment on and ridicule the photographs.

Online Threats to Minors

According to the Pew Research Center, today 95 percent of young people in the United States are online, and 74 percent of teens aged twelve to seventeen are mobile Internet users, often accessing the online world via cell phones and tablets. Moreover, 95 percent of young people aged ten to twenty-three have at least one social media account. Much of this Internet access takes place outside the purview of their parents, 74 percent of whom say they are overwhelmed by modern technology and don't have the energy, time, or ability to monitor what their children do online. That is unfortunate, for although cyber bullying by peers is a major source of stress for young people, they face even greater dangers in our increasingly connected world.

Child predators have used technology to great effect to zero in on children for the purposes of sexual abuse. So common is the practice it even had its own television show highlighting the phenomenon, NBC's *To Catch a Predator*. The challenge for children is that four out of five of them cannot tell when they are talking to an adult posing as a child online. Their new online friend—the other eight-year-old girl one town over—could just as likely be a fifty-year-old man two states away, willing to travel across state lines for the purpose of child abduction.

Given that pedophiles have noted preferences in the children they pursue (age, gender, hair color, height, and so forth), any photograph posted on social media or elsewhere online can be used as a shopping catalog or virtual marketplace for child sex abusers looking for victims to target. Pedophiles make it their business to know the very latest games, messaging services, and virtual worlds of interest to children and will seek out their victims in every possible online forum, using a variety of tools ranging from Xboxes to iPads. Lest you think the demand for such disturbing photographs is limited, law enforcement sources have identified at least twenty-two million such images and videos in the United States alone, and some password-protected child pornography Web sites have up to thirty thousand paying members.

Today the volume of pedophile images is growing, not because an adult has necessarily abducted a child and abused him or her, but because young people are readily targeted via subterfuge and social engineering.

Such was the case with Amanda Todd of British Columbia, Canada, who at the age of twelve was coerced into flashing her breasts on a live video chat site popular with teens known as blogTV. The anonymous person who made the request seemed nice and complimented and flattered young Amanda on how pretty she was. In a moment of teen naïveté, Amanda revealed her breasts, assuming the requester was another teen. As time passed, however, she realized she had encountered a much darker force. A year after her disrobing, Amanda received a message on Facebook from a man under a pseudonym who demanded the young girl reappear nude and perform sex acts on camera for him. If she refused, he threatened to release the original video of her topless. To prove he was serious, the attacker revealed the names of Amanda's friends and family, her address, and the school she attended and said all would be shown her video. The young girl demurred, and the harassment began.

Her tormentor created a fake Facebook profile in Amanda's name and used a photograph of her bare chest as the profile picture. He then began sending friend requests to all of Amanda's friends, family members, and teachers whom he had discovered on her true account. Amanda was unaware of the incident until the police, wor-

ried about the implications, came knocking on her family's door at 4:00 a.m. on Christmas Eve. Amanda was horrified. Upon returning to school, she was bullied and harassed relentlessly. For the young teen, the pressure was unbearable. Depression, anxiety, and panic disorders set in. She cried herself to sleep every night and was disowned by her friends, who blamed her for appearing in the video. She ate lunch alone every day and began cutting herself.

To avoid the pain and ridicule, Amanda switched schools and moved to a different town. Sadly for her, the persecution continued. Her stalker followed her activities online and created a fresh Facebook page to advise her new teachers and classmates of her topless video. At the new school, the bullying in class got so bad that a group of girls attacked her on the playground, punching her and pushing her into a muddy ditch. Adding insult to injury, the perpetrators even posted a video of their attack on YouTube. Amanda went home that afternoon and drank from a gallon of bleach in an effort to bring all her pain and suffering to an end. She was rushed by ambulance to a hospital, where her stomach was pumped. Though Amanda survived, the harassment continued. On her Facebook page, other students posted photographs of Clorox containers and encouraged her to "try harder next time." In response, on September 7, 2012, Amanda posted a nine-minute YouTube video detailing her struggle with bullying and self-harm. In the deeply emotional video, she shared her experiences of being bullied, while powerfully moving music played in the background. Shortly thereafter, the pain became too much for Amanda to bear, and she committed suicide at the age of fifteen.

Amanda's video went viral after her death and was viewed millions of times. Some police thought that Amanda could have been a victim of "cappers," a disturbing trend in which gangs of online pedophiles revel in coercing kids into stripping on camera and recording them. Worse, the pedophiles then use the videos to blackmail teens into performing more explicit sex acts online and in person. The tragedy of the Amanda Todd affair is multifold. A young girl innocently leaks data about herself online and is stalked on social media and in the real world, leading to her death. But tragic though it may be, this is not an isolated occurrence, and the speed at which the trend is growing is disturbing. Big data bring

with them big risks, and even information innocuously shared by an adult can be used by pedophiles.

