

Boston University School of Law

## Scholarly Commons at Boston University School of Law

---

Books

---


3-2022

### **Breached!: Why Data Security Law Fails and How to Improve It**

Woodrow Hartzog

Daniel Solove

Follow this and additional works at: <https://scholarship.law.bu.edu/books>

 Part of the [Computer Law Commons](#), and the [Science and Technology Law Commons](#)



# 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.

© Daniel J. Solove and Woodrow Hartzog 2022

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, without the prior permission in writing of Oxford University Press, or as expressly permitted by law, by license, or under terms agreed with the appropriate reproduction rights organization. Inquiries concerning reproduction outside the scope of the above should be sent to the Rights Department, Oxford University Press, at the address above.

You must not circulate this work in any other form  
and you must impose this same condition on any acquirer.

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

*To Pamela and Griffin—DJS*

*To Mom and Dad—WH*

Oxford University Press

Oxford University Press



## TABLE OF CONTENTS

1. Introduction: Chronicle of a Breach Foretold 1

### **PART I: A Broader Understanding of Data Security**

2. The Data Breach Epidemic 17  
3. The Failure of Data Security Law 35

### **PART II: Holistic Data Security Law**

4. The Big Picture: System and Structure 65  
5. Responsibility Across the Whole Data Ecosystem 81  
6. Reducing Harm from Data Breaches 111  
7. Unifying Privacy and Data Security 128  
8. Designing Security for Humans, the Weakest Link 158  
9. Conclusion: The Holistic Approach 190

ACKNOWLEDGMENTS 199

NOTES 201

INDEX 235

Oxford University Press

# Introduction

## *Chronicle of a Breach Foretold*

Sometimes the thing we are looking for is right in front of us and yet we still don't see it. A great novella by Gabriel Garcia Marquez called *Chronicle of a Death Foretold* begins with the vicious fatal stabbing of the main character. The rest of the story reveals that all the warning signs about the murder were in plain sight yet ignored by everyone. The murder was readily preventable—but, because of human nature, it was almost inevitable.

The story of most data breaches follows the same pattern. We have read about thousands of data breaches, and the moral of most of these stories boils down to the same thing: The breaches were preventable, but people made blunders. What is quite remarkable about these stories is that they haven't evolved that much in decades. The same mistakes keep happening again and again. After so many years, and so many laws to regulate data security, why haven't the stories changed?

Let us begin with a classic data breach tale involving one of the largest and most notable breaches of its time—the Target breach of 2013. The story has many of the common themes of data breach stories, and what

makes it particularly fascinating is that it is a sinister version of a David-and-Goliath story. Target was Goliath, and it was well-fortified. With its extensive resources and defenses, Target was far more protected than most organizations. Yet, it still failed. This fact should send shivers down our spines.

In mid-December 2013, right in the middle of the holiday shopping season, executives at Target found out some dreaded news: Target had been hacked. It was cruel irony that the second-largest discount store chain in the United States quite literally had a target sign on it—Target's logo is a red and white bullseye. The hackers hit it with an arrow straight into the center.

Executives at Target learned about the breach from Department of Justice officials, who informed them that stolen data from Target was appearing online and that reports of fraudulent credit card charges were starting to pop up.<sup>1</sup> Quite concerned, the Target executives immediately hired a forensics firm to investigate.

What they discovered was devastating. Target's computer system had been infected with malware, and there had been a data breach. It wasn't just a small breach, or a sizeable one, or even a big one—it was a breach of epic proportions.<sup>2</sup> Target had the dubious distinction of having suffered the largest retail data breach in U.S. history.<sup>3</sup>

Over the course of two weeks starting in November 2013, hackers had stolen detailed information for about 40 million credit and debit card accounts, as well as personal information on about 70 million Target customers.<sup>4</sup> The hackers had begun to sell their tremendous data haul on black-market fraud websites.

The timing couldn't have been worse for Target. It suffered the single largest decline of holiday transactions since it first began reporting the statistic.<sup>5</sup> Target sales plummeted during a season which traditionally accounts for 20 to 40 percent of a retailer's annual sales.<sup>6</sup> To stop the bleeding, Target offered a 10 percent discount across the board. Nevertheless, the damage was catastrophic. The company's profits for the holiday shopping period fell a whopping 46 percent.<sup>7</sup>

The pain was just beginning. On top of the lost profits, costs associated with the breach topped \$200 million by mid-February 2014. These costs

would rise significantly due to bank reimbursement demands, regulatory fines, and direct customer service costs.<sup>8</sup> About 90 lawsuits were filed, leading to massive lawyer bills.<sup>9</sup>

What made this all the more unnerving for Target is that it had devoted quite a lot of time and resources to its information security. Target had more than 300 information security staff members. The company had maintained a large security operations center in Minneapolis, Minnesota, and had a team of security specialists in Bangalore that monitored its computer network 24/7. In May 2013—just six months before the hack—Target had implemented expensive and sophisticated malware detection software from FireEye.<sup>10</sup>

With all this security—an investment of millions of dollars, state-of-the-art security software, hundreds of security personnel, and round-the-clock monitoring—how did Target fail?

A common narrative told to the public is that this entire debacle could be traced to just one person who let the hackers slip in. In caper movies, the criminals often have an inside guy who leaves the doors open. But the person who let the hackers into Target wasn't even a Target employee and wasn't bent on mischief. The person worked for Fazio Mechanical, a Pennsylvania-based HVAC company, a third-party vendor hired by Target. The Fazio employee fell for a phishing trick and opened an attachment in a fraudulent email the hackers had sent to him. Hidden in the email attachment lurked the Citadel Trojan horse—a malicious software program that took root in Fazio's computers.<sup>11</sup>

The Citadel Trojan horse was nothing novel—it was a variant of a well-known malware package called ZeuS and is readily detectable by any major enterprise anti-virus software. But Fazio lacked the massive security infrastructure that Target had, allowing the malware to remain undetected on the Fazio computers. Through the Trojan horse, the hackers obtained Fazio's log-in credentials for Target's system.

With access to Target, the hackers unleashed a different malware program, one they bought on the black market for just a few thousand dollars.<sup>12</sup> Experts such as McAfee director Jim Walker characterized the malware as “absolutely unsophisticated and uninteresting.”<sup>13</sup>

At first, the malware went undetected, and it began compiling millions of records during peak business hours. This data was being readied to be transferred to the hackers' location in Eastern Europe. But very soon, FireEye flagged the malware and issued an alert. Target's security team in Bangalore noted the alert and notified the security center in Minneapolis. But the red light was ignored.

FireEye flagged as many as five different versions of the malware. The alerts even provided the addresses for the "staging ground" servers, and a gaffe by the hackers meant that the malware code contained usernames and passwords for these servers, meaning Target security could have logged on and seen the stolen data for themselves.<sup>14</sup> Unfortunately, the alerts all went unheeded. Furthermore, given that several alerts were issued before any data were actually removed from the Target systems, FireEye's automated malware deletion feature could have ended the assault without the need for any human action. However, the Target security team had turned that feature off, preferring a final manual overview of security decisions.<sup>15</sup>

With FireEye's red lights blinking furiously, the hackers began moving the stolen data on December 2, 2013. The malware continued to exfiltrate data freely for almost two weeks. Law enforcement officials from the Department of Justice contacted Target about the breach on December 12, armed not only with reports of fraudulent credit card charges, but also actual stolen data recovered from the dump servers, which the hackers had neglected to wipe.<sup>16</sup>

The aftermath of the breach caused tremendous financial damage to Target. It remains unknown what the precise cost of the breach was, but an estimate in Target's annual report of March 2016 put the figure at \$291 million.<sup>17</sup> The company's reputation was harmed. The CIO resigned. For customers, there was increased risk of future fraud. Daily spending and withdrawal limits had to be placed on many affected accounts, and new credit cards had to be issued, causing consumers significant time loss while updating their card information everywhere.<sup>18</sup>

The breach went down in the annals of data breach history—one for the record books. But it would soon be overshadowed by even bigger breaches.

