BREACHED!

WHY DATA SECURITY LAW FAILS AND HOW TO IMPROVE IT

DANIEL J. SOLOVE AND WOODROW HARTZOG

A novel account of how the law contributes to the insecurity of our data and a bold way to rethink it.

Digital connections permeate our lives—and so do data breaches. It is alarming how difficult it is to create rules for securing our personal information. Despite the passage of many data security laws, data breaches are increasing at a record pace. In *Breached!*, Daniel Solove and Woodrow Hartzog, two of the world's leading experts on privacy and data security, argue that the law fails because, ironically, it focuses too much on the breach itself.

Drawing insights from many fascinating stories about data breaches, Solove and Hartzog show how major breaches could have been prevented or mitigated through a different approach to data security rules. Current law is counterproductive. It pummels organizations that have suffered a breach but doesn't address the many other actors that contribute to the problem: software companies that create vulnerable software, device companies that make insecure devices, government policymakers who write regulations that increase security risks, organizations that train people to engage in risky behaviors, and more.

Although humans are the weakest link for data security, policies and technologies are often designed with a poor understanding of human behavior. *Breached!* corrects this course by focusing on the human side of security. Drawing from public health theory and a nuanced understanding of risk, Solove and Hartzog set out a holistic vision for data security law-one that holds all actors accountable, understands security broadly and in relationship to privacy, looks to prevention and mitigation rather than reaction, and works by accepting human limitations rather than being in denial of them. The book closes with a roadmap for how we can reboot law and policy surrounding data security.

Buy *Breached!* on Amazon

Praise for *Breached!*

"An exceptionally insightful and accessible overview of key data security challenges and the law's dysfunctional attempts to deal with them."

– **Edward McNicholas**, Global Cybersecurity Practice Co-Leader, Ropes & Gray

"A readable and smart account of how policymakers keep focusing on the wrong details at the expense of the bigger picture. *Breached!* is a book for anyone who is interested in why data breaches keep happening and what the law should do about it."

– **Bruce Schneier**, author of *Click Here to Kill Everybody*

"*Breached!* shows how the future of data security requires us to look at the problem holistically and understand that good privacy rules can also promote good security outcomes. A breath of fresh air on an important and often-ignored topic."

– **Neil Richards**, Professor of Law, Washington University

"A fascinating exploration of the ways that our fixation on individual data breaches has limited the effectiveness of data security law."

– **Josephine Wolff,** Associate Professor of Cybersecurity Policy, Tufts University

"[A] foundational contribution to data security law. With deep insight, compelling storytelling, and even humor (and some needed fright), the scholars show that lawmakers must better understand that beneath the high-tech wizardry and data security do's and don'ts are normal, fallible people. This book is a must read for everyone concerned about the security of our personal data."

-- **Danielle Keats Citron**, Distinguished Professor, University of Virginia School of Law

"A compelling account of where data security law has gone wrong plus convincing advocacy of where it should go. This book should be read by anyone involved in privacy and cybersecurity."

– **Paul Schwartz**, Jefferson E. Peyser Professor of Law, Berkeley Law School

"A clear, accessible, persuasive case that data security today needs a systematic approach, far beyond just mopping up breaches. I hope every regulator or legislator working on the subject reads this book and follows their advice."

– **William McGeveran**, Associate Dean for Academic Affairs, U. Minnesota Law School

Buy *Breached!* on Amazon

Breached!

Why Data Security Law Fails and How to Improve It

DANIEL J. SOLOVE

& WOODROW HARTZOG

OXFORD
UNIVERSITY PRESS

OXFORD
UNIVERSITY PRESS

Oxford University Press is a department of the University of Oxford. It furthers the University's objective of excellence in research, scholarship, and education by publishing worldwide. Oxford is a registered trade mark of Oxford University Press in the UK and certain other countries.

Published in the United States of America by Oxford University Press
198 Madison Avenue, New York, NY 10016, United States of America.

CIP data is on file at the Library of Congress
ISBN 978–0–19–094055–3

9 8 7 6 5 4 3 2 1

Printed by LSC communications, United States of America

TABLE OF CONTENTS

7

Unifying Privacy and Data Security

In April 2015, representatives from CyTech Services, a small forensics analysis company, met with officials at the U.S. Office of Personnel Management (OPM). The CyTech employees were at OPM to demonstrate their new tool, which would perform a diagnostic scan on OPM's servers.

OPM maintains personnel records of millions of federal employees and applicants to federal jobs. Because these jobs include sensitive positions, including FBI officers and others, applicants must undergo background checks. These background checks can be very intrusive, involving questions about financial troubles, drug and alcohol use, any criminal wrongdoing, psychological information, and much more. OPM maintained records of these background checks—nearly 21.5 million records involving current federal employees and retirees. CyTech Services initiated the diagnostic scan. Everyone expected the scan to be clean.[1] Nobody was prepared for what happened next.

The scan identified odd unknown processes occurring on the server.[2] Everyone in the room was stunned. Their jaws dropped. Something was very wrong.

The House Oversight and Government Reform Committee began a massive investigation, resulting in thousands of pages of documents and transcribed interviews. After nearly a year, the Committee's investigation revealed that CyTech's demonstration wasn't the first time that OPM had learned about the intrusion.[3] In fact, OPM had discovered a breach in March 2014, more than a year earlier. Later in 2014, two breaches occurred at KeyPoint Government Solutions, a company that provided services to OPM and that had access to OPM's data. OPM failed to terminate KeyPoint's access, even though KeyPoint's credentials were used to access OPM's network.

One of the hacked OPM databases, the Central Personnel Data File, contained personnel records of current and former federal employees. The database included their Social Security Numbers, job positions, and performance evaluations.

Another hacked OPM database, the Electronic Questionnaires for Investigations Processing (e-QIP) system, contained security clearance and background check information. This data included information on 1.8 million spouses, children, and family members of security clearance applicants.[4]

OPM also maintained fingerprint data, which dated back to 2000. Initially, OPM reported that only 1.1 million fingerprint records were compromised, but it later updated the figure to 5.6 million. OPM stated that "Federal experts believe that, as of now, the ability to misuse fingerprint data is limited."[5] This statement, however, strains credulity. Many experts criticized OPM for downplaying concerns about the compromised fingerprints. One expert declared that undercover agents could be "completely compromised," noting that "a secret agent's name might be different. But they'll know who you are because your fingerprint is there. You'll be outed immediately."[6]

As far back as 2007, OPM's Inspector General Office (OIG) was delivering semi-regular audit reports to Congress criticizing OPM's security

practices as a "material weakness"—the lowest possible assessment on its scale.[7] Later reports noted that "[t]he continuing weakness in OPM information security program results directly from inadequate governance. Most if not all of the [information security] exceptions we noted this year result from a lack of leadership, policy, and guidance." A 2014 information security audit also noted OPM's poor security, faulting OPM for failing to implement multi-factor authentication, which had been recommended much earlier and would have likely prevented the breach.[8] Time and again, the warnings had been made that OPM's security was poor, but nobody did anything about it.[9]

The OPM breach was not only the product of bad security practices but also of poor privacy practices. Nuala O'Connor, former head of the U.S. Department of Homeland Security's privacy office, noted that "OPM didn't have the most basic data map or a simple inventory list of its servers and databases, nor did it have an accounting of all the systems connecting to its network."[10] This is a data privacy flaw. A key dimension of protecting data is maintaining a data inventory to keep track of the data being stored and who is responsible for it.

Moreover, OPM was storing all this data in a centralized location, making it easy for the hackers to obtain a lot of data.[11] Keeping massive stores of personal information is also a privacy no-no. Even worse, OPM retained the data seemingly forever; it had data going back decades, including information about people's families. Why did it need to keep all this data and why keep it for so long?

Had OPM collected and stored less data and regularly deleted some of it, the breach wouldn't have been as damaging. Moreover, had OPM segmented the data or better restricted access to it, the hackers would have had a harder time hauling it all away. Had OPM assigned a data steward for the data, someone who would be accountable for it and who would make sure it was properly being cared for, the breach might never have occurred.

OPM maintained background check information to protect security—to prevent government personnel from being compromised and betraying the United States by giving up secrets, helping foreign governments break

into computer systems, or other things. Ironically, the hacked data not only violated people's privacy but it created a grave security threat—and it continues to pose such a threat to this day. Several security experts have warned that the information in security clearance and background checks could be used to blackmail government employees in sensitive positions.[12] A former assistant director of the FBI's Criminal, Cyber, Response and Services Branch told *The Washington Post* that the OPM breach provided hackers with "very detailed information about people who hold very sensitive clearances."[13] Hackers could use this information to conduct spear phishing, targeted attempts to glean personal information to "gain access to sensitive computer accounts and even potentially conduct a physical attack or attempt extortion."[14]

The story of the OPM breach certainly reveals a stunning display of bad security practices. The story also demonstrates how poor privacy practices made the breach more possible and much worse than it should have been. In this chapter, we address the relationship between privacy and security. Good data security is almost impossible without a robust commitment to privacy values. Privacy is a key and underappreciated aspect of data security. Lawmakers and industry should break down the regulatory and organizational silos that keep them apart and strengthen our privacy rules as one way to enhance data security and mitigate breaches.

UNDERSTANDING CYBERSECURITY, DATA SECURITY, AND DATA PRIVACY

At the outset of our discussion, it is essential to understand the general scope of the domains of cybersecurity, data security, and privacy. *Cybersecurity* is generally used to broadly refer to the security of all forms of information and technical infrastructures, such as intellectual property, critical infrastructure data, trade secrets, personal data, and more.[15] *Data security* is a narrower domain that involves the security of personal data. As David Thaw observes, cybersecurity as a whole can have different goals than protecting personal data.[16] He elaborates, "The security techniques

and goals for protection of strategic weapon control systems are different than the techniques and goals for an average consumer, for example, protecting their personal computer used primarily for entertainment purposes."[17]

Privacy involves, among other things, a wide array of protections of personal data. Because privacy is an important aspect of personal data, it is closer to data security, but still not entirely the same. In some formulations, privacy is a broader domain that encompasses data security, which is a subset of the protections given to personal data. It is this formulation that we prefer, as we see data privacy as a pie with many essential pieces, one of which is data security.

In many ways, the EU's terminology is better. The EU uses the term *data protection* to encompass both data privacy and data security. The EU is exactly right—data privacy and data security are both, essentially, about protecting data. The EU doesn't see privacy and security as separate domains, at least not in the same way that the United States does.

Although privacy and data security are related and intertwined, they aren't identical. As law professor Derek Bambauer observes, "Privacy establishes a normative framework for deciding who should legitimately have the capability to access and alter information. Security implements those choices."[18] Jeff Kosseff notes that security "promotes the confidentiality, integrity, and availability of public and private information, systems, and networks." Security "must address more than just the confidentiality of personal information, and also seek to protect from unauthorized alteration of data and attacks such as ransomware that cause data or systems to become unavailable."[19]

We caution against clean and rigid distinctions between privacy and data security, at least in law and policy. Much of data security involves duties and administrative policies and procedures that are similar to those for privacy. Moreover, as we argued earlier, data security is more of an art than a science, and it involves difficult policy tradeoffs just like privacy does. Although privacy and security are distinct in many ways, they have quite a lot in common. Viewing data security policy primarily as a collection of requirements for breach notifications and technical controls

excludes many of the most important issues from security, and it silos privacy and security in ways that are unproductive.

THE SCHISM BETWEEN PRIVACY AND SECURITY

A major schism exists between privacy and security. This schism arose in part because data security gets lumped with cybersecurity, and much of security these days is the province of the Information Technology department.

Different Silos and Different Languages

Organizations often place privacy functions in Compliance or Legal while data security is commonly in Information Technology (IT).[20] When companies organize their departments in this way, privacy and security professionals interact less and have a lower ability to change each other's practices, habits, and fluencies. Not only do privacy and security teams infrequently speak to each other, they often speak in different languages. It's like the Tower of Babel.

Law professor Ari Waldman noticed two important issues that came up in his extensive interviews with technologists and lawyers working on privacy and security within organizations.[21] First, some corporations conflate privacy and security (and then focus only on security). Others bracket off the presumably non-security aspects of "privacy" into compliance departments with workers whose expertise is in paper trails, not privacy. Privacy is then given a meager budget, while IT departments get tasked with "security" and budgets that allow them to do their work. Then, Waldman notes, comes the magician's misdirection. Having empowered IT departments to fix security flaws, corporations then report that they are protecting their customers' privacy when, in fact, they have done quite little.[22]

Based on his interviews with technologists, Waldman observes that many technologists believe privacy merely involves providing users with

notice about the company's privacy practices. Others think privacy is synonymous with encryption, which in this context is driven more by a desire to secure company data than to safeguard against consumer privacy risks. As Waldman also notes, "Few engineers remembered meeting with lawyers or privacy professionals one-on-one to discuss integrating privacy considerations into their work. Many found it difficult to design with user needs in mind; therefore, engineer-only design teams not only minimized the importance of privacy, but also missed how their designs impacted consumers."[23] This kind of organizational schism has led to a mentality around privacy and data security that ends up limiting the effectiveness of both domains.

One of the problems with separating data security and privacy is that people working in these areas cannot learn from each other. This means they often repeat the same mistakes or miss out on different ways of thinking about problems. People can get a little myopic, thinking that their little patch of responsibilities is the cosmos. This kind of narrow thinking also leads to a breakdown in cooperation where privacy interventions could help improve data security and vice versa.

Waldman's interviews with technologists reveal that the companies they work for often do very little to prioritize privacy by design. As Waldman observes, "Privacy professionals or other personnel trained in privacy rarely met with engineers and programmers, even during weeks of intense design work." Even at companies that had "privacy teams that were supposed to 'insinuate' themselves into design, high turnover, a laissez-faire attitude, and corporate silos kept privacy mostly orthogonal to design."[24]

Further, Waldman's work reveals that privacy is often deprioritized while other values take precedence. The mandate often comes from the top, where executives want engineers to prioritize "speed, agility, [and] functionality.'"[25] Waldman noted that "[i]nterviewees used words and phrases like 'hands off,' 'absent,' 'uninvolved,' and 'not really a factor,' to describe their employers' approach to privacy. Privacy is akin to security's distant cousin, whom everyone forgets to invite to the party. Even when privacy is at the party, it is relegated to the small children's table off to the side.

Beyond a lack of privacy protection, the schism between privacy and data security has resulted in organizations viewing data security mainly as an IT issue. Certainly, many components of good data security involve IT, such as encryption, firewalls, access controls, and more. But many more security issues involve a human dimension. Many security decisions involve human behavior, such as how to deal with cognitive limitations, carelessness, cheating, denial, ignorance, gullibility, and misconduct—security's seven deadly sins. Security decisions also involve policy, such as managing the tradeoff between security on the one side, and ease, convenience, and ready accessibility on the other.

We have heard people call the security side "hard" or "left-brained" and the privacy side "soft" or "right-brained." IT technologists are often not well-trained in addressing complex issues involving people and values; they are more often trained mostly in "hard" technological problems and solutions. They know how computer systems and code operate, but often they aren't sufficiently trained about how to respond to human behavior or how to think through challenging policy choices. Privacy professionals, in contrast, receive a heavier dose of training about so-called soft issues such as human behavior, values, law, and policy. We aren't fond of the terms "hard" and "soft" or "left-brained" or "right-brained," but we agree that there is certainly a distinction between the kinds of training IT and privacy professionals receive. The key difference is that privacy draws more from the humanities and data security is more steeped in engineering. For effective data security, however, both types of thinking are essential.

Privacy is (or at least should be) about much more than just effectuating peoples' personal preferences about who should have their data. Privacy is about trust, power, dignity, and the collective autonomy to set the preconditions of human flourishing.[26] In a broader sense, privacy is about all the rules that govern our personal information.[27] Data security policy similarly cannot escape a web of value-laden decisions, because it, too, requires tradeoffs guided by ethics and normative considerations.

A Schism in the Law

The schism between security and privacy also exists in the law, especially in U.S. law. Broadly speaking, the law began with a more unified view of privacy and security, but after the ChoicePoint breach, data security law spun off into a more separate domain.

In the early laws of the 1970s through 2000, data security evolved alongside and within privacy laws and frameworks. Data security is one of the original Fair Information Practice Principles (FIPPs), which were the principles proposed to address concerns with the rise of computer databases of personal information.[28] The FIPPs arose in a 1973 report by the U.S. Department of Health, Education, and Welfare (HEW) called *Records, Computers and the Rights of Citizens*.[29] The HEW report was prompted by concerns about the computerization of records, and the committee that drafted the report was charged with recommending legal and policy responses. The primary recommendation of the report was to enact a code of fair information practices to regulate all repositories of personal data. Data security was one of the main recommendations in the report: "Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data."[30]

The FIPPs have become the backbone of privacy laws around the world. In 1980, the OECD Privacy Guidelines included the "Security Safeguards Principle," which stated that "Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data."[31] The OECD Privacy Guidelines have formed the blueprint for the EU's privacy laws, starting with various member nation's laws, then the EU Data Protection Directive, and today's General Data Protection Regulation (GDPR). Laws in the United States and around the world include many of the FIPPs. There are now more than 200 countries with data privacy laws, and most of them are built upon the FIPPs specified by the OECD.[32] Many of these privacy laws include protections for data security.

Starting in the early 2000s, a separate and more distinctive body of law around data security developed, especially in the United States. Breach notification laws and safeguards laws started popping up everywhere, and these laws focused more exclusively on data security.

Although data security is often lumped in as part of privacy and data protection regimes, it is now treated as a distinct area centered around safeguards and notification. If organizations provide notification of breaches and properly implement safeguards, in the eyes of the law, they will be seen to have fulfilled their data security obligations. The law often has stronger penalties for data security violations than for privacy violations, so when data breaches are caused by privacy problems, such as in the Cambridge Analytica case (discussed below), companies want to frame them in terms of privacy rather than security and avoid giving them the dreaded moniker of "data breach."

The classic formulation of data security is to protect the confidentiality, integrity, and availability of data—a triad often referred to with the acronym CIA. It is important to note that the first element of this triad—confidentiality—is a key dimension of privacy. Data integrity also involves privacy, as many privacy laws protect a principle called "data quality," which involves the accuracy and completeness of data.

Privacy and data security have much in common. Over time they have become estranged relatives, but they should go hand-in-hand. Recent data security breaches indicate that it is time for them to be united again.

THE FRONT DOOR AND THE BACK DOOR

Everyone is so obsessed with preventing a breach through the back door that they neglect to pay enough attention to the front door. The "back door" is a metaphor to describe the illicit break-ins by hackers or other intruders. We clearly know that they don't belong in the computer network. The "front door" describes the many people who are invited into the network or who already have access to the network.

Security focuses mostly on the back door, on keeping the bad guys from intruding. Privacy focuses mostly on the front door. The people coming into the front door often don't appear to be bad guys, but they are also a security risk. Like a nosy visitor to one's home, front-door people might start snooping into things that they are not authorized to see.

Hackers know that sometimes the easiest way to break in is through the front door, so they pose as regular customers. Recall the ChoicePoint breach that we discussed earlier. In that breach, the hackers posed as a legitimate ChoicePoint customer. They didn't need to break in—ChoicePoint opened the door and let them in. No security alarm bells went off because the hackers weren't intruding; they were customers. The problem was one that is typically in the domain of privacy—decisions about who has access to data and how it is shared. ChoicePoint was too loose about who could be its customer; it too freely shared personal data without making sure it was doing so carefully.