In 2011, police in Melbourne, Australia, uncovered a number of child molesters targeting lonely single mothers with young daughters by trawling their online profiles and searching references to their children. The goal of the pedophiles was to work their way into the home, usually using a false name and pretense, in an effort to begin a relationship with the child's mother. Once invited into the home and welcomed there, the pedophile would use his time alone to ultimately target the single mom's young daughters. Criminals and predators play by different rules and are happy to use all our data as fodder for a wide variety of unwanted consequences.

Haters Gonna Hate

Your social media profile may also make you vulnerable to another type of attack—a hate crime—one in which bigots, racists, and homophobes target individuals online based on their race, religion, creed, color, gender, or sexual orientation. Such incidents have taken place on Facebook, Instagram, ICQ, Twitter, and numerous other social media services. Facebook was accused of hosting so much violent hate speech that CNN ran a story titled “Facebook/Hatebook?” to document the phenomenon.

Online data allow criminals to locate victims based on the attacker's individual biases. In one case, an assailant in Texas targeted a gay man whom he met on the social media platform MeetMe.com. After arranging a rendezvous with the victim, the attacker kidnapped him, beat him unconscious, bound his wrists, and threw him into the trunk of his car before dumping him on the roadway. Brice Johnson of Fort Worth was charged in the attack and upon his arrest said he just wanted to teach the gay man a lesson but admitted “the joke may have gone too far.”

As horrific as the Texas incident was, the volume of hate crimes involving social media in the United States pales in comparison to that in Russia, with thousands of attacks credited to an emerging neo-Nazi youth movement in the country. In a one-hour documentary produced for the U.K.'s Channel 4, reporters documented over

fifteen hundred kidnappings in which bands of vigilantes hunted young gay men on the streets and online. The victims, mostly teenagers, are kidnapped, assaulted, and terrorized during their abductions, which are often boldly filmed. The attackers fear no retribution from complicit police in the country and thus have posted videos of their brutal attacks on both Facebook and Instagram in an effort to further humiliate those injured. Despite the volumes of documentary evidence posted online in hundreds of cases, no arrests or prosecutions have ever occurred, even when the victims were murdered or left permanently disabled—an odd incongruity given the ability of Russian police to systemically monitor all Internet activity in the country across all social media channels.

Burglary 2.0

Have you ever casually posted on Facebook that you were going on vacation? A strikingly large percentage of people will talk about their future travel plans online, mentioning how much they are looking forward to their trip to Disney World or their weekend beach getaway. What they don't realize, however, is that criminals are perfectly capable of scraping these data off the Internet and using them for their own purposes (think Goodman's law: *the more data you produce and store, the more organized crime is happy to consume*).

In the old days, if a burglar wanted to target a particular home, he would traditionally look for the telltale signs that the residents were away on vacation—a pile of newspapers in front of the house or a porch light that remained off at night. But even burglars have modernized their tools and are increasingly using technology to find their targets and property to steal. Welcome to the world of burglary 2.0. These criminals are increasingly searching your postings on Facebook, Google+, and Twitter and using the data you leak there for lead generation purposes, just as would any other good salesman or prospector. To highlight this threat, a group of Dutch computer developers concerned by our oversharing created a Web site called PleaseRobMe.com. There they aggregated locational data from people's tweets and Foursquare check-ins and cre-

ated a searchable database of the information collected. The result: would-be burglars could check by postal code and see who was away and for how long and was thus suitable for burglary. It's criminal target selection at the click of a mouse.

The threat is not purely hypothetical: real-world burglars are indeed monitoring social data. One such example was uncovered in 2010 when a group of local criminals in Nashua, New Hampshire, turned to Facebook to determine when victims were away from their homes. Nashua police discovered that this crime ring checked Facebook updates of their victims before carrying out more than fifty break-ins and stealing nearly \$200,000 in property during their burglary spree. These are not your grandfather's burglars, and criminals are rapidly adapting to technologies that help them commit more crime. According to a 2011 study of convicted burglars in the U.K., 78 percent of them admitted monitoring Facebook, Twitter, and Foursquare before pinpointing a specific home to rob. They also admitted using tools such as Google's Street View to scope out the property beforehand and plan escape routes when fleeing from the scene of the crime. The results highlight the ways in which criminals can use the data we are leaking against us.

