

Boston University School of Law

Scholarly Commons at Boston University School of Law

Faculty Scholarship

2017

Privacy's Trust Gap

Neil M. Richards

Woodrow Hartzog

Boston University School of Law

Follow this and additional works at: https://scholarship.law.bu.edu/faculty_scholarship



Part of the [Privacy Law Commons](#)

Recommended Citation

Neil M. Richards & Woodrow Hartzog, *Privacy's Trust Gap*, in 126 Yale Law Journal 1180 (2017).
Available at: https://scholarship.law.bu.edu/faculty_scholarship/3071

This Article is brought to you for free and open access by Scholarly Commons at Boston University School of Law. It has been accepted for inclusion in Faculty Scholarship by an authorized administrator of Scholarly Commons at Boston University School of Law. For more information, please contact lawlessa@bu.edu.





NEIL RICHARDS & WOODROW HARTZOG

Privacy's Trust Gap: A Review

Obfuscation: A User's Guide for Privacy and Protest

BY FINN BRUNTON AND HELEN NISSENBAUM

CAMBRIDGE AND LONDON: THE MIT PRESS, 2015.

AUTHORS. Neil Richards is Thomas and Karole Green Professor of Law, Washington University School of Law; Affiliate Scholar, The Center for Internet and Society at Stanford Law School; and Affiliated Fellow, Yale Information Society Project. Woodrow Hartzog is Starnes Professor of Law, Samford University's Cumberland School of Law; and Affiliate Scholar, The Center for Internet and Society at Stanford Law School. For helpful suggestions and conversations, we would like to thank Frederik Borgesius, Brannon Denning, and Evan Selinger. We are especially indebted to Nico van Eijk, whose invitation for us to participate in the 2015 Amsterdam Privacy Conference at the Institute for Information Law (IViR) at the University of Amsterdam was the genesis of this Book Review.



BOOK REVIEW CONTENTS

INTRODUCTION	1182
I. OBFUSCATION AND THE INDIVIDUALISTIC STORY OF PRIVACY	1188
A. The Appeal of Obfuscation	1189
1. <i>Obfuscation's</i> Argument	1189
2. A Pragmatic Rebuttal to Overly Simplistic Notions of Privacy	1191
3. The Need for Privacy Outside Trustworthy Relationships	1195
B. Privacy Islands	1197
II. OBFUSCATION REQUIRES TRUSTWORTHY ALLIES	1201
A. <i>Obfuscation's</i> Call for a Lonely Revolution	1201
B. Obfuscation Requires Reliance on Designers	1205
C. Obfuscation Requires Cooperation from Confederates	1206
III. OBFUSCATION AS SECOND-BEST PRIVACY	1207
A. Obfuscation Promotes Distrust	1207
B. Legal Reform Is Not Hopeless	1209
IV. THE POTENTIAL OF TRUST	1213
A. A Theory of Privacy and Trust	1213
B. Privacy Problems from a Trust Perspective	1215
C. Promoting Trust in a Digital Society	1219
CONCLUSION	1223

INTRODUCTION

It can be easy to get depressed about the state of privacy these days. In an age of networked digital information, many of us feel disempowered by the various governments, companies, and criminals trying to peer into our lives to collect our digital data trails.¹ When so much is in flux, the way we think about an issue matters a great deal. Yet while new technologies abound, our ideas and thinking—as well as our laws—have lagged in grappling with the new problems raised by the digital revolution.

Reading between the lines in the debate over surveillance and data collection, it is easy to think that protecting privacy is all on you. Most privacy discussion is framed in individualistic terms. For example, we talk about an individual's "right to privacy" and whether that individual right has any meaning any more. Policymakers fight for a person's "individual control" over personal information. Companies promise to give consumers "personal choice" to empower their personal preferences about how their information is collected, used, and shared. It is as though we are all islands, each waiting to exercise our individual ability to protect our privacy against those who would surveil us, whether they are private companies or government agents.

Thinking of privacy as an issue of personal choice, preferences, and responsibility has powerful appeal. It resonates with American ideals of individualism, democracy, and consumerism. It flatters our sense of autonomy and accommodates our diverse notions of privacy and preferences for disclosure. For instance, you might not want to broadcast the details of your life on Instagram or Snapchat, but others might. Individualistic notions of privacy lead us to favor solutions that help us choose and put us in control of our own unique lives.