At the end of the day, front-door breaches and back-door breaches are both breaches, but front-door breaches are often harder to guard against. Many front-door people differ from hackers because they don't think they are doing anything wrong, or they think what they are doing is only a minor transgression.

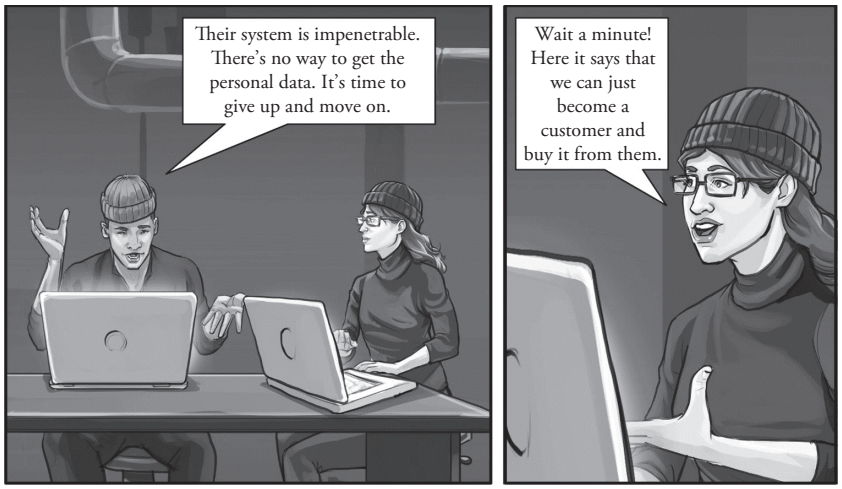

Figure 7.1

To address back-door and front-door breaches, security and privacy must work together. Guarding the back door is all for naught if the front door is left wide open.

The Moneyball "Hack"

Jeff Luhnow, Sig Mejdal, and Chris Correa were executives with the St. Louis Cardinals major league baseball team. Luhnow and Mejdal built a database called Redbird, which contained information and statistics about players. The database adopted the Moneyball approach to baseball, which is chronicled in the bestselling book of the same name by Michael Lewis. This approach involves analyzing enormous troves of data to make baseball decisions, as opposed to the good old-fashioned technique of going with one's gut. Essentially, Moneyball is baseball's version of Big Data.

Correa and Mejdal were rivals who worked under Luhnow. Later, Luhnow left the Cardinals to become the general manager for the Houston Astros, a team that was one of the main rivals to the Cardinals in the same NL Central division.[33] Luhnow hired Mejdal to join him in Houston and named him to be head of the analytics department. There, Luhnow and Mejdal launched a similar Moneyball-style program called Ground Control.

Back in St. Louis, Correa had become head of analytics. He sought to access the scouting data Luhnow and Mejdal were gathering in Ground Control for the Astros. Correa knew Mejdal's password to Redbird because Mejdal was required to turn over his laptop and password when he left the Cardinals, and Correa figured that perhaps Mejdal, like so many other people, might reuse the same password for his other accounts, including his account for Ground Control.[34]

In March 2013, Correa tried the old password, and it worked. Over the next two-and-a-half years, Correa accessed Ground Control numerous times. He viewed scouting reports, player health information, and other data.[35]

In January 2014, Correa lost access to Ground Control when there was a system-wide password reset. But a few months later, the Astros reset all Ground Control user passwords to a default password. Correa found the default password in Mejdal's email, and he was back in.

In June 2014, the Astros were last in their division, but *Sports Illustrated* ran a feature story called "Astro-Matic Baseball" filled with praise for Mejdal and Luhnow about their Moneyball approach. The cover of the issue had an Astros player swinging his bat with the title: "Your 2017 World Series Champs." Mejdal was also featured in another article in the issue.

Perhaps sparked by the fact that his rival Mejdal was being praised even though his team was currently dead last in the division, Correa again attempted to log back into Ground Control. Correa then allegedly leaked confidential notes about Astros' trade discussions.[36] The leaks created tensions between several baseball teams and their players, and the Astros ended up apologizing individually to other teams.

It was these leaks that would be Correa's undoing. The FBI began investigating, and everything came to light.[37] The FBI discovered that Ground Control had been infiltrated from a location occupied by executives from Cardinals. The Cardinals launched an internal investigation. The hacking was traced back to Correa, who had been promoted to scouting director.

Correa was fired by the Cardinals. He was criminally charged under a federal hacking statute, and he pled guilty. He was sentenced to prison for nearly four years and ordered to pay restitution of $279,038.65. The Major League Baseball Commissioner banned Correa permanently from baseball, a sanction imposed only on a few others such as Pete Rose and players from the 1919 scandal-ridden Chicago White Sox. The Cardinals were fined $2 million, and they had to forfeit their first two picks in the draft to the Houston Astros.

"Hacking" Is Often Just Snooping

There are some who object to the word "hacking" to describe what happened here. Hacking connotes high-tech wizardry, the stuff chronicled

in the movie *War Games* or regularly on TV where people can break into any network by typing for 10 seconds on a keyboard.

The methods used by Correa to access the Astros' system were not very sophisticated. Correa used some old passwords he knew from when Luhnow and others were working with the Cardinals. The passwords weren't changed when they went to the Astros. So, Correa wasn't a tech wiz, but he did know some of the ancient wisdom passed down through generations of computer fraudsters: *People often have poor password practices.* People select bad passwords, they put them on sticky notes near their computers, and they often never change them. Correa guessed correctly that Luhnow or the others didn't bother to change the password after they went from the Cardinals to the Astros.

Whether you call it "hacking" or not, the key thing for the law is that someone is accessing a computer in ways that are not authorized. This doesn't need to occur through any kind of technological acumen.

The federal Computer Fraud and Abuse Act (CFAA) imposes criminal penalties when a person "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer."[38] A protected computer is defined very broadly—essentially, it includes any computer connected to the Internet.

There are a variety of different types of crimes under the CFAA depending upon the circumstances, but the foundation of all of them is unauthorized access. And based on the facts reported, there was unauthorized access. Even though the password was readily guessable—and even though it appears the Cardinals already had the list of passwords in its possession—the ease of access doesn't matter. No matter how careless Luhnow might have been with security, accessing his computer without authorization is still a crime.

Many people have the misconception that computer crime is very sophisticated, but often it isn't. Hackers often break into a system through con artistry—by tricking people into giving them their password. If you read about the exploits of reformed hacker Kevin Mitnick, the inspiration for the movie *War Games*, many of his techniques seem closer to the movie *Dirty Rotten Scoundrels*.

We don't know for sure, but we are willing to bet that Correa didn't think of himself as a hacker. Hackers are often depicted in photos as teenagers in hoodies or criminals in ninja suits. In movies and TV, hackers are sophisticated techies who can break into the most secure systems with just a few keystrokes. In heist movies, they can instantly pull up the architectural plans to the building to be robbed. A few more keystrokes gets them into the power grid.

But in real life, a large component of hacking isn't high-tech. Correa didn't use technical wizardry to break into Ground Control. He just used a password he knew. He was a snooper. But under the law, he was a hacker.

In the analog world, people do a lot of snooping. A person in the bathroom at a friend's house might peek into the medicine cabinet. A spouse might peek at their partner's diary or private papers that are sitting out on the bed. People might put their ears against the door to listen in on a conversation in the next room. These forms of non-digital snooping are not punished very severely; many instances are not even punished at all by the law.

But when it comes to digital snooping, it's a different story. Snooping into email accounts or other online accounts will violate state and federal electronic surveillance statutes which penalize many intrusions as felonies with steep prison terms.

The CFAA rightly punishes front-door snooping such as Correa's. Other forms of snooping, such as when employees of an organization look into people's records out of curiosity rather than as part of their job, are dealt with by privacy laws such as HIPAA. It is still common for most people to associate the front door with privacy and the back door with security. Understanding that the front door is also essential to security is a necessary step toward more robust security.

POOR PRIVACY LEADS TO POOR DATA SECURITY

Poor privacy will undermine even the best data security. Good privacy practices involve having more than just the bare minimum of procedural

safeguards like getting consent or being transparent about data practices. To have good privacy practices an organization must severely curb its data appetite, collect only the data that is necessary and justified, delete data when it is no longer needed, and avoid data processing that threatens people's rights, exposes people to an undue risk of harm, or leads to socially detrimental effects.

Many organizations are looking for ways to try to hook everything up to the Internet, to collect more personal data, to use it in more ways, to gather it all together, and to keep it for longer, possibly forever. These are problematic privacy practices, and they are a recipe for a security Titanic. There are several ways that bad privacy can lead to bad security: (1) Weak privacy controls can lead to improper access through the front door; (2) Collecting and storing unnecessary data can make data breaches much worse; (3) Poor privacy regulation can allow for more tools and practices that compromise security; and (4) A lack of accountability over data can increase the likelihood that the data will be lost, misplaced, or misused.

Weak Privacy Leads to Front-Door Breaches

On the Sunday morning of March 18, 2018, *The Guardian* published a bombshell story: "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach."[39] The story showed how, through third-party apps on Facebook, data analytics company Cambridge Analytica extracted massive amounts of data from Facebook's users.[40] Cambridge Analytica worked for Donald Trump's election team and the Brexit campaign. Cambridge Analytica used the data that it plundered to create psychological profiles of voters, whom it then targeted and attempted to influence their voting in the 2016 Presidential election and the Brexit referendum.[41]

A big debate arose over whether Cambridge Analytica's access to the data was a data breach. People didn't even regularly use the term "data breach" until the 2000s, so it's relatively new and undefined, even though

it is legally significant.[42] Nicholas Thompson, editor-in-chief of *Wired* said of the incident:

> "Breach" is a word in the tech community that means they cracked the protections, right? You got over the moat and you got in through the door. . . . Facebook, a company of engineers, [is] really proud that hasn't happened at Facebook, so if you say data is breached, to Facebook it's like, "Oh my God, that's the most offensive thing you can say." To the rest of the world, it's like, "Of course this is a breach!" Right? "They got the data!"[43]

But Facebook Vice President Andrew Bosworth declared on Twitter: "This was unequivocally not a data breach. People chose to share their data with third-party apps and if those third-party apps did not follow the data agreements with us/users it is a violation. No systems were infiltrated, no passwords or information were stolen or hacked."[44] Then in a series of later-deleted Tweets, Facebook Chief Security Officer Alex Stamos said, "The recent Cambridge Analytica stories by the *New York Times* and *The Guardian* are important and powerful, but it is incorrect to call this a 'breach' under any reasonable definition of the term. . . .We can condemn this behavior while being accurate in our description of it."[45]

Two years later, the updated top line in Facebook's first press release in response to the Cambridge Analytica scandal reads "The claim that this is a data breach is completely false. [The app developer] requested and gained access to information from users who chose to sign up to his app, and everyone involved gave their consent. People knowingly provided their information, no systems were infiltrated, and no passwords or sensitive pieces of information were stolen or hacked."[46]

Although Facebook was parsing the distinction between privacy and security, one harm was identical to the harm of a data breach—billions of pieces of personal data were compromised when they were improperly exposed to third parties.[47]

Facebook's privacy failures led to the practical equivalent of a security incident. Specifically, the failure of Facebook to meaningfully consider

privacy in the design of its system and user interfaces left users vulnerable. According to scholar Ian Bogost, when a person accesses Facebook's troublesome interface that was at issue in the Cambridge Analytica scandal, "the user must accept [a third-party] app's request to share data with it as soon as they open it for the first time, even before knowing what the app does or why."[48] Facebook, not the third party, presented the request for users to consent to data practices, which made the request seem "official, safe, and even endorsed." But of course, it wasn't. Facebook simply passed data to the third party.[49] The third-party apps only once asked users (during their first use) for permission to collect and process peoples' data (including the data of their "friends"). After that, the data flowed unencrypted to the app company for years.[50] Apps were required to have privacy policies, but Facebook didn't review them. Instead, Facebook just checked to see if the link to the privacy policy went to a valid webpage.[51]

In its complaint against Facebook, the U.S. Federal Trade Commission (FTC) stated that Facebook's controls to address privacy risks created by third-party apps "did not include screening the third-party developers or their apps before granting them access to user data." Facebook inconsistently enforced its own policies.[52]

The FTC ultimately slapped Facebook with an unprecedented $5 billion fine.[53] Two Commissioners dissented, arguing that even this whopping fine wasn't enough.[54]

The Cambridge Analytica scandal demonstrates that the relationship between privacy and security is vitally important and increasingly frayed. Malicious parties compromised and exfiltrated Facebook users' data in a way that was different than your standard "hack n' breach," but to nearly the same effect. The key difference is that the third parties that filched people's data didn't bypass Facebook's technological safeguards. They used Facebook for the exact purpose for which it was designed. In other words, this was a breach that didn't occur through a break-in at the back door but through a walk-in at the front door. We can't protect data by locking it in a safe if we then give out the combination to anyone who asks for it. Although the front door is essential for security, it is often isolated in the privacy silo, where it doesn't receive the extensive resources from the

security silo. For many organizations, too myopic a focus on the back door results in insufficient protection for the front door.

Unnecessary Data Makes Data Breaches Worse

Data that doesn't exist can't be compromised. The central privacy principle of *data minimization*—to collect only data necessary for the purpose at hand and to avoid retaining unnecessary data—can play a key role at minimizing the harmful effects of breaches. Many organizations collect far too much data and keep it for far too long. They should be collecting less from the outset (and designing tools incapable or discouraging of collecting more), which will soften the impact if their databases ever get breached.

For example, companies invest billions in an insatiable desire to collect as much information about you as possible so they can target you with ads (for questionable efficiency gains).[55] One such company you have probably never heard of is BlueKai, an ad tech tracking startup bought by Oracle in 2014 for over $400 million. But BlueKai has heard of you. It has amassed "one of the largest banks of web tracking data outside the federal government."[56] And, for a time "that web tracking data was spilling out onto the open Internet because a server was left unsecured and without a password, exposing billions of records for anyone to find."[57]

In another case, Ashley Madison was a popular adultery website created by Noel Biderman, a former sports agent. The website had the slogan "Life is short. Have an affair." People could create a free profile, where they would list their turn-ons, sexual preferences, and location, as well as include their photo. Male users had to pay fees to send messages to female members. Although Ashley Madison promised users that their information would be "100% discrete" if they cancelled their accounts, they had to pay an additional $19 to remove all their information from the website. By 2015, Ashley Madison claimed to have 37.6 million users in more than 46 countries.

Unfortunately for Ashley Madison and its users, a group of hackers broke into its database and posted 3.2 million records online. The

aftermath of the breach was ugly. People were fired and marriages were destroyed. Some people received threats of extortion. Some people committed suicide.

Ashley Madison demonstrates in the starkest terms—through blood and death—how privacy and security are related. Protecting privacy depends upon protecting security. Moreover, good privacy rules can help keep data secure. Ashley Madison kept data it shouldn't have kept. And although Ashley Madison offered a "Full Delete" option where users could pay to remove all their information from the site, Ashley Madison actually retained the information in its database for a year. It flaunted people's trust, and everyone involved got burned.

The lesson for data security in the Ashley Madison case is that heeding the key privacy principle of data minimization can significantly lessen the harm of a data breach. As we noted earlier, data breaches can't all be stopped; they are inevitable. But their damage can be reduced by having good privacy practices.

Poor Privacy Regulation Allows for More Tools that Compromise Security

Good privacy rules will also regulate and minimize the harmful impact of manipulation and microtargeting made effective by our personal data, which can lead to massive data security vulnerabilities. Not only are surveillance ad networks vectors for the delivery of malware, but they allow criminals to use our own personal information against us to entice us to click links or share information.

Tools of surveillance, such as spyware, are regularly re-purposed by attackers to gain access to databases by stealing credentials or merely improperly accessing the same information that triggers breach notification. Privacy laws restrict spyware, but the laws thus far haven't been effective enough. As Professor Danielle Citron notes, "At least in theory . . . the providers of stalking apps could face federal and state criminal charges if it can be proved beyond a reasonable doubt that they knew or had reason

to know the apps were designed to be 'primarily useful' for secret surveillance."[58] Unfortunately, Citron also observes that "[t]here have been few, if any, state prosecutions against the entities providing covert surveillance tools and a modest number at the federal level."[59]

Beyond being a grave threat to privacy, spyware also threatens data security by allowing fraudsters to obtain essential data to carry out a breach. Spyware such as keystroke loggers is often used to pilfer passwords to gain access to encrypted files.[60]

Surveillance tools like trackers and the ubiquitous devices that make up the "Internet of Things" do hackers' jobs for them. The fitness app Strava was designed to be used with fitness trackers like FitBit to record users' exercise activity and share it with others. It did that, and more. In a data visualization map released by the company that showed all the activity tracked by its users, "military analysts noticed that the map is also detailed enough that it potentially gives away extremely sensitive information about a subset of Strava users: military personnel on active service."[61] The map leaked "[s]ensitive information about the location and staffing of military bases and spy outposts around the world."[62] This is exactly the kind of information hackers break into databases to obtain.

Lawmakers and those responsible for enforcing the law should target software primarily designed to invade privacy without sufficient legitimate uses. For example, those that create and deploy spyware should be faced with civil liability and even criminal prosecution in some cases. Right now, the FTC is limited in its fight against spyware, but new privacy and security legislation could allow those harmed by spyware to pursue lawsuits against spyware makers under "means and instrumentalities" theories similar to products liability lawsuits.[63]

Lack of Accountability Leads to Compromised Data

A key component of strong privacy protection is to ensure that all repositories of personal data are mapped and have a data shepherd—a person who is responsible for looking out for that data and who is accountable for what happens to that data. Far too often, organizations don't know all the

personal data that they maintain or where it is kept. Personal data can be collected in so many different ways and at many different times and places.

For example, a company can collect personal data when people submit a form to sign up for a newsletter, purchase an item, create an account, call customer service, and so on. Personal data is collected even when people visit the company's website. The company also maintains personal data about its employees. These repositories of personal data are often maintained by different departments in different places in the company. Without a shepherd, over time, the data could be forgotten, lost, or find its way outside of the security bubble and onto areas of servers that are accessible to the public.

In fact, the amount of data that is left exposed on unprotected areas of servers is shocking. The website DataBreaches.net, which has been chronicling data breaches since 2009, has covered, at the time this book was written, over 3,500 stories about the online exposure of data.[64] Just a few of the recent headlines on DataBreaches.net include "Twitter-owned SDK leaking location data of millions of users";[65] "Misconfigured cloud storage bucket exposed Pfizer drug safety-related reports";[66] "A prison video visitation service exposed private calls between inmates and their attorneys";[67] and "Dr Lal PathLabs, one of India's largest blood test labs, exposed patient data."[68] This list goes on and on.

Proper accounting for this data would have helped companies properly configure their systems to avoid exposure. Doing a data inventory and having all data assigned to data shepherds are key components of good privacy hygiene. They are also essential for strong security. If organizations don't know what data they have, where it is located, and how it should be used, then it is hard to imagine how they can keep it secure. Despite the oft-used security metaphor of locks and safes, good security isn't really about locking up data; it's more about looking after data.

THE PRIVACY COSTS OF DATA BREACHES

Poor privacy practices weaken data security, and data breaches are often data security violations as well. Likewise, poor security practices weaken privacy protections, and data breaches are often privacy violations.

The Sony Breach

Sony was planning to release a new movie, a comedy called *The Interview* that mocked North Korean leader Kim Jong-un. Apparently, in retaliation for the movie, North Korean hackers launched a major attack against Sony.

The hackers were able to break in because they were able to steal the login credentials of a Sony systems administrator through a spear phishing attack. The hacker spent several months exploring Sony's computer system trying to find ways to wreak the most havoc.[69]

On Friday, November 21, 2014, some Sony executives received an email from a group calling itself "God'sApstls" that demanded "monetary compensation" or else Sony "[would] be bombarded as a whole." The spam filters picked it up or it went otherwise unread.

The first Sony employee to log in after that weekend must have received quite the shock. A blood-red skeleton with razor fangs had conquered every single computer on the Sony lot, rendering the machines useless and sparing neither interns nor executives. Superimposed in blocky crimson letters were the words "HACKED BY THE #GOP," along with a demand to "obey" and five links that led to repositories of internal Sony records. Also included was a deadline of 11 p.m. that very night, even though GOP's demands were ambiguous.[70]

Sony hoped to keep the matter quiet, but an anonymous person posted a picture of the garish lockdown interface on Reddit, eliciting a flurry of media attention.[71] Still, at the time, Sony officials thought there wasn't much to worry about. Employees returned to their work. One Sony supervisor called it "a one-day problem."[72] No one imagined the immensity of the storm to come.

To their dismay, Sony officials learned that the hackers hadn't just vandalized them; the hackers had wreaked near total destruction. "Wiper" malware, known as "Destover" or "Wipall," erased everything stored on 3,262 of the company's 6,797 personal computers and 837 of its 1,555 servers, mixing in a "special deleting algorithm that overwrote the data seven different ways," before disabling the computers' boot software.[73]

The destruction wasn't even the worst part. The hackers had created a wound, but they wanted to maim. The hackers thus took a turn in the direction of privacy and transformed a bad breach into an utter catastrophe. On November 24, the GOP posted four unreleased Sony data files to file-sharing sites. A few days later, several journalists received an email purporting to be from "the boss of G.O.P." with links to the anonymous sharing site Pastebin, along with a password. The links led to a neatly organized set of folders containing over 26 gigabytes of unencrypted Sony personnel data, including almost 50,000 unique Social Security Numbers and detailed biographical information, compensation details, work histories, and confidential medical information.[74] They also spread the leaked details to media outlets such as Gawker, BuzzFeed, and The Verge.

The first news reports hit the Internet on December 1. Sony employees began "coming to work afraid," as multiple reports of attempted identity theft poured in.[75]

The GOP dumped more files over several days in early December 2014.[76] On December 8, the GOP finally articulated a motive, linking their actions to Sony's forthcoming *The Interview*, which the group called "the movie of terrorism which can break the regional peace and cause the War!" The GOP called for Sony to pull the movie or face further reprisals. In addition to the note, GOP released another round of leaked information, this time the private emails of Sony President Steve Mosko and Sony Entertainment executive Amy Pascal. In total, the group leaked over 20,000 emails addressing sensitive personal and business issues, as well as thousands of stored contact details, many of which included home addresses.[77] Pascal's emails, in particular, stirred up a media circus because many included insensitive comments about friends, associates, industry figures, and even President Obama.

Additional emails were posted on December 13 and 14, which GOP dubbed "Christmas" gifts.[78] A final leak on December 16 warned of a "bitter fate" for anyone present wherever *The Interview* was to be screened and invoked the September 11 attacks while warning readers to keep their distance from screenings and warning those who lived nearby to

flee altogether. The actual leak consisted of over 12,000 emails and 7,000 contacts from the account of Michael Lynton, chairman and CEO of Sony.

Prior to this leak, Sony had already cancelled several media appearances involving the cast of *The Interview*, as well as most promotional events. Upon reading the December 15 warning, Sony immediately provided security for the film's actors and producers. Sony cancelled star Seth Rogen's appearances on late-night programming. Theater chains began to pull out of the film's screening. Sony later issued a press release announcing the cancellation of *The Interview*'s theatrical release—a decision that was criticized by many as cowardly. President Obama even called this decision "a mistake."[79]

December 19 brought a final communication from the GOP. In it, the group declared that Sony had suffered enough, and that they "lift[ed] the ban," allowing the *The Interview* to be released provided that Kim Jong-Un's death scene not be "too happy," and that Sony not "test [them] again." On December 24, on Google's servers, *The Interview* received an online release, earning a modest $40 million.

The Sony hack exposed a wealth of embarrassing information about both the company and its top executives. Amy Pascal apologized profusely and stepped down as co-chairwoman of Sony Pictures Entertainment and chairwoman of Sony's motion picture group.

At least two former Sony employees brought lawsuits while the leak was ongoing, though theirs and many others were later consolidated into a class action. The parties reached a settlement, approved in early 2016, which cost Sony $15 million. As part of the agreement, Sony also agreed to provide identity-theft protection through the end of 2017 and a compensation fund for class members who paid to protect themselves out of pocket.

The Sony breach was so harmful because of its privacy dimensions. This is one reason why privacy regulation is so essential to data security; not only can privacy regulation help prevent breaches, but it can also help lessen the harm that breaches cause. Typically, the privacy harm is felt by an organization's employees and customers. The Sony case is somewhat unusual in that the privacy harms were also experienced by upper management.

As we discussed in the previous chapter, the law can work to lessen privacy harm and take the sting out of many breaches. It is not clear that the law could have done much for the Sony executives, but the law could have helped the employees prevent identity theft and privacy harms.

Although it is especially difficult for the law to help prevent breaches caused by state-sponsored attacks, we highlight the Sony case because it demonstrates the enormous potential privacy implications of data breaches. Unfortunately, hackers and attackers are becoming increasingly aware of this fact, and they are finding new ways to threaten or inflict privacy harms to further their nefarious aims.

Ransomware's Grave Threat to Privacy

As we discussed earlier, ransomware is a significant data security threat. Ransomware is malicious software that encrypts the files on a computer or network. Criminal hackers then demand a ransom to decrypt the files. Otherwise, the files remain inaccessible and the data is lost.

Nearly all experts recommend that to protect against the increasingly likely threat of a ransomware attack, organizations should routinely back up their data and test the backup to make sure it works. With the data backed up, one of the main threats of the ransomware is neutralized.

A big debate with ransomware is over whether organizations should pay the ransom. Some contend that paying ransoms is the quickest way to get back up and running. Many others argue that ransoms should never be paid. They contend that the criminals will become emboldened by the payoff and might continue their extortion. Another argument against paying is that it encourages other criminals to use ransomware and sends the message that ransomware pays.[80] The main focus of the decision is on the possibility and ease of the restoration of the files. For example, in an intelligence memo, the FBI stated:

> The FBI does not advise victims on whether or not to pay the ransom. . . . Individuals or businesses that regularly backup their files on an external server or device can scrub their hard drive to remove

> the ransomware and restore their files from backup. If all individuals and businesses backed up their files, ransomware would not be a profitable business for cybercriminal actors.[81]

In recent years, criminals have added a frightening new dimension to their use of ransomware. They have realized, much like the Sony hackers, that heightening the privacy harms can make the breach much worse. Hackers exfiltrate a copy of the data before they encrypt it. In typical practice, they demand a payment to provide the decryption key to the encrypted data on the victim's system. But some criminals are demanding an additional payment to destroy the copy of the data that they exfiltrated. They threaten to release the data to the public if they aren't paid.[82] Security experts refer to this practice as the "double extortion" model.

In 2016, stories began to circulate about a nasty piece of malware called "Delilah" that allowed hackers to gather personal information and webcam data from people who do sensitive things online (such as visiting pornography websites). Hackers could then use that information to blackmail those people under the threat of disclosing their secrets to the world.[83] A user on Reddit reported a similar kind of attack in 2018.[84] The criminals extorted victims into providing them with insider information at targeted companies.

In 2020, five law firms were hit with ransomware called Maze. Instead of just encrypting the data, the criminals exfiltrated it first and then posted a small amount of it online when their victims didn't pay their ransom demands. The criminals then threatened to post the remainder of the data online unless the ransom was paid. According to one article: "Recent reports have shown the hacking group behind Maze ransomware has been steadily posting the data of its victims online after the organizations fail to pay the ransom demand. A compiled list of victims shows the data of several healthcare organizations are included in those postings, despite a lack of public reporting of those incidents."[85]

Maze's double-extortion model caught on. By the end of 2020, there were approximately 20 different threat actor groups that had created leak sites where they posted victims' data to pressure them into paying ransoms.

One of the most dramatic law firm attacks involved an attack on Grubman Shire Meiselas & Sacks, an entertainment law firm with many celebrity clients. The attackers initially demanded a ransom of $21 million. When the firm refused to pay, the attackers doubled the ransom to $42 million and dumped a small sample of data. When the law firm still didn't pay, the attackers started auctioning off celebrities' files.[86]

With the introduction of the threat to publicly disclose personal data, it is much harder for victims to refuse to pay ransoms. Before the data disclosure threat, the main considerations for whether to pay the ransom had been the amount of data that would be lost and how much more quickly the victim could be back in action again. Organizations that routinely backed up their data could protect themselves. But with a copy exfiltrated and the possibility it could be dumped publicly, not paying the ransom means that people's private data will be exposed. Imagine a hospital that decided not to pay the ransom, resulting in the hackers posting all their patient records online. The hospital owes a duty to its patients to protect their data. Does this duty extend to paying the ransom to prevent the data from being exposed?

The law hasn't yet figured out an answer to this question. Much of the advice for ransomware involves urging organizations not to pay ransoms so as not to encourage future ransomware attacks. This strategy aims to further the common good by trying to dry up the criminals' revenue source, but the strategy doesn't account for the privacy harms created by leaked personal data. Ratcheting up the privacy harms has changed the ransomware playbook and has made the situation far more complicated and terrible.

IMPROVING SECURITY THROUGH STRONGER PRIVACY RULES

Lawmakers and companies should bridge data security and privacy to make them go hand-in-hand, and even be mutually reinforcing. As a first step, lawmakers should embolden privacy law to strengthen data security efforts. The rampant manipulation of people, as well as the amassing of

swollen troves of personal data, not only threatens privacy but poses significant risks to security.

A holistic approach to data security law would better integrate privacy and data security. Strengthening certain controls and protections, typically found on the privacy side of the ledger, will help strengthen data security as well. Below, we provide two examples of types of privacy controls that improve security.

Maximizing Data Minimization

The idea that companies should only be able to collect and retain data that is adequate, relevant, and necessary is a bulwark against data abuse and the essence of privacy because it either prevents data from being created in the first place or compels its destruction. It also demonstrates how privacy and security must work together to achieve their separate goals.

Security can focus on how to retain data and how to protect its integrity. It can ensure that only authorized people can see data and that information doesn't get improperly accessed or leaked. Privacy focuses on difficult substantive questions such as how long the data is retained, how it can be used, and specifically who is authorized to see it and change it. Privacy focuses on determining when data should be destroyed, which is often based on regulatory requirements. Security plays a role in ensuring that the data is properly destroyed.

Lawmakers should embrace data minimization with the same zeal they embrace data security rules and for the same reasons. Although privacy and data security have slightly different functions, they work in tandem and roughly overlap to achieve the same goals.

Data Mapping

Privacy requirements such as data mapping provide awareness about potential security vulnerabilities. Data mapping shows what data is being collected

and maintained, the purposes for having this data, the whereabouts of this data, and other key information. Without good data mapping, personal data is often forgotten. When this occurs, data can fall outside the security bubble or be improperly accessed, with this access not being readily detected.

Data mapping is useful for both privacy and security. Keeping track of data ensures that it remains within the security bubble and has the proper security controls. There should be data stewards with accountability for each repository of data. Security can set controls to make sure that those who should have access do and that those who shouldn't have access don't, but it is often in the realm of privacy where the determination of who should have access is made.

Recently, privacy laws have been the main driver behind organizations engaging in data mapping. Laws such as the California Consumer Privacy Act (CCPA) require that businesses provide people with the specific personal data collected about them.[87] Even more helpful than individuals knowing the specific data business have about them is the byproduct of businesses being compelled to respond to individual requests to know. To be able to respond, businesses are forced to have a better understanding and inventory of the data they possess. The CCPA doesn't directly require data mapping, but the practice becomes necessary to carry out the CPPA's obligation to respond to individual demands to know about their data.

More privacy laws should require data mapping, ideally directly rather than indirectly like the CPPA. Laws should require that organizations ensure that all personal data is accounted for and have a person assigned to be accountable for it.

■

In addition to improving data minimization and data mapping rules, lawmakers could create improvements for data security by fortifying existing privacy preservation rules around concepts such as deidentification and rules against manipulation. Understanding the security benefits from good privacy practices could generate broader legislative support for privacy regulation. Companies would also benefit from learning not to undermine their efforts to promote security by having poor privacy practices.