Another way in which burglars are targeting you is via the locational data embedded in the files you've posted online. As noted previously, these so-called metadata are silently implanted and hidden in the photographs, videos, and status updates you share with others via your mobile devices and reveal the date and time the photograph was taken, the serial number of the phone or camera, and, most important, the longitude and latitude (GPS coordinates) of where the picture was snapped. The metadata containing this information, though not immediately obvious when watching a video or viewing a picture, lie there readily accessible by anybody who knows how to download a simple browser plug-in to access them. With any one of hundreds of free tools, suddenly your photographs come to life and magically appear on a Google Map that allows anybody to zoom in on the precise location where the picture was taken. Such is the miracle of cyber casing—using hidden geo-locational data to plan one's crimes.

Those very same metadata are contained in millions of photo-

graphs posted to sale and auction sites such as Craigslist and eBay. For example, a photograph of a diamond ring or an iPad posted on Craigslist might have embedded with it the precise location of your home where the photograph was taken. This information allows tech-savvy thieves to use Craigslist as nothing more than a shopping catalog for goods soon to be stolen.

When Keri McMullen and Kurt Pendleton of New Albany, Indiana, decided to sell their plasma TV and stereo system, they posted photographs of the items online. A few days later, the couple mentioned on Facebook they would be attending a concert in nearby Louisville that Saturday night. That's all the information that thieves needed to burglarize the home containing the electronic goods they were seeking. The burglars knew they could take their time because the couple would be at the concert for hours. In the end, the couple were robbed of their flat-screen television, two laptops, a stereo rack and all its components, and a high-end 35 mm digital camera. This is but one of several ways in which criminals too are engaging in e-commerce, cyber casing your home from the inside with the data you are leaking.

Targeted Scams and Targeted Killings

Another way in which criminals take advantage of your online vacation postings and travel status updates is by scamming your grandparents. Yes, criminals monitor your social media and watch you post your vacation photographs online in real time. Once you've done so, con artists analyze your social networks looking for elderly relatives, usually grandparents, whom they notify of your "unfortunate accident." The scam goes something like this: "Hello, Grandma? Yes, I have some terrible news. Your grandson Peter was involved in a terrible accident in Barbados. The hospital won't accept his American insurance and refuses to treat him until we put down \$10,000 for the surgery. If you don't help, Grandma, he may not make it." How do criminals get away with this? Because we help them, though unwittingly, through the information we share in the new world of big data. Facebook tells the world—including orga-

nized crime—exactly who our grandparents are and how to find good old Aunt Margaret to pressure her: “It’s looking really bad . . . Peter has gone into a coma . . . Please send the funds immediately!” Hundreds of victims have been defrauded by the scam, and millions of dollars have been sent via Western Union and MoneyGram as a result.

While Internet scammers monitoring your social media actions may cost you a few thousand dollars, when narcos follow you on Twitter, it may cost you your life. Drug cartels implement a wide variety of sophisticated counterintelligence programs to collect data from social media platforms, blogs, and government tip lines as a means of exposing potential threats.

Comments made online that are perceived to be unfavorable to the cartels are dealt with swiftly. In September 2011, just across the Texas border in Nuevo Laredo, Mexico, residents on their way to work awoke to find two bodies strung up by their arms and legs, hanging in the air from a pedestrian overpass. The victims, a man and a woman in their twenties, had been badly tortured, and the female was fully disemboweled. Above the dangling bodies read an ominous warning on a large posted sign: “This will happen to all the internet snitches . . . Be warned, we’ve got our eye on you. Signed, Z,” a reference to the Zetas, one of Mexico’s largest and most violent drug cartels. These cartels are equally savvy with their social media campaigns, uploading photographs and videos of themselves on Facebook and Twitter in the act of decapitating their victims with chain saws and machetes.

Meanwhile, terrorists not only leverage social media for operational purposes, as we saw in Mumbai, but also tweet in real time to drive public opinion and cause more fear among their targets. During the September 2013 assault on the Westgate shopping mall in Nairobi, Kenya, members of the al-Shabab group who carried out the attack live tweeted their slaughter from inside the shopping center. The Somali-based terrorists murdered sixty-three innocent civilians and wounded nearly two hundred more. The group even posted photographs on Twitpic of the carnage inside the Westgate and accused the Kenyan government itself of destroying the shopping center, using the hashtag #Westgate.

Counterintelligence Implications of Leaked Government Data

Organized crime and narcotics organizations are using social media to gather intelligence on government and law enforcement officials. For example, when two Maricopa County, Arizona, sheriff's deputies pulled over a vehicle in 2010 for DUI, a search of the vehicle uncovered a variety of data CDs, including one with the names, photographs, and Facebook profiles of nearly thirty patrol and undercover officers. Non-state actors and hacktivist groups such as Anonymous and LulzSec also go after the social data leaked by government officials.