Yet there is a problem with this view of the digital world, and it is a problem of power. In the digital economy, the real power is not held by individual consumers and citizens using their smartphones and laptops to navigate the twists and turns of their lives, but by the large government and corporate entities who monitor them. The digital consumer is not like the classic American myth of the cowboy, a rugged and resilient island of autonomy set against the backdrop of the digital frontier. On the contrary, she is increasingly disempowered, marginalized, and subject to monitoring and sorting by powerful institutions about whose existence she may not know, and whose activities she may not be able to resist. In the digital world, we may heap responsibility on indi-

1. Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013) (outlining the modern surveillance problem, in which individuals are monitored by government and corporate watchers, and explaining when and why surveillance is particularly dangerous).

vidual users of technology, but they lack options for protecting themselves.² This is another form of the “digital divide”—it is not merely that some people have access to technology while others do not, but that most people are vastly less powerful than the government and corporate institutions that create and control digital technologies and the personal data on which those technologies run.

If the monitored are responsible for protecting themselves, one possible strategy is to obscure their tracks, thereby turning the digital realm into a big game of hide and seek. In their book *Obfuscation: A User's Guide for Privacy and Protest*, Finn Brunton and Helen Nissenbaum put forward a manifesto for the digitally weak and powerless, whether ordinary consumers or traditionally marginalized groups who lack the knowledge or means to effectively protect their digital lives from monitoring.³ They tell us at the outset that “[w]e mean to start a revolution with this book. But not a big revolution—at least, not at first.”⁴ Brunton and Nissenbaum develop the idea of obfuscation, which they define as “the deliberate addition of ambiguous, confusing, or misleading information to interfere with surveillance and data collection.”⁵ This can take many forms, but for consumers, it might include swapping their phone SIM cards with those of their friends or using software that buries genuine search engine queries in a crowd of irrelevant ones.⁶ Brunton and Nissenbaum argue that obfuscation is necessary to counteract information power imbalances that occur “when data about us are collected in circumstances we may not understand, for purposes we may not understand, and are used in ways we may not understand.”⁷

Obfuscation is attractive because it offers to empower individuals. It is a chance for people to strike back against forces that have the ability and incentive to exploit informational power for surveillance and data collection, whether government law enforcement agencies or Internet tracking and marketing companies. It carves out spaces for privacy against the powerful—a digital treehouse, French Resistance hideout, or Dagobah swamp. Obfuscation is a “weapon of the weak,” offering the romantic promise of restoring some of the

2. *Id.*; see Ryan Calo, *Can Americans Resist Surveillance?*, 83 U. CHI. L. REV. 23 (2016).

3. FINN BRUNTON & HELEN NISSENBAUM, *OBUSCATION: A USER'S GUIDE FOR PRIVACY AND PROTEST* (2015).

4. *Id.* at 1.

5. *Id.* (emphasis omitted).

6. *Id.* at 13, 18.

7. *Id.* at 2-3.

digital age's power imbalances in favor of the plucky underdog.⁸ Obfuscation is appealing, even seductive, but we must ultimately put it in context. Obfuscation is a powerful idea, but as Brunton and Nissenbaum are careful to admit, it is only part of the larger privacy puzzle.⁹

Even with this caveat, obfuscation seems ill suited to be the stuff of revolutions, because privacy built on obfuscation can be at most a second-best kind of privacy. Instead of a first-best privacy in which rules and design ensure safe, sustainable processing of personal data, and personal control is properly treated as a scarce resource, obfuscation offers only the kind of privacy that requires the disempowered to grab it for themselves. As such, it falls into the all-too-common trap of thinking about privacy in primarily individualistic terms, leveraging the weak power of individuals rather than the strong power of law and society. It reinforces the standard narrative of privacy that emphasizes control, choice, and privacy self-management above all else—a narrative that is likely doomed to failure if we continue to accept it.¹⁰

This reinforcement of the default story can be a serious problem. How we think about legal problems matters a great deal, especially in areas like privacy where technologies, economics, and social norms are in flux. The frames and metaphors we use to describe issues like privacy are essential because they allow us to understand or confuse issues, problems, and potential solutions.¹¹

Brunton and Nissenbaum are careful to position obfuscation as a realistic, affordable, and reliably good enough tactic to protect our privacy. This is a real and important contribution. A healthy dose of pragmatism regarding how to preserve our privacy is welcome in the modern climate, in which the utopian dreams of some global regulators can sometimes create irrational and ineffective obligations regarding data. Consider, for example, the implications of a broad reading of the European “Right to Be Forgotten,” which is sometimes

8. *Id.* at 55.