## THE SYSTEM IS DOWN

On paper, the hackers never should have been able to breach Target. The hackers used cheap methods, such as readily detectable malware that wasn't state-of-the-art. They were quite sloppy and made careless mistakes. Target had much better technological tools and a large and sophisticated team. It conducted phishing tests and employed forensic investigators. The hackers were grossly outspent and outnumbered. Yet Target was still felled.

At first glance, it seems that Target's Achilles' heel was one employee at one of its third-party vendors. Most large companies have hundreds of third-party vendors. This person made just one wrong click of the mouse, and that was all the hackers needed. Had that one person not clicked, then a data breach leading to more than half-a-billion dollars might not have occurred. That's one very expensive mouse click!

However, a prolonged look reveals a host of systemic vulnerabilities. Although on a checklist Target looked healthy, it lost because one key factor wasn't accounted for—human behavior. Spending millions of dollars and installing high-tech software still couldn't prevent the humans from their fateful blunders.

It doesn't necessarily take technical wizardry or great skill to be a highly successful criminal on the Internet. Technologies and data ecosystems are so fragile and flawed that it is far too easy for hackers to break in. The black market is overflowing with cybercrime start-up kits.<sup>19</sup> Just download the tools and it's off to the races. Because crime committed using the Internet is rarely tracked down and enforced, in most cases, the fraudsters get away with it.

## WE HAVE MUCH TO LOSE

The stakes for data security are enormous. Data breaches, by which we mean the unauthorized exposure, disclosure, or loss of personal information, are not only more numerous; they are more damaging. Every year, millions of people are victimized by identity theft. Their personal data is

used by fraudsters to impersonate them. Victims suffer because their credit files become polluted with delinquent bills. Creditors go after victims for the unpaid bills, and victims struggle to prove that the bills weren't theirs. Identity thieves also steal people's identities to obtain medical care, and this has resulted in people losing their health insurance. There are cases where the police have arrested victims because their police records were tainted by the identity thieves.

Ransomware attacks are rising dramatically. Ransomware works by encrypting files on people's computers so that the files are unreadable and inaccessible. The data is held hostage. To get the data back, victims must pay the hackers a ransom. Ransomware is incredibly profitable for hackers. It is a frightening world where at any moment, all our computer files—our documents, our precious photos and videos, our music, our most important information—can be held hostage for a ransom. In 2018, the city of Atlanta, Georgia, spent \$2.6 million to recover from a ransomware attack on the city's systems that asked for the rough equivalent of about \$50,000 worth of the electronic currency Bitcoin.<sup>20</sup>

Malicious hackers can readily frame people when data is compromised. They can put incriminating files onto people's computers and then tip off law enforcement authorities.<sup>21</sup> Hackers can also access your most private photos and writings and publish them to the world.<sup>22</sup> They can take over your computer and use it to spam other people or to serve as a conduit through which to commit crimes.

As more devices, appliances, and vehicles are hooked up to the Internet, physical safety is at grave risk.<sup>23</sup> Hackers can break into our home devices. They can peer at our children through our baby cameras. They can snoop around through our home security cameras. They can listen in on us through our home assistant devices. They can gain control of our cars. They can also hack into implantable devices in our bodies, such as pacemakers or insulin pumps.

As more and more of our sensitive data is maintained in vast dossiers about us, as our biometric information is gathered and stored—such as our fingerprints, eye scans, facial data, and DNA—what will the future look like if organizations can't keep it secure?



In *Minority Report*, a 2002 movie based upon a short story by Philip K. Dick, the protagonist John Anderton is on the run, being pursued exhaustively by the authorities. The movie is set in the future—2054—where the government and businesses use extensive surveillance technologies. To evade capture via ever-present retinal scanners, John must undergo an operation to replace both of his eyes. The procedure is rather gruesome, but it is necessary given the pervasive use of biometric identification in the story.

Imagine the data breach notification letters of the future:

*We regret to inform you that we have suffered a breach, and hackers have obtained your retinal data, which they could use to impersonate you and gain access to accounts. To guard against future harm, we recommend that you immediately schedule an operation to replace your eyes.*

We are hurtling forward into a perilous future, with organizations collecting more data and with the consequences of its misuse becoming more dire—and even deadly.

## DATA SECURITY LAW'S GRAND ENTRANCE

During the past two decades, policymakers have rushed out a body of law to address the worsening data security nightmare. The most significant development is the rise of data breach notification laws, which require organizations that are breached to notify regulators, affected individuals, and sometimes the media. Breach notification is immensely popular; every state in America, as well as many countries, now have these laws. Unfortunately, breach notification merely alerts victims that their data was compromised in a breach. It doesn't cure the harm; it just informs people of the danger.

Then come the class action lawsuits. Sometimes mere hours after a breach is made public, attorneys file lawsuits against companies on behalf

of those whose data was compromised. Many of the suits fail. Others end up settling, with companies paying to save on the cost of litigating the case. Consumers often don't receive any significant benefits or compensation.

In the Target case, the consumer lawsuits for the breach settled for a pittance—just \$10 million. The settlement was a fee paid not on the merits of the case but to make it go away. The Target breach affected between 70 and 110 million individuals, which means that the recovery amounted to just a few pennies per person.<sup>24</sup> Victims did not see significant restitution as the settlement only applied to the reimbursement of notoriously elusive “documented damages” and reimbursements for “lost time,” which is often not given much value.

After breaches, regulators also step in to enforce, but many times regulators take a pass. There are too many breaches each year, and regulators only have the resources to go after a small fraction of them. When regulators step in, their penalties often just increase the cost of the breach to a small or modest degree. For example, a group of state regulators settled with Target for \$18.5 million.<sup>25</sup> With the Target breach costs at an estimated \$291 million, this regulatory penalty represents less than 10 percent of the total. Even if regulators or individual litigants were to recover more in penalties and damages, it's not clear that things would be any different. Of course, greater monetary pain after a data breach might provide a stronger incentive to keep data secure, but organizations already face significant costs for breaches, and the additional incentive is not likely going to be a game changer. Target was already taking security quite seriously and devoting significant resources to it. Target failed not because of a lack of commitment to data security but because it made mistakes.

Breaches set in motion a series of legal responses that often drag on for years and mire organizations in millions of dollars in expenses. By this time, however, it is far too late. The damage has been done, and the law mostly serves to heighten the expense to companies. While it is important to make sure that organizations internalize the risks they create, the law isn't addressing all other actors that create risk. To make matters worse, the law often fails to help individual victims whose data was compromised in the breach.

Despite data security law's obsession with data breaches, the law doesn't seem to be reducing the size, severity, or number of breaches. Data breaches are steadily increasing.<sup>26</sup> The news is inundated with stories about data breaches that were readily preventable through rather inexpensive, non-cumbersome means. Why aren't data breaches slowing down? Why doesn't the law seem to be making any difference?

## THE ARGUMENT OF THIS BOOK AND A ROADMAP

This is a book about how to improve the law's approach to data security. Our goal is to reorient the way the law addresses actors who create and participate in systems that leave personal information vulnerable to exposure and misuse.

Our book is not about cybersecurity in the broadest sense of the term, which applies to all forms of security with systems that use the Internet.<sup>27</sup> Instead, our focus is on *data security*, a significant piece of the cybersecurity pie that involves personal data. Data security law is largely part of privacy, data protection, and consumer protection frameworks like the Federal Trade Commission's (FTC) enforcement of rules against deceptive and unfair trade practices, the European Union's General Data Protection Regulation (GDPR), statutes that govern entities using personal data like the Health Insurance Portability and Accountability Act (HIPAA), and the law of torts that provides a remedy for negligent data practices.<sup>28</sup>

Although there is a lot of overlap between optimal regulation for data security and cybersecurity, there are important differences. The risk thresholds, threat modeling, actors affected, and type and magnitude of harm can differ when personal data is involved rather than when supply chains, machinery, or infrastructure are involved. It thus makes sense in some contexts to treat data security as unique from other areas of cybersecurity, and the law does so. Data security law emerges more from privacy law than cybersecurity law.

Unfortunately, data security law currently exists in an awkward space between cybersecurity and privacy. Being in this space has been a detriment

to data security law, which has often failed to incorporate the strengths of both cybersecurity and privacy. Laws addressing privacy issues often include data security as part of their framework. Because the legislative lens is on privacy, legislators typically focus on the individual. Breach notification dominates data security law. The security rules are often vague and sparse. In contrast, cybersecurity law frequently includes more robust security rules based on systems-focused security frameworks.

In a cruelly ironic way, data security law also fails to draw strengths from privacy law. Data security remains quite siloed from privacy. When it is part of privacy laws, data security is often cabined to narrow sections. Data security law has not fully incorporated privacy law's evolving recognition about designing to accommodate human behavior and protecting human values beyond confidentiality. To make matters worse, the protections in privacy law often fall short in ways that are bad for data security.

The fact that data security is often part of the fabric of privacy law is a missed opportunity. Lawmakers could draw from privacy law's toolbox to bring a richer and more nuanced approach to securing personal data. Yet so far, they have not.

In this book, we hope to bring data security law out of this "no man's land" to better reflect the overlapping wisdom of privacy and cybersecurity. Because we focus mainly on personal data, we largely leave to others more general critical cybersecurity issues such as infrastructure security, industrial espionage, cyberwarfare, computer crime, trade secrets and proprietary data, and the nuanced debates surrounding the market for and disclosure of security vulnerabilities.<sup>29</sup> Of course, these issues overlap with data security problems.<sup>30</sup> But in this book we are examining the data security piece of the pie.

We also are not seeking to critique the established strategies technologists have developed to protect information. Nor are we proposing new technological approaches to the field of cybersecurity. Rather, as legal scholars, we are drawing from existing security knowledge that the law often fails to embrace. Because we are not technology experts, we will not delve too deeply into technical specifics of data security. Instead, our goal is to

develop principles and theories that can guide the law for the foreseeable future. In this book, we propose a general approach lawmakers and judges can take to improve the security of personal data, and we outline a broad set of principles to bring coherence and consistency to a body of law that for too long has been focusing in the wrong direction.

Our argument is built around one overarching point: To improve the rules for securing personal information, policymakers must counter-intuitively shift the law's focus beyond data breaches. Too much of the current law of data security places the breach at the center of everything. Turning data security law into the "law of breaches" has the effect of over-emphasizing the conduct of the breached entities while ignoring the other actors and factors that contributed to the breach. We present an alternative, broader vision of data security policy in three areas: accountability, redress, and technological design.

It is tempting to say to organizations: "Come on, just be more secure!" But data security is notoriously complicated and needs a great deal of calibration. Ironically, some attempts by lawmakers and industry to add more security can actually make systems more vulnerable.<sup>31</sup> Security measures come with difficult costs and tradeoffs, so the choice of which ones to use and how many is quite challenging.

Data security is a delicate dance between technology and people. The ideal amount of data security is not necessarily to be as secure as possible and avoid a breach at all costs. In most cases, it is a poor policy choice for an organization to have the strongest possible security because the tradeoffs are too significant. It is easy to underappreciate the costs of many security measures because costs are often thought of in monetary terms. But the biggest costs of many security measures are that they can reduce functionality, make things inefficient and inconvenient, and be difficult and time-consuming.

One of the challenges with data security is that there are no absolute answers, as we are dealing with a continuum of risk and an ongoing cat-and-mouse game between attackers and defenders. Policy choices depend upon not only an assessment of risk but also an assessment of the costs of addressing those risks. A complicated balancing must take place.

Current data security rules fail to address risk effectively. In many circumstances, the law penalizes breaches with little regard to considerations of risk and balance. Other times, the law levies no penalty against organizations even though their actions created enormous unwarranted risks.

We contend that there is a better role for law to play. The main lesson of this book is that time and again, data security law and policy are missing the bigger picture. Lawmakers should move beyond the reactionary “blaming the breached” and hold accountable all the actors in the data ecosystem that contribute to the problem. They should break down the silos between privacy and security. They should promote human-centric security that accounts for the way people actually think and act.

Part I of this book focuses on the challenges to data security and why the law is not adequately addressing these challenges.

In Chapter 2, we provide a brief history of data security in this century. We discuss how and why data breaches started to capture news media headlines. In our brief sweep through the past two decades, we cover the most historic breaches and the new security threats that emerged. When looking at the big picture, the war against data breaches is being lost, one battle at a time. There is a lot to learn from data breach stories; there are common plot lines that clearly show us why data security is so often failing.

In Chapter 3, we survey the law and policy of data security and analyze its strengths and weaknesses. We conclude that despite some small successes, law and policy are generally failing to combat the data security threats we face. Data security law is too reactionary. The law often merely increases the cost of data breaches but fails to do enough to prevent them. Moreover, the law has failed to protect individuals who are being put at greater risk by inadequate data security.

In Part II of this book, we propose a different approach to data security that we call “holistic data security.” Under this approach, the law would apply earlier, more frequently, to more actors, and to more activity.

In Chapter 4, we introduce our approach, holistic data security, which focuses on the mitigation of risk in an entire data ecosystem. Instead of

concentrating solely on individualized harm and specific breaches, data security law should aim to ensure the wellbeing and resilience of the data ecosystem. Our approach draws insights from fields that focus on entire systems, such as public health.<sup>32</sup> Both data security and public health rules seek to keep a complex and dynamic system safe and thriving. Both frameworks address complex, opaque, and ever-shifting risks that make attributing causation and effective enforcement at the individual level difficult. Both fields are tasked with mitigating the spread of “viruses.” Yet public health law seeks to sustain the health of an entire population by mandating practices that reduce risk across the board.<sup>33</sup> Meanwhile, data security law struggles to look beyond the place where a virus took hold, addressing only the last links in the chain.

In Chapter 5, we contend that lawmakers and courts can better distribute responsibility among all the different actors who play a role in the problem of data security even if they are not proximate to an actual breach. Data breaches are not just caused by the particular organizations that have the breach. Breaches are the product of many actors—it takes a village to create a breach. We provide a survey of these various actors and their contributions to the problem.

Unfortunately, the law doesn’t hold most of the actors accountable. Policymakers often focus rather myopically on the particular organizations being breached, and they often overlook the fact that data security is a systemic problem.

In Chapter 6, we argue that policymakers also often fail to address practices by other organizations that increase the harm of data breaches to people as well as increase the costs. We can’t eliminate all breaches, but we can significantly reduce the harm that they cause.

In Chapter 7, we address the relationship between privacy and security. Privacy is a key and underappreciated aspect of data security. Right now, there is a schism between privacy and security in companies. Privacy functions are commonly addressed by the compliance and legal departments, while security is handled by the information technology department. The two areas are commonly split apart and rarely speak to each other.

We should bridge data security and privacy and make them go hand-in-hand in both law and policy. Strong privacy rules help create accountability for the collection, use, and dissemination of personal information and can reduce vulnerabilities and risk by minimizing the use and retention of personal information. Good privacy strengthens security.

In Chapter 8, we argue that although most failures in data security involve human error, policymakers are not designing security measures with humans in mind. Instead, humans are expected to do things that are beyond the bounds of normal cognition. Far too little emphasis and resources are given to educating people about their role in data security. The result is that policymakers have failed to address the greatest security vulnerability—the human factor.

Consider again the Target breach. On a checklist, Target looked healthy—it had good policies, a large security team, significant resources, and strong security software. Spending millions of dollars and installing high-tech software still couldn't prevent human blunders. Humans turned off the software. Humans ignored the blinking red lights. A human clicked on the wrong link.

Rethinking law with humans at the center is not just a simple rethink—it goes to the very core of our law and policy regarding data security. It means that many of our existing policies are flawed and that a number of commonly accepted good security practices are, in fact, bad.



In this book, we are calling for policymakers to take a new direction, a fundamental shift in focus. Along the way, we suggest some specific things that the law should require, but we are not aiming to provide a laundry list of particular measures. Our focus is on the big picture. We propose a different way of thinking about data security, and we set forth our vision for how the law can take a different approach.