

CHAPTER 7

I.T. Phones Home

Mobile phones are one of the most insecure devices that were ever available, so they're very easy to trace and they're very easy to tap.

EVGENY MOROZOV

On March 21, 2002, Milly Dowler, a thirteen-year-old from Surrey, England, phoned her father to say she'd be home soon. Hours later, the teen still hadn't arrived, and calls to her cell phone went unanswered. By the following evening, a massive search of the area was under way, and Milly's disappearance had made national news.

As part of their investigation, the Surrey police accessed the mobile phone voice mail of the missing girl in their search for clues. Ongoing checks with her mobile phone carrier revealed that five days after her disappearance, the voice-mail system had been accessed, and a new message that had arrived that day was played by parties unknown. The discovery gave the Dowlers hope that their daughter was still alive. As the weeks dragged on, additional messages left on Milly's voice mail continued to be retrieved and deleted, leading investigators to question whether the missing girl was in fact a runaway.

Sadly for the Dowlers, Milly was no runaway but was abducted, her body discovered twenty-five miles away from where she was

last seen alive six months prior. In an instant, Milly's case was declared no longer that of a missing person but a full-blown murder investigation. But one fact continued to confound police: Who had been repeatedly accessing the young girl's mobile phone long after she was missing and now presumed to have been dead? Was it the killer? A jealous boyfriend? Her parents? For nearly a decade, the haunting question went unanswered until June 2011 when the mystery was finally solved. The culprit was one nobody would ever have guessed.

In a lengthy article published by the *Guardian* newspaper, it was revealed that Milly's phone was among those targeted by Rupert Murdoch's *News of the World* in a scandal dubbed Hackgate by the British press. Milly's phone was hacked not by the killer, her parents, or a boyfriend but by those looking for a scoop for their tabloid pages. Poor Milly and the Dowlers were not the only victims of Hackgate; so were numerous celebrities, politicians, and even members of the British royal family, which might make sense given their high public profiles. But ultimately, it was discovered that reporters and private investigators hired by the *News of the World* had extended their mobile data theft operations well beyond that of high-profile public figures. Shamefully, they had also hacked into the mobiles of the relatives of British soldiers killed in Iraq and Afghanistan, as well as victims of the tragic 7/7 London terrorist bombings. The appalling details of the case led to a global public outcry and the closure of Murdoch's *News of the World* after 168 years of continuous publication. Dozens of employees and contractors of the paper were arrested, including the private investigator it had hired to gain details of the young girl's disappearance.

Of course for two grieving parents, the sanctions and arrests of those involved were of little comfort. For the Dowlers, the news that it was a newspaper that had broken the security of Milly's phone was unfathomable. Had this unlawful mobile phone hacking of a missing thirteen-year-old girl somehow impeded the investigation of their missing daughter's whereabouts? What police resources were wasted trying to get to the bottom of what appeared to be a prominent clue possibly left behind by Milly's suspected murderer—precious time wasted that might have prevented her

tragic and untimely death. We will never know, nor will the Dowlers, who have to live with the tragedy and the burning question every day for the rest of their lives.

While the actions are indeed deplorable, sadly they are all too easy to perpetrate. Our mobile phone security—that of the device that most modern citizens hold most dear—is a farce, easily exploited by organized crime, stalkers, terrorists, and even journalists lacking a moral compass or a shred of decency.

Mobile Phone Operating System Insecurity

Mobile phones are becoming our computers of choice. These “snitches in our pockets” serve as constant beacons of our activities and our locations. Just as mobile phones provide a treasure trove of data to advertisers, so too do they for criminals. Even worse, mobile phones may be the most insecure of all devices. The software is notoriously easy to subvert, the risks are poorly understood, and the systems for device protection are immature and wholly underdeveloped. As a result, smart phones are among the easiest devices to hack. While law enforcement and security services have been able to target and tap mobile phones for years, now the very same techniques are readily available to criminal enterprises and everyday hackers as well.

Today, there are viruses and Trojans specifically designed to give attackers access to your cell’s microphone, recording any sounds nearby, even when you are not on a call. Anything you do or any data you store on your mobile phone—your entire text-messaging history, your address book, photographs, call logs, social networking passwords, and account information—can all be intercepted, hacked, and forwarded to criminal organizations for future exploitation.

Mobile phone malware can be used to track your present location and allow criminals to see your position in real time, conveniently plotted on a Google map. Even your smart phone’s video camera can be turned on (without any warning light) to record you. There are so many YouTube videos, instructional Web sites, and

prefabricated criminal software programs for sale that even novices can hack a mobile phone. In fact, it's often as easy as sending an infected SMS message to your target.

One might legitimately ask, how can mobile phones be so readily compromised? The answer is that it's all about the operating system. Mobile phone operating systems are newer than their long-standing desktop counterparts and even more insecure. Criminals fully recognize that the world of big data is going mobile, and that is where they are concentrating their efforts to ensure the largest return on their malware investments. Mobile is the platform of choice. It is intimate and always with us, and criminals are adapting and innovating with alacrity.