9. *Id.* at 3 (“Obfuscation has a role to play, not as a *replacement* for governance, business conduct, or technological interventions, or as a one-size-fits-all solution (again, it’s a deliberately small, distributed revolution), but as a tool that fits into the larger network of privacy practices.”).

10. For extended critiques of this narrative, see Neil M. Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. (forthcoming 2017), <http://ssrn.com/abstract=2655719> [<http://perma.cc/5HAU-ZRLS>]; and Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880 (2013).

11. Woodrow Hartzog, *The Fight To Frame Privacy*, 111 MICH. L. REV. 1021 (2013) (reviewing DANIEL J. SOLOVE, *NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY* (2011)); Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087 (2006) (reviewing DANIEL J. SOLOVE, *THE DIGITAL PERSON: PRIVACY AND TECHNOLOGY IN THE INFORMATION AGE* (2004)).

described as creating an internet that could be edited like Wikipedia by individuals who do not like the facts reported about them in newspapers.¹² All too often, a privacy policy like this can make the perfect the enemy of the good by seeking to outright prevent or control data collection or surveillance, rather than to mitigate problems through regulations designed to serve human ends. More nuanced understandings of privacy are necessary to temper overambitious regulations which fetishize consent in ways that elevate form over function. Society's adoption of a more pragmatic approach to privacy can also ease the pressure on regulators to adopt draconian privacy rules such as data localization laws, which can provide cover for countries seeking to preserve their own economic interests, while providing few real benefits for citizens.¹³ Brunton and Nissenbaum show that sometimes a bit of pragmatic privacy can be enough to do what is needed.

More fundamentally, however, pragmatism will not be enough if the conceptual foundation for protecting our privacy is deficient. In talking about the foundation for a privacy revolution, we can do better than making incremental improvements to the standard story of a highly individualistic, atomistic privacy. We must think about privacy instead as the rules which govern personal information and take into account more complex social contexts, the increasing importance of *information relationships* in the digital age, and our need to rely on (and share information with) other people and institutions to live our lives.¹⁴ Information relationships are relationships in which information is shared in trust and in which the rules governing the information sharing create value and deepen those relationships over time. If privacy is increasingly about these information relationships, it is also increasingly about the *trust* that is necessary for them to thrive, whether those relationships are with other humans, governments, or corporations. Trust is particularly important for the

-
12. E.g., NEIL M. RICHARDS, *INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE* 90-92 (2015); Woodrow Hartzog, *A Stronger Online Eraser Law Would Be a Mistake*, NEW SCIENTIST (Nov. 6, 2013), <http://www.newscientist.com/article/mg22029420-200-a-stronger-online-eraser-law-would-be-a-mistake> [<http://perma.cc/8M8C-EYTY>].
 13. See Eoin Carolan & M. Rosario Castillo-Mayen, *Why More User Control Does Not Mean More User Privacy: An Empirical (and Counter-Intuitive) Assessment of European E-Privacy Laws*, 19 VA. J.L. & TECH. 324, 326 (2015); Anupam Chander & Uyen P. Lê, *Data Nationalism*, 64 EMORY L.J. 677, 677 (2015) (arguing that concerns about surveillance and security "are justifying governmental measures that break apart the World Wide Web, without enhancing either privacy or security"); Omer Tene, *Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws*, 74 OHIO ST. L.J. 1217, 1247-48 (2013).
 14. Neil M. Richards, *The iPhone Case and the Future of Civil Liberties*, BOS. REV. (Feb. 25, 2016), <http://www.bostonreview.net/us/neil-richards-apple-iphone-privacy> [<http://perma.cc/RNC6-QXDA>].

large tech companies with which we increasingly share vast amounts of often-intimate data. For instance, the battles that Apple and Microsoft have fought with the Federal Bureau of Investigation (FBI) and the Department of Justice (DOJ) are battles fought to earn and keep the trust of their customers.¹⁵ In this direction lies a better digital future for all of us—a digital society in which privacy rules promote trust and make life better for the humans who inhabit it. This is what we will call “first-best” privacy protection.