In a 2012 incident, the hacktivist group LulzSec demonstrated its power to even go after the FBI. Because the hacktivist organization had begun to tap the personal e-mail addresses of individual police officers, especially those working the cyber-crime beat, they were able to intercept an e-mail message notification of a conference call taking place between the FBI, Scotland Yard, and several other global police agencies. The topic of the call? A discussion of "the on-going investigations related to Anonymous, LulzSec, Antisec and other associated splinter groups." Once in possession of the e-mail, the hacktivists merely used the dial-in information and access code to silently participate in the call. As the world's premier law enforcement organizations discussed the case against Anonymous and LulzSec, there the hackers sat on the line listening to police unknowingly brief them on the status of the investigation. The call was even recorded by LulzSec, which then posted it to YouTube, greatly embarrassing the police authorities involved and undermining their investigation.

So No Online Profile Is Better, Right?

Not necessarily. Given all the risks from posting social data online, it may seem as if not participating in Facebook or LinkedIn would be the obvious solution. But a social media boycott brings its own challenges. If you don't own and control your own online persona, it's extremely easy for a criminal to aggregate the known public information about you and create a social media profile for you and

use it for a wide variety of criminal activity, ranging from identity theft to espionage. Indeed, there are many such examples of this occurring, particularly for high-profile individuals. For instance, in late 2010, an organized crime group commandeered the identity of the secretary-general of Interpol, Ron Noble, and created a Facebook Web page for him. The criminals took his official photograph from Interpol's own Web site and extracted data from his official biography to build out his fake Facebook profile. The organized crime group began friending other senior law enforcement officials around the world in the persona of Noble and posed operational questions of them via the social media service. In particular, criminals posing as Noble tried to gather intelligence regarding Operation Infra-red, an Interpol global undercover operation to locate and arrest high-priority international fugitives. It is unclear how many fell for the ruse and how much data is shared, but dozens of the world's most senior police officials accepted the purported friend requests.

The Spy Who Liked Me

Industrial espionage too has found a powerful ally in social networks. In the second chapter of this book, we learned about the Massachusetts wind-turbine firm AMSC, which lost nearly a billion dollars of valuation after its computer source code was stolen via a Chinese espionage operation. What wasn't explained, however, is how the attack was carried out.

When the Chinese officials decided to purloin the source code on behalf of Sinovel, a state-owned company whose wind turbines were supplied by AMSC, a simple check of LinkedIn would have provided their agents with access to the roster of employees working at the Massachusetts firm. Once the Chinese had completed a review of all employees and their positions, a list was generated highlighting those targets likely to have best access to AMSC's highly prized source code. One such person identified was a Serbian engineer working for AMSC's office in Austria by the name of Dejan Karabasevic.

The Chinese began monitoring Karabasevic across a variety of

social media sites such as LinkedIn, Facebook, and Twitter. They learned he was going through a nasty divorce and had recently been demoted at work—the exact types of vulnerabilities any modern intelligence agency looks for when targeting potential recruits. Through his various postings, the Chinese were able to re-create Karabasevic's "pattern of life"—plotting on a map his favorite coffee shops, gyms, and restaurants, his home and office, his travel times, and his daily routines. They also learned that he had a penchant for Asian women. Armed with all of this information, the Chinese began their recruitment process.

Chinese handlers approached Karabasevic and offered him a "consulting" opportunity to work with them. In the end, they were readily able to persuade Karabasevic to provide the source code (secret sauce) that allowed Sinovel to build its own wind turbines without AMSC. Most important for Karabasevic, his Chinese handlers established an office in Beijing for him and promised "all the human contact he could want . . . in particular with female co-workers." After the theft occurred, hundreds of Skype chats and e-mail messages were uncovered between Karabasevic and his Chinese handlers. In one note Karabasevic wrote, "All girls need money. I need girls. Sinovel needs me." To allay his financial concerns, meet his companionship needs, and bolster Sinovel's bottom line, the Chinese offered Karabasevic \$1.7 million for the source code. The economics of the deal were fascinating and instructive: Karabasevic receives \$1.7 million; AMSC loses a billion dollars in valuation and intellectual property, which Sinovel captures by purportedly selling pirated AMSC products around the world. A great return on investment for Sinovel and for those unencumbered by the moral implications of such dealings.

As should be obvious by now, there are numerous risks from the exponentially growing sea of data in which we find ourselves. Not only do we face an onslaught of data mining from Internet companies, marketers, and third-party data brokers, but criminals, terrorists, and rogue governments too have us under constant assault and surveillance, forever aggregating and amassing. Those trails of data detritus, however, are growing exponentially longer thanks to the computers we're now carrying with us at every turn—our mobile phones.