By 2014, McAfee had already identified nearly four million distinct pieces of mobile phone malware, a 614 percent increase over the previous year. Moreover, according to a study by Cisco (and widely touted by Apple's senior vice president of worldwide marketing, Phil Schiller), 99 percent of all mobile malware is targeted against Google's Android mobile operating system. The findings are deeply troubling, especially given that 85 percent of smartphone handsets shipped worldwide as of mid-2014 were Android and that it is expected that one billion additional Android mobile devices will shipped by 2017. To be sure, the open-source nature of Android's operating system is one of the platform's biggest selling points, but with such openness and the ability to customize the free software as one sees fit comes a huge liability—security. The majority of device manufacturers and phone carriers simply implement the software poorly.

So what is it that makes it so easy to pilfer data from Android devices? Simply stated, it is a lack of updates and bug fixes to the mobile phone's operating system. New versions of Android dribble out to users from carriers as a means of forcing upgrades. In addition, carriers and handset manufacturers need to tweak each installation of Android and customize it to work with individual mobile phone models, an expensive and time-consuming process resulting in far fewer updates per device in the Android world. Worse, according to several studies, it is this customization process and the insecure software added by mobile phone companies and handset manufacturers that lead to 60 percent of the security threats

in the Android ecosystem. All those annoying apps and skins that come with your phone are known as bloatware, because they take up space on your device, are of dubious value, and serve as little more than marketing gimmicks for your handset manufacturer or wireless carrier. Not only are they bothersome, but their poorly thought-out implementation leads to the majority of security threats on Android devices.

By comparison, Apple controls its entire hardware and software ecosystem. As such, it can ensure that its mobile iPhone operating system (iOS) software works more seamlessly, and carriers are prohibited from fundamentally altering the underlying operating system with their bloatware. A comparison between Android and iOS clearly tells the story: five months after its release in 2013, 82 percent of Apple's 800 million mobile devices were using 7, the most up-to-date version of its mobile operating system. Only about 4 percent of Android users were running the latest version of Google's Android, also released the same year. What is deeply frustrating about these figures is that if all Android users were simply upgraded to the latest version of the mobile phone operating system, a full 77 percent of security threats could be largely eliminated. It is the failure of Google and its partners to make security updates widely available to its user base that allows criminals the time they need to find hole after hole in the Android OS and target it for exploitation.

Mind the App

App makers such as Rovio, Zynga, and Snapchat aren't the only ones creating apps as a means of acquiring and selling your data; organized crime groups have also adopted the practice. Though one might logically presume that any app submitted by a developer to Google's Android or Apple's App Store would have undergone a vigorous security review of its computer code and its developer, all is not as it seems. With more than a million apps in both the Android and the iOS ecosystems, strikingly little if any human verification occurs—a fact known by criminals, who have subverted the mobile app stores on numerous occasions. Instead, computer-

automated algorithms do all the heavy lifting in the review process, and the app store creators just hope it all works out.

As a result, mistakes are common, and apps that contain malware are increasingly hosted in what you would presume to be a reputable app site. By 2013, more than forty-two thousand apps in Google's store had been found to contain spyware and information-stealing Trojan programs. The malware in these apps specifically targets the data on your phone, particularly financial information. Just days after the original Android Market app store had launched, criminals had uploaded fake banking apps for major financial institutions around the world. The apps were deeply realistic and used the correct bank logos, fonts, and color schemes to add to their credibility. Tens of thousands of people were tricked into downloading the apps, and when they failed to work, angry customers called their banks, only to find out "we don't have an Android app yet."

Cyber criminals have retooled their operations to create many more fake banking apps. Though only sixty-seven banking Trojans had been identified in 2012, the number had grown to more than thirteen hundred by the end of 2013, according to Kaspersky Lab. To date, mobile malware packages have been uncovered targeting customers of the world's largest banks, including Citibank, ING, Deutsche Bank, HSBC, Barclays, and sixty-six other financial institutions around the world.

And malware is even more rampant in third-party app stores. While there is at least some limited algorithmic security screening in the official Android marketplace, there is often none whatsoever in third-party sites. As a result, more than five hundred such third-party app vendors have been found to be offering Android apps containing malware. Because there are no security reviews in these app stores, apps containing viruses and Trojans can have near-infinite shelf lives, providing lifetime annuities to the criminals who create and upload them.

While much less common, malicious apps have also been found in Apple's App Store. Although the Apple iOS ecosystem is tightly regulated and controlled, many users find the environment too stifling. When they initially purchase their products, iPhone users cannot customize their keyboards, change their default browsers,

manage files locally, or add widgets to their home screens—all features standard in Android. To get around these limitations, many users “jailbreak” their iOS devices, using specialized software to hack their own mobiles in order to obtain root administrative access to phones and control over features locked down by Apple. Jailbreaking an iOS device allows users to gain access to thousands of software programs not officially approved by Apple. Nearly ten million iOS devices have been jailbroken, and their users have turned to third-party app stores like Cydia to download their apps. While jailbreaking these devices provides much greater control to users, it also opens iOS mobile devices to the same security threats common in the Android ecosystem, including a variety of financial frauds.

Why Does My Flashlight App Need Access to My Contacts?

Hundreds of millions of smart phone users around the world have downloaded that ever-popular and convenient flashlight app. It's so useful when looking for keys in a purse or trying to open the door late at night, and most of us paid absolutely nothing for the privilege. But why does your flashlight app need access to your contacts? Why does it ask for my location? My location should be obvious: I'm in the dark; that's why I need a flashlight app! As it turns out, the majority of these apps, especially in Android, are just convenient mechanisms to steal your data, download all your contacts, ascertain your persistent location, install keystroke loggers, and capture your financial information. As a result, we are seeing the “app-fication” of crime, criminal acts reduced to the simplicity of a mobile phone application.

The permissions granted to these apps, especially in the Android ecosystem, where there is no way to deny a specific permission to a given app prior to installing it, mean you and your data are at risk. App permissions on mobile devices are akin to terms of service: we all click yes but never really stop to think about the implications of our decision. The reality is that permission means a rogue or criminal app developer now has the authority needed to commit fraud or steal from your bank account via your mobile device.

Criminals are also creating fake apps specifically to com-

mit telecommunications fraud. Three-quarters of all cell-phone malware exploits loopholes in mobile payment systems by sending fraudulent premium-rate SMS messages, each one generating \$10 in immediate profit. Multiplied by hundreds of thousands of fake SMS premium messages, the money generated is huge. In one incident, scammers were able to post fake versions of well-known popular games such as *Angry Birds* and *Assassin's Creed* into an app store. Once the app was downloaded, every time the user opened it, it would send three premium SMS messages without the user's knowledge at \$7.50 per message. In just a few hours, thieves generated tens of thousands of dollars of fraudulent charges.

Hijacked mobile phones are increasingly being used to send spam e-mail messages as they join so-called botnet networks. Botnets are a collection of enslaved, malware-infected computers that work in unison, under the control of hackers or criminals, to pump out massive amounts of spam or take part in DDoS attacks unbeknownst to the device's legitimate owner. While botnets were previously limited to desktops or laptops, now millions of mobile phones have also been commandeered, and these drone devices are under the full control of criminals and hackers who have joined them to their exponentially growing "zombie networks." These massive networks of hacked devices lie in wait, ready to be unleashed against any target at a moment's notice. Given that mobile device shipments are outpacing desktops and laptops by a factor of ten to one, it is clear that the future of computing is mobile. As such, criminals have figured out that the future of data theft, DDoS, and malware is mobile too.

Even legitimate apps can put you and your data at risk if the software is poorly written or contains undetected security vulnerabilities. Such was the case with the highly popular "social photo booth" app known as Snapchat. Snapchat is a service that allows users to send "selfie" photographs (often involving nudity) that purportedly disappear in just a few seconds after arriving on the recipient's phone. More than one billion photographs have been sent via the service, and in late 2013 Facebook unsuccessfully tried to buy the company for \$3 billion. In early 2014, it was revealed that Snapchat contained a security flaw that exposed millions of iPhone users to denial-of-service attacks.

The vulnerability meant that hackers could target your phone specifically by sending a thousand Snapchat messages in just five seconds, thereby crashing your phone and making it unavailable for your use until you performed a hard reboot of the device. Moreover, hackers were also able to compromise nearly five million Snapchat user accounts and published a database of user names and phone numbers on a hacker Web site. Worse, it was revealed that Snapchat's foremost feature—the ability to send naked photographs that would self-destruct in ten seconds or less—was also flawed. The images did not self-destruct as promised and could still be retrieved both on the recipient device and on Snapchat's own computer servers. As a result, tens of thousands of Snapchat photographs thought to have been deleted have shown up across the Internet, reposted on Instagram and on numerous revenge-porn sites. The photographs have subsequently been used for the purposes of extortion and other criminal offenses.

Mobile Device and Network Threats

The emerging threats to the data we carry on our mobile devices are not only affecting consumers but also having a major impact on business. In today's modern enterprise, BYOD, or bring your own device, has become the standard and allows employees privileged access to sensitive corporate data and applications from their own personal mobile devices. Today 89 percent of employees are accessing work-related information on their mobile phones, and 41 percent are doing so without permission of their companies.

The phenomenon, now standard practice in the workplace, means more and more corporate information is at risk thanks to point-and-click spyware attacks against mobile devices. Even when a corporate network is locked down and protected, personal mobile phones are an easy place from which to pilfer data. Criminal organizations won't waste their time going to the most secure place where you have stored your information; they will always go after the weakest link in the chain to get what they want.

Criminals are growing increasingly inventive in how they target the information on your mobile device and even the phone

networks themselves. For just a few hundred dollars, criminals can purchase and set up a femtocell, a wireless network extender to help people improve mobile phone service in areas with poor network signals. The device is in effect a mini-mobile-phone tower, and criminals can hack it to trick your mobile into believing it is legitimate, when in fact it is merely connecting to a portable mobile phone tower run and operated by criminals. Their goal in doing this? To capture all the data that is sent from your mobile, such as the password you type for your bank account or sensitive e-mails you might be sending. Rogue femtocells can be particularly useful for industrial espionage, and hackers need only set up the device outside the perimeter fences of your corporation to take advantage of the data coming off the mobile devices of hundreds of your employees. Other prime targets would be airports and big conferences where lots of businesspeople congregate. As it turns out, you are not the only one with an affinity for the data on your smart phone.

Hacking Mobile Payments

Of course, today's mobile phones are just at their earliest stages of development, and many new sensors, such as radio-frequency identification (RFID) and near-field communication (NFC), will bring new capabilities to mobile phones, as well as new vulnerabilities. One area in which this will be most clearly seen is in the disappearance of physical currency. The future of money is mobile and virtual, and a bevy of new sensors and apps are on track to replace your wallet and the cash in your pocket. In fact, some mobile phone providers, such as Safaricom in Africa, dominate the overall payment space. In Kenya, for example, 25 percent of the nation's GNP is actually transacted on Safaricom's M-PESA payment system. Mobile money payment systems, which did not even exist at the turn of the last century, are now available in over seventy countries and are used to move billions of dollars every month. In particular, they have been incredibly useful in getting previously "unbanked" populations in the developing world access to the global world of commerce with significant positive impact for local economies. In the developed world, there has also been a rush to adopt and

deploy mobile phone payment systems. MasterCard and Visa have implemented numerous NFC payment programs that allow users to launch an app on their phones and wave or tap the device on a contactless sensor to quickly charge goods and services. From Starbucks, to Best Buy, to parking meters in San Francisco and cabs in New York City, "wave and pay" is increasingly the choice of users for quick checkout and payment. Though Google was an early adopter of NFC payment systems for its Android phones, in September 2014 Apple joined the bandwagon and added swipe-and-pay technology to its latest batch of iPhones. Within the Android ecosystem, Google's Wallet payment system allows users to store their debit and credit card information with Google and launch the Google Wallet app to check out in an increasing number of stores via any PayPass-enabled store checkout terminal. Google Wallet works with the NFC chips on a wide variety of mobile phones from HTC, LG, Motorola, and Samsung.

The money as represented on these mobile devices is nothing more than data—data that are stored in vulnerable applications, controlled by deeply vulnerable mobile operating systems, using insecure sensor technologies and sensor data-transfer protocols. The obvious result? The future of mobile money may also be the future of mobile pick pocketing. The Google Wallet system has already been subverted by criminals on numerous occasions, and apps such as Wallet Cracker allow anybody to see a user's personal identification code (PIN) number for the system on demand. Moreover, if and when a user loses his or her Android phone, any pre-stored money in the user's Google Wallet (data on the device) can readily be spent in a store by the person who happens to steal or find the device. With the rise of NFC applications, and Apple's notable entrée into mobile payments, we will undoubtedly see growing hacker attention targeting these and other sensors embedded in mobile devices, including GPS.

Your Location Becomes the Scene of the Crime

Advertisers and data brokers are not the only people interested in persistently tracking your location. Criminals, fraudsters, and

stalkers have also found good use for the GPS chip on your smart phone. Often hackers can merely piggyback on the good work already done by data brokers as a means of subverting the data you are already leaking. Take, for example, the location-based dating application Tinder, which we discussed in chapter 4. Given the volumes of data, salacious photographs, and potential sex partners, it was not surprising that hackers worked to discover a security vulnerability in the app that allowed anybody to uncover the real-time location of any other users within five feet, information that was designed to be kept private. The best-case scenario with this locational data is that they lead to a positive dating experience. The worst-case scenario is that they and locational data generated by rogue apps such as Girls Around Me could prove a tremendous tool for stalkers, rapists, and potential child abusers. In fact, in 2012 police in South Australia warned members of the public that pedophiles were using geo-tagging data embedded in photographs of children posted online to track down potential targets, putting the subjects of these photographs at risk.

Increasingly, mobile data are being used to ill effect in cases of relationship discord and domestic violence. In 2012, the U.S. Department of Justice revealed that there were 3.4 million victims of stalking annually among those hundreds of thousands who were tracked by spyware and GPS hacks. Welcome to the world of point-and-click surveillance. To be clear, using such spyware is considered an unlawful interception under federal law and is illegal, but the tools are widely available to even novice hackers—or exes—with no prior experience. One product, Mobile Spy, will turn any phone into a bugging device, allowing for ambient recording of the surroundings, even when not on a call. The company also makes an “iPad monitor” product, and all of its software includes a “stealth camera” mode that allows third parties to remotely activate and monitor your camera in real time and store any photographs or videos they choose to record from your device on a central server for later download. Another product, Mobistealth, was used in 2011 by the convicted murderer Simon Gittany, a jealous and abusive boyfriend, to monitor the mobile phone activity of his fiancée, Lisa Harnum, in Sydney, Australia. Thus when Harnum sent an

SMS message to her girlfriend confiding that she planned on leaving her abusive relationship, Gittany was immediately notified via Mobistealth of her intent on his own mobile phone. Furious with her plan to leave him, Gittany drove to her home and, in the altercation that ensued, threw her off the fifteenth-floor balcony of her apartment.

But in some cases, domestic abusers did not even need to add third-party spyware to a phone: they just activated the AT&T FamilyMap program offered as a service by the wireless carrier, which allows a cell-phone account holder to track all the devices on his plan. Using his wireless carrier's family mapping service, Andre Letevec of Scottsdale, Arizona, was able to locate his estranged wife and their two children, whom he murdered. Today it's no longer even necessary to pay for such a service from carriers like AT&T; the features are already built in to both iOS and Android devices, services with names such as Find My Friends and Find My Phone, which can be turned on to remotely track others. To help combat these threats, domestic violence shelters have learned the moment a new client arrives at their facilities to take away her mobile phone, remove the battery, and disassemble it to avoid acting as a beacon to potential stalkers and violent individuals. It's not just victims of domestic violence who need to worry about inadvertently sharing their locations; even soldiers on the battlefield have cause for concern as terrorists monitor their online activities for potential avenues of attack.

"Is a badge on Foursquare or a check-in worth your life?" That question, now commonly asked by the U.S. Army of its soldiers, is not rhetorical when even terrorists are taking advantage of geo-tagged data. For instance, when American military forces received a new fleet of AH-64 Apache helicopters at their base in Iraq, some deployed soldiers uploaded photographs of themselves in front of their new choppers to Facebook. Unbeknownst to them, their phones had accidentally embedded their GPS coordinates in the photographs. Not only were insurgents monitoring the soldiers' Facebook postings, but they were also downloading the photographs and analyzing them for useful intelligence. The longitude and latitude information embedded in the photos allowed the ter-

rorists to launch a series of precise mortar attacks that directly targeted and destroyed four of the newly arrived Apaches on the compound.

Not only can we be tracked via the data we are leaking from our mobile phones and embedded files, such as photographs and videos, but increasingly we are leaking our locational data in the physical world. GPS bugging devices are cheap to buy online and are even available for sale in the ubiquitous *SkyMall* magazine available on every flight we take. In that catalog, Tracking Key sells a GPS hardware bug that attaches via magnet or Velcro to any car and allows owners of the device to replay on an online map everywhere the targeted vehicle drove, including speed of the vehicle, determined at one-second intervals. "Useful to see whether your teenager was speeding, where your spouse is going or where your employees are driving." Previously, such high-tech gear would only have resided in a spy agency or with the FBI, but now, given the exponential drop in pricing of these technologies, even a neighborhood mom can spy on her kids or potentially cheating spouse.

In the world of big data, we can even leak our physical location without a bugged mobile phone or GPS tracker hidden in our car. A new technology, known as an automatic license plate reader (ALPR), allows both governments and individuals to use video cameras and optical character recognition to record the locations of cars as they pass from one camera point to another, revealing the real-time movement of any vehicle throughout a city or country with great detail. From Minnesota to New Jersey, and from Ankara to Sydney, hundreds of millions of individual license plate records have been stored. As a result, a query can be applied against these massive databases to determine the position of any vehicle over time. Interestingly, those being photographed are not charged with or suspected of any crime in the overwhelming majority of cases, but these data are being stored nonetheless, because they might be useful for a criminal investigation at some point in the future.

ALPR units are also being mounted on police cars and even tow trucks, vastly expanding these databases. Private companies

such as Digital Recognition Network of Texas and MVTRAC of Illinois are also building massive databases of ALPR data, which they sell to agents in the vehicle repossession business. This way, if somebody falls behind on his payments, these companies know all the locations the vehicle has been and can send out a tow truck to repossess it. Just as Google Street View cars are driving up and down our city streets recording video of all they see, so too are private ALPR companies. They want to track your car and place its location in front of your home, at your workplace, and at all the places you shop. These data too of course will be monetized, and the practice in 2014 is entirely legal. But as these massive databases of ALPR mushroom, so will the criminal and privacy risks.

If Experian and Acxiom can suffer data breaches or sell their data sets to criminal organizations, why would ALPR vendors be any different? As a result, even victims of domestic violence who had no online presence and did not even carry mobile phones could still be tracked by where they drove in their cars. We've seen abuse of ALPR data in the past, way back in 1998, when a Washington, D.C., police lieutenant used his computer system to identify the owners of vehicles parked in the parking lot of a popular gay bar in town. He then used the data to extort the men, threatening to out them, unless they paid him a bribe. While the nature of the threats to ALPR data may be different today, they no doubt exist. How might this information be used in divorce cases (his car was parked at the home of the other woman) or by health insurers (we see his car parked at the bar five days a week)? There are other risks as well: ALPR systems are not flawless in their reading of license plate data, and errors can lead to grave consequences. In 2009, a forty-seven-year-old woman was pulled over in San Francisco by multiple police cars at gunpoint with six police officers pointing weapons at her—all because the ALPR system misread a single digit on her license plate, flagging her car as stolen, when in fact the woman was just out to buy groceries.

Even retailers have begun to pilfer our locational details in new and unexpected ways. The Nordstrom department store, for example, recently began tracking its customers via their Wi-Fi signals and MAC addresses on their smart phones when shopping

in its stores. As you walked through the stores, Nordstrom could digitally follow you to see how much time you were spending in ladies' underwear versus men's shoes. The high-end retailer contracted with Euclid, a company specializing in helping retailers track customer movements via in-store Wi-Fi connections. To date, Euclid has fingerprinted and tracked more than fifty million mobile devices in the four thousand locations using its service, including hundreds of national retailers such as Home Depot; yes, the same company that leaked fifty-six million credit cards because of a data breach in September 2014 wants to collect even more data on you and your location within its stores. Absent any regulation of the phenomenon, shopping under surveillance will undoubtedly become the new norm, and technology is increasingly turning to tracking people off-line in real space.

At Nordstrom, the only notification customers were given about its use of the new tracking technology was a small, well-hidden sign, barely visible at the entrance to stores. The verbiage on the sign made it clear that this was an opt-out model only, meaning that if you did not want to participate, you had only two choices: don't come in the store, or turn off your cell phone. Data obtained from services such as these can and will be stored in perpetuity. As a result, your spouse's divorce attorney will be able to subpoena Nordstrom and Euclid to see if you and your mistress were in the same store together buying intimates. Your boss will be able to contract with a data broker to find out your location that day you called in sick: "If you were sick, why were you (and your cell phone) at the movie theater and Hooters that afternoon?" Worse, criminals will gain access to all this information over time via the digital underground and use it to blackmail, bribe, and stalk targets of their choosing.

Even Disneyland, the "Happiest Place on Earth," is turning to location-based technologies to track its guests using bracelets called MagicBands, RFID-chip-enabled devices that allow Disney to track its guests throughout its parks. Its goal is to use big data to maximize your stay (and spending) in the Magic Kingdom. As goes Disney, others are likely to follow, and you can expect such human-tracking technologies to be deployed at casinos, resorts, and even airports in the future.

Cloudy Weather Ahead

Though massive amounts of data are leaking from our mobile devices, an increasing number of big-data risks come from the world of "cloud computing." The cloud refers to the massive network of computing resources available online and the practice of using these remote servers to store, manage, and process the world's information. The changing paradigm in computing means that less information is stored locally on our machines and is instead being hosted elsewhere on earth. We mostly do not buy software anymore; we just rent it or receive it for free using a new business model known as Software as a Service (SaaS).

On the personal front, cloud computing means Google is storing our mail, Instagram our photographs, and Dropbox our documents—not to mention what mobile phones are automatically uploading to the cloud for us. In the corporate world, enterprising customers not only are using Dropbox but also have outsourced primary business functions that would have previously been handled inside the company to SaaS providers such as Salesforce.com, Zoho.com, and Box.com. From a crime and security perspective, the aggregation of all these data, exabytes and exabytes of it, means that our most personal of information is no longer likely stored solely on our local hard drives but now aggregated on computer servers around the world. By aggregating everybody's important data, financial and otherwise, on cloud-based computer servers, we've obviated the need for criminals to target everybody's hard drive individually and instead put all the jewels in a single place for criminals and hackers to target—think Willie Sutton and his love of banks.

The cloud is here to stay, and at this point there is no going back. In early 2014, Google decreased the pricing of its cloud storage offerings by nearly 70 percent, to just \$0.026 per gigabyte per month (just under three cents versus the \$437,000 it cost in 1980). The move sent shock waves through the industry, and a price war ensued with the cloud storage giants Amazon and Microsoft also joining the fray. The availability of such cheap computing resources and a growing array of SaaS offerings will have untold positive impact on personal productivity, entrepreneurship, and innovation, which in turn will only hasten the inevitable transition

to cloud computing. But with this move to store all available data in the cloud come additional risks. Think of the largest hacks to date—Target, Heartland Payment Systems, TJX, and Sony PlayStation Network. All of these thefts of hundreds of millions of accounts were made possible because the data were stored in the same virtual location. The cloud is equally convenient for individuals, businesses, and criminals. To deal with these risks, organizations such as the nonprofit Cloud Security Alliance have been formed to promote best practices and improve security in the age of cloud computing.

The virtualization and storage of all of these data are highly complex and raise a wide array of security, public policy, and legal issues. First, where exactly is this magical cloud storing my data? Most users have no idea when they check their status on Facebook or upload a photograph to Pinterest where in the real world this information is actually being stored. That we do not even stop to pose the question is a testament to the great convenience, and opacity, of the system. Yet from a corporate governance and personal risk perspective, whether your data are stored on a computer server in America, Russia, China, or Iceland makes a difference.

The corporate and individual perimeters that used to protect our information internally are disappearing, and the beginning and end of our computer networks are becoming far less well defined. It's making it much harder to see what data are coming and going from a company, and the task is nearly impossible on the personal front. The transition to the cloud is a game changer for security because it completely redefines where data are stored, moved, and accessed, creating sweeping new opportunities for criminal hackers. Moreover, the nonlocal storage of our data raises important questions about our deep dependence on cloud-based information systems. When these services go down or become unavailable via DDoS attack, or you lose your Internet connection, your data become unavailable, and you are out of business.

As Mat Honan discovered, entrusting highly prized personal information, such as photographs of one's child and years of e-mail, to cloud service providers comes with particular risks. All the major cloud service providers have already been remotely targeted by criminal attacks, including Dropbox, Google, and Microsoft,

and we can surely expect more in the future. Indeed, several years after Honan was attacked and published an entreaty to "kill the password" for its near-total inefficacy, thousands upon thousands of individuals and businesses continue to have their cloud-based accounts compromised and their data stolen, including a number of high-profile Hollywood actresses. In late 2014, hundreds of photographs—many of them of a deeply private nature and containing nudity—were stolen from celebrities such as Jennifer Lawrence and Kate Upton when hackers successfully subverted the user names, passwords, and security questions protecting their Apple iCloud accounts. Although it may be your cloud service provider that is targeted in the attack, you're the victim, and the data taken are yours. Of course the rights reserved in the ToS mean that companies bear little or no liability for when data breaches occur. These attacks threaten intellectual property, customer data, and even sensitive government information.

In 2008, the top secret design specs for the president's Marine One helicopter were found freely available online, hosted on a peer-to-peer (P2P) network in Iran. These P2P networks allow for easy decentralized file sharing and are most often associated with the distribution of pirated films and music on the digital underground. How did the top secret plans and capabilities of one of the most technologically advanced helicopters in the world end up in the hands of the Iranians? Simple. A military contractor in Bethesda, Maryland, working on the Marine One project decided he wanted to listen to free music on his work laptop. When he downloaded the popular P2P sharing software, he accidentally and unknowingly installed the program in the wrong directory on his computer. As a result, the plans and defensive security features of the military helicopter that shuttles the president from the White House to Air Force One leaked to P2P music-sharing networks around the world, including those in Iran. For the want of free music, a billion-dollar military project was compromised, and the blueprints for the president's Sikorsky VH-3D helicopter ended up on a peer-to-peer network in Iran, hosted next to the pirated songs of both Michael Jackson and Shadmehr Aghili, the undisputed king of Persian pop. The former military contractor, interrogated by both the FBI and the Department of Defense, admitted his error, but by then the

damage had been one. Our global interconnections and never-ending storage of more and more data mean leaks are inevitable. What data might you or your company be leaking to the cloud?

Big Data, Big Brother

Interestingly, governments are not only victims of data leaks but the cause of many as well. Information is the driving force of all intelligence operations, and governments of all sizes are targeting big data with a vengeance. It is not only the Chinese who are hacking the world; so too are the Americans, Brits, Russians, Australians, Canadians, Syrians, Israelis, Egyptians, Iranians, and even Ethiopians. In fact, there are more than a hundred countries with active, offensive computer-hacking programs, though perhaps none quite as extensive as that of the U.S. government and the National Security Agency. Every single day, the NSA is reported to intercept and stockpile more than 1.7 billion e-mails, phone calls, and SMS messages, compiling a database of nearly 20 trillion data transactions just since 9/11. The agency catalogs who calls whom, who e-mails and texts whom, and who wires money to whom.

Given the exponential growth in its big-data holdings, however, the electronic espionage agency is running out of storage space. In response, the government is in the process of building a new massive operations facility deep in the Utah desert that will allow the NSA to cache and process 100,000 times more data than what is currently held by the Library of Congress. But that is just the beginning . . .

The revelations of Edward Snowden have documented the extensive number of data streams pursued by the NSA, including the ever-growing mounds of social and locational details we all generate. Though the complete list of Snowden's disclosures is too long to outline here, a review of the highlights released to date should make it clear that the private sector is not alone in its aggressive pursuit of big data. NSA's PRISM program allowed the government to collect copious volumes of data from companies such as Microsoft, Google, Facebook, Skype, AOL, and Apple, including users' e-mails, videos, photographs, status updates, and locations.

Snowden also revealed that the NSA accessed and downloaded the interpersonal connections of social media users (whom they spoke to, how often, and where they were located), including the social data graphs of U.S. citizens. These network graphs were supplemented by millions of online user contact lists and address books that the agency had also collected. You see, when you choose to use Google Contacts or iCloud to store the personal details of your friends, family members, and business associates, they can be readily targeted and taken by others, including governments.

Not only did the NSA have cooperative relationships with American firms, but it also targeted them when convenient, including Google and Yahoo!, whose data centers the spy agency infiltrated without authorization. Using the same basic techniques employed by hackers and organized crime groups, the NSA infected more than fifty thousand computer networks around the world with malicious software in order to get access to targets of interest. The agency even posed as Facebook in numerous "man in the middle" attacks to pursue individuals across their social networks. The technique caused targets of interest to connect through a replica Facebook site controlled by the government, allowing the agency to install malware on the machines of its marks.

The NSA did not do all this work by itself, but rather cooperated with sister organizations such as Britain's NSA equivalent, the Government Communications Headquarters. Together, the agencies participated in the program Optic Nerve, which intercepted millions of Yahoo! video chats by commandeering the video cameras on users' laptops and snapping photographs every five minutes. Millions of images were stored, including a large number of sexually explicit pictures containing nudity. Shockingly, many of the video chats intercepted were of individuals not specifically targeted for any particular intelligence operation but because it was easier to grab all the chats than to decide on an individual basis which ones should be seized.

The NSA also replicated the already proven techniques of advertisers and marketers and their commercial data-gathering operations. For example, the spy agency created and installed tracking cookies on hard drives and mobile phones to record the locations and online habits of those under surveillance. Accord-

ing to Snowden, the NSA was even tapping smart-phone apps, such as Rovio's *Angry Birds*. The spy agency recognized that *Angry Birds* was already doing such an excellent job of pilfering data that the NSA needn't bother duplicating its efforts. Instead, the NSA merely intercepted the colossal sums of data already forwarded to Rovio by those who naively thought the app's only true purpose was to sling birds at chortling green pigs for amusement.

Only a tiny percentage of the 1.7 billion *Angry Birds* users understood that their "free" app was sharing data ranging from their persistent location to their sexual orientation with Rovio. None—including the app company itself—however, realized that they were now also providing these data (unwittingly of course) to the NSA. Individual NSA analysts were even using the agency's vast spying tools to target their boyfriends, girlfriends, spouses, and ex-lovers. Numerous violations were documented wherein NSA officers entered the e-mail addresses and phone numbers in order to read their e-mails, track their locations, and listen to their phone calls. The actions of these individual employees raise the proverbial but important question of who watches the watchers?

While the overwhelming majority of the NSA's targets appear to be overseas, dozens of security services around the world use electronic espionage to surveil and repress their domestic populations. In China, Iran, Egypt, Syria, Bahrain, and elsewhere, data stored online are routinely monitored and intercepted for reasons of political intelligence and to ensure the status quo. Most countries do not build these surveillance systems, but rather buy them from companies based in other nations, such as Germany's Gamma International, maker of the FinFisher electronic surveillance suite. FinFisher allows domestic intelligence services to monitor thousands of targets simultaneously across their mobile phones, social media networks, and online activities.

Once these systems of mass data surveillance have been established, they can be used for the common good, such as disrupting an imminent terrorist attack, or to the common detriment, such as repressing and harassing human rights activists and subverting the democratic process. While social media did much to empower dissidents in Egypt and Tunisia during the Arab Spring, a story that received tremendous press worldwide, there was a flip side to

the social data coin. The millions of tweets and Facebook postings also provided very useful tools for governments to go after critics. Organizing a protest on Facebook gives the government clear access to what opposition activists are planning, and nearly all governments have the skill set to take advantage of such leaking data.

In the uprising against Bashar al-Assad that began in 2011, the Syrian government, with technical support and assistance from Iran, developed a wide variety of programs to monitor social media sites such as Facebook and Twitter to track communications among opposition figures. Leaders of the anti-Assad movement identified online have been targeted for attack, as have members of their families. In the waning days of the former Ukrainian president Viktor Yanukovich, his government forces demonstrated the power of technology to repress and intimidate opposition forces. As demonstrators gathered on the streets of Kiev, the Ukrainian government detected the locations of all mobile phones in proximity to street clashes between riot police officers and protesters. The mobile phones (and their owners) were identified in real time and received what may be the "most Orwellian text message a government has ever sent: 'Dear subscriber, you are registered as a participant in a mass disturbance.'" The language was carefully chosen as Yanukovich had made such participation illegal days earlier and anyone found in violation was subject to immediate arrest.

The Darker Side of Big Data

The emerging legacy of big data may well be one of persistent surveillance, the abolition of privacy, and a rash of criminal threats never previously envisioned. Social media, smart phones, mobile apps, the cloud, and a host of other technologies mean that not only can Nordstrom, Acxiom, Facebook, and Google find you at will, but so too can the Zetas, Lashkar-e-Taiba, domestic abusers, and stalkers. What most people do not understand, however, is that any data collected will invariably leak. Our current computing systems are too insecure to safely store the volumes of information we are generating.

To date, the major threat to big data has been their theft and

leakage. But that was only the beginning. As we move forward, we will encounter dangers that may prove to be even more perilous—unauthorized alteration of the information upon which the world depends to run its daily activities. Although we have placed tremendous trust in the data we are feverishly hoarding away, the underlying accuracy of this information, as we will discover, can easily be subverted, with significant consequences for all. For just as bad actors can steal our data, so too can they change it. This gathering storm will leave us vulnerable and shake the foundations of our faith in a data-dependent world in ways not yet fully appreciated.