By contrast, obfuscation is a creature of distrust—a last resort of the weak, the marginalized, and the betrayed. Obfuscation is not merely *motivated* by distrust; it also *creates* additional distrust by hiding from the surveillance economy or intentionally feeding bad data into it. Obfuscation is a kind of pollution of the information economy, which can be useful in the short term but costly or even unsustainable in the long run. While obfuscation can be useful to those who have no other options, it can also sow distrust when injected into existing relationships. We believe that a better strategy for a sustainable digital future is to promote trustworthy information relationships—the building blocks of a digital society. In these relationships, obfuscation by one party against another can sow damaging distrust. By further undermining the potential of trust, ob-

-
15. *Id.* In February 2016, the FBI attempted to compel iPhone maker Apple to create a piece of software that would allow the FBI to access the locked iPhone that belonged to Syed Farook, a man who, together with an accomplice, killed fourteen people in San Bernardino, California. The FBI relied upon the authority granted under the All Writs Act to compel Apple to create this software. Apple refused and after a brief but intense legal challenge, the FBI withdrew its request, saying it had found another way to access the phone. See Julia Powles & Enrique Chaparro, *In the Wake of Apple v FBI, We Need To Address Some Uncomfortable Truths*, GUARDIAN (Mar. 29, 2016), <http://www.theguardian.com/technology/2016/mar/29/apple-fbi-encryption-san-bernardino-uncomfortable-truths> [http://perma.cc/GNH6-BBWW]; Neil Richards & Woodrow Hartzog, *Apple v the FBI: Why the 1789 All Writs Act Is the Wrong Tool*, GUARDIAN (Feb. 24, 2016), <http://www.theguardian.com/technology/2016/feb/24/apple-v-the-fbi-why-1789-all-writs-act-is-the-wrong-tool> [http://perma.cc/TE8L-RAPF]; Sam Theilman, *Apple v the FBI: What's the Beef, How Did We Get Here and What's at Stake?*, GUARDIAN (Feb. 20, 2016), <http://www.theguardian.com/technology/2016/feb/20/apple-fbi-iphone-explainer-san-bernardino> [http://perma.cc/UX49-CJ3G]. Microsoft has also challenged the authority of the DOJ to force the disclosure of customer emails stored on servers outside of United States under the Stored Communications Act. In July 2016, a federal court of appeals found in favor of Microsoft, forcing the DOJ to seek the emails through alternative international frameworks, such as the mutual assistance in law enforcement treaty, a legal device facilitating international cooperation between police departments. Sam Theilman, *Decision in Microsoft Case Could Set Dangerous Global Precedent, Experts Say*, GUARDIAN (Sept. 9, 2015), <http://www.theguardian.com/technology/2015/sep/09/microsoft-federal-case-data-security-precedent> [http://perma.cc/ZW3M-Y65V]; Sam Theilman, *US Cannot Force Microsoft To Hand over Emails Stored Abroad, Court Rules*, GUARDIAN (July 14, 2016), <http://www.theguardian.com/technology/2016/jul/14/microsoft-emails-court-ruling-us-government> [http://perma.cc/YY5G-FFHE].

fuscation thus offers a kind of “second-best” privacy that will actually cause us to lose ground in the long run. If we fall prey to the pessimistic and isolationist aspects of obfuscation, we risk seeing our only option as a guerrilla war against privacy forces with which we might otherwise be able to work. It is a war we cannot win.

This Book Review proceeds in four parts. In Part I, we discuss the central arguments and contributions of *Obfuscation* through the lens of the standard individualistic conception of privacy. We welcome the book's pragmatism and leveraging of practical, financial, and cognitive limitations to frustrate those who would engage in surveillance and data collection. However, we critique *Obfuscation*'s adoption of the individualistic conception of privacy. This account, which is the dominant story of privacy for both regulators and citizens, has been handicapped by a conceptual vocabulary that fails to fully take the importance of relationships and trust into account. Modern privacy policy and discourse thus have a trust gap, failing to account for the importance of trust to our digital society, and failing to provide the incentives to create that trust. By accepting the dominant frame, and by encouraging distrust over trust, obfuscation theory not only falls into the trust gap, but deepens it.

Against the backdrop of privacy's trust gap, we then offer both an internal and an external critique of Brunton and Nissenbaum's obfuscation theory. We develop our internal critique in Part II, taking issue with Brunton and Nissenbaum's description of obfuscation as a largely solitary and independent strategy. We argue that even within the parameters of obfuscation theory, people often have to depend upon others to obfuscate effectively. Unless people can trust designers, intermediaries, confederates, and lawmakers to help them obfuscate, the tactic will frequently fail. It is those who must trust others, the weak and vulnerable, who need obfuscation the most. Yet by feeding bad data into the system, obfuscation can have the perverse effect of further corroding social trust.

In Part III, we offer a broader, external critique of obfuscation. We caution against leveraging the wisdom of obfuscation into a premature guerrilla war for our privacy. Such a strategy has an undeniable romantic appeal, but we do not yet need to resort to a guerilla war of individuals against the powerful institutions that seek our data. As lawyers, we believe that the first-best solution to problems of social power that *Obfuscation* catalogs is not revolution, but regulation. Although it may not always be obvious, privacy is not doomed. Law and public policy can and should play a role in promoting trust and privacy. Con-

trary to popular and legal rhetoric about the “death of privacy,”¹⁶ there is substantial evidence that the campaign for privacy rights can be not only viable, but also effective. It would be a mistake to cede the high ground of legal reform to fend for ourselves by embracing self-help obfuscation at the expense of trust-based solutions like confidentiality, data ethics, transparency, and data security. But by ignoring both the current evidence that privacy law can do helpful work and rejecting the potential of law, this is essentially the strategy that Brunton and Nissenbaum recommend.

In Part IV, we offer an alternative frame for thinking about privacy problems in the digital age. We propose that a conceptual revolution based upon trust is a better path forward than one based on obfuscation. Drawing upon both our prior work and that of the growing community of scholars working at the intersection of privacy and trust, we offer a blueprint for trust in our digital society. This consists of four foundations of trust—the commitment to be *honest* about data practices, the importance of *discretion* in data usage, the need for *protection* of personal data against outsiders, and the overriding principle of *loyalty* to the people whose data is being used, so that it is data and not humans that become exploited. We argue that we must recognize the importance of information relationships in our networked, data-driven society. There exist substantial incentives already for digital intermediaries to build trust. But when incentives and markets fail, the obligation for promoting trust must fall to law and policy. The first-best privacy future will remain one in which privacy is safeguarded by law, as well as private ordering and self-help.

I. OBFUSCATION AND THE INDIVIDUALISTIC STORY OF PRIVACY

Obfuscation aims to spark a rebellion by the weak and powerless using whatever tools are available for resistance. Despite such an insurrectionist objective, Brunton and Nissenbaum surprisingly accept the terms of the privacy debate as they are. This capitulation is the source of the book’s greatest contributions as well as its most significant limitation. By accepting the status quo and leaving loftier challenges to privacy theory for another day, Brunton and Nissenbaum have the freedom to seek out realistic and practical privacy strate-

16. E.g., DAVID BRIN, *THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM?* (1999); Thomas Friedman, *Four Words Going Bye-Bye*, N.Y. TIMES (May 21, 2014), <http://www.nytimes.com/2014/05/21/opinion/friedman-four-words-going-bye-bye.html> [<http://perma.cc/CCP3-ALQZ>] (declaring that “privacy is over”). But see Neil M. Richards, *Four Privacy Myths, in A WORLD WITHOUT PRIVACY: WHAT LAW CAN AND SHOULD DO?* 33 (Austin Sarat ed., 2015) (debunking the “Privacy is Dead” myth); A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461 (2000).

gies that can be effective even if they are flawed or only modestly effective. But this clear-eyed realism still buys into the framework that dominates almost all our modern thinking about personal information—that privacy is largely an individual pursuit. Before we address the limitations of *Obfuscation*, let us first review its principal arguments and most noteworthy contributions.

A. *The Appeal of Obfuscation*

Obfuscation is one part a saboteur's user manual and one part an exploration of the ethics of that sabotage. The privacy stories that dominate our news headlines show no likelihood of dying down, and they have left people bewildered and worried. This book offers one way out.

1. *Obfuscation's Argument*

Brunton and Nissenbaum explicitly aim to start an obfuscation revolution.¹⁷ They seek to empower people with the potential of digital technologies to conceal, disrupt, and fight back against the exposure and manipulation of our data. They explain that “[t]he focus of our limited revolution is on mitigating and defeating present-day digital surveillance” using ready-to-hand components.¹⁸ They tout obfuscation as “a lexicon of ways to put some sand in the gears, to buy time, and to hide in the crowd of signals.”¹⁹ There is much to like in this proposal, in particular its rebuttal of simplistic notions of privacy and its offer of a weapon to those most in need of protection from the power imbalances of our digital age.

In their Introduction, the authors lay out their conceptualization of obfuscation as “the deliberate addition of ambiguous, confusing, or misleading information to interfere with surveillance and data collection.”²⁰ The first and prototypical example of obfuscation in the book is the use of “chaff” by pilots during the Second World War to frustrate military radar and weapon targeting systems by giving off a confusing and overwhelming number of signals, all but one of them false.²¹ The goal of *Obfuscation* is to explicate that concept as a starting point for resistance and revolution by individuals or groups of individ-

17. BRUNTON & NISSENBAUM, *supra* note 3, at 1 (“We mean to start a revolution with this book. But not a big revolution—at least, not at first.”).

18. *Id.*

19. *Id.* at 2.

20. *Id.* at 1 (emphasis omitted).

21. *Id.* at 8.

uals against the surveillance and data collection that exist within asymmetrical power relationships.

Part I of the book develops a common vocabulary of obfuscation to better understand how the technique can be generalized into a pattern.²² The authors argue that while the techniques of obfuscation can vary, they all share the attempt to thwart or frustrate the observation of others, frequently by feeding bad information towards those corporate and government watchers.²³ Brunton and Nissenbaum use this Part to describe how we can “create many plausible, ambiguous, and misleading signals within which the information we want to conceal can be lost.”²⁴ For example, they describe the collective deployment by many people of one pseudonym to confound data collection and poker players using “false tells” to trick trained observers.²⁵ In the digital age, these techniques can include the use of software that adds hundreds of false Google search queries to each legitimate one, hiding the user’s true interests in a cloud of gibberish to thwart the building of a profile of that user.²⁶

Part II of *Obfuscation* tackles the hard ethical and political problems posed by its theory, as well as questions about obfuscation’s purposes and the circumstances under which obfuscation is useful.²⁷ Brunton and Nissenbaum draw on philosophical literature to argue that while some uses of obfuscation may be problematic, other uses (particularly by Internet users resisting surveillance) can survive a searching ethical inquiry.²⁸ They maintain that obfuscation is not merely a useful “weapon of the weak,” but one that has significant potential to change the terms of the privacy debate by empowering individuals who are vulnerable to surveillers and data collectors that have enormous advantages in resources and ability.²⁹

We argue that the central arguments and contributions of *Obfuscation* are best understood through the lens of the modern individualistic conceptualization of privacy, a lens that they implicitly adopt for individuals or groups of individuals acting together.³⁰ This notion of privacy revolves around principles of autonomy and control. It conceives of us as each individually responsible for

22. See *id.* at 1-42.

23. *Id.* at 7.

24. *Id.*

25. *Id.* at 15-16.

26. *Id.* at 13-14.

27. See *id.* at 45-95.

28. *Id.* at 64-65.

29. *Id.* at 55-58.

30. See *e.g., id.* at 85 (“How can obfuscation work for me and my particular situation?”).

protecting our own little privacy islands. It is the dominant story of modern privacy law and policy³¹ and is reflected in the examples and rhetoric in *Obfuscation*. Brunton and Nissenbaum make the best of this framework by helpfully focusing on practical defenses that leverage transaction costs and surveillers' practical, financial, and cognitive limitations to frustrate data collection and comprehension.

2. *A Pragmatic Rebuttal to Overly Simplistic Notions of Privacy*

Embedded in the heart of *Obfuscation* is pragmatism regarding the kind of privacy people can actually expect and a celebration of what we think can best be called a "good enough" privacy. The authors explicitly jettison ideal notions of privacy, recognizing that sometimes even temporary, incomplete privacy interventions can be enough to serve people's needs.³² They note that in many situations, optimal systems for privacy, like encryption, are not possible, accessible, or desirable.³³ People often need to be at least partially or temporarily visible, and their information must be somewhat comprehensible to others to interact in the world. The act of being online for any activity usually requires a certain kind of visibility.

Enter obfuscation. The authors argue that "[t]he strength of an obfuscation approach isn't measured by a single objective standard (as safes are) but in relation to a goal and a context: to be *strong enough*."³⁴ Instead of making someone completely invisible, obfuscation can buy them time before detection. Instead of erasing one's tracks, obfuscation can provide plausible deniability and disrupt the ability of surveillers and data collectors to profile or otherwise single out individuals. When people obfuscate, they raise the transaction cost of effective surveillance and data collection. This can temporarily delay surveillance and perhaps even discourage surveillance and data collection efforts alto-

31. See e.g., *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, WHITE HOUSE 9 (Feb. 23, 2012), <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf> [<http://perma.cc/2EEV-ZFCZ>] ("To meet this challenge, the Consumer Privacy Bill of Rights carries FIPPs [Fair Information Practice Principles] forward in two ways. First, it affirms a set of consumer rights that inform consumers of what they should expect of companies that handle personal data. The Consumer Privacy Bill of Rights also recognizes that consumers have certain responsibilities to protect their privacy as they engage in an increasingly networked society.")

32. BRUNTON & NISSENBAUM, *supra* note 3, at 48, 57-58.

33. *Id.* at 57.

34. *Id.* at 87.

gether. Obfuscation does not promise protection—only the possibility of minimized risk and an outlet for protest.

The pragmatism of *Obfuscation* comes just at the right time in our modern privacy debate. Because there is no set definition of privacy, our resulting policy has latched onto overly idealistic notions of privacy that do not scale well. Thinking about privacy as individual control over information has resulted in myriad boilerplate contracts, and even privacy-conscious persons may not have enough time to read through all of the privacy policies they wish to opt out of.³⁵ Additionally, thinking about privacy in terms of an individual's secrets fails to cover information we want to share with some, but not all.³⁶ Secrecy and control are too simplistic and unforgiving. While obfuscation lends some support to the same individualistic framework that equates privacy with control, it adeptly rebuts the misguided and myopic notion of privacy as secrecy.

One of the most common fallacies employed in our modern privacy discourse is the belief that once information is shared with others, it ceases to be private, and many scholars, including Nissenbaum, have critiqued this “secrecy paradigm” or “public/private dichotomy.”³⁷ Yet this false binary persists in our rhetoric, law, and policy. One judge wrote that because Internet users voluntarily share information with others, privacy on social media is “wishful thinking.”³⁸

Simplistic and myopic notions of privacy are dangerous. They compel harsh laws that elevate form over function in the name of advancing an unreal-

35. Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S 543, 565-68 (2008); *250,000 Words of App Terms and Conditions*, NORWEGIAN CONSUMER COUNCIL (May 24, 2016), <http://www.forbrukerradet.no/side/250000-words-of-app-terms-and-conditions> [http://perma.cc/RK5B-4E5N] (“The Norwegian Consumer Council has downloaded the terms of service and privacy policies for apps that you would find on an ‘average’ mobile. Together they exceed the New Testament in length—and would take more than 24 hours to read out loud.”).

36. Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 923-25 (2005).

37. See HELEN NISSENBAUM, *PRIVACY IN CONTEXT* 91 (2010) [hereinafter NISSENBAUM, *PRIVACY IN CONTEXT*] (critiquing the “public/private” dichotomy); DANIEL J. SOLOVE, *THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE* 42-43 (2004) (critiquing the “secrecy paradigm”); Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 136-37 (2004) [hereinafter Nissenbaum, *Privacy as Contextual Integrity*]; Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 L. & PHIL. 559, 570 (1998) [hereinafter Nissenbaum, *Protecting Privacy*]; Strahilevitz, *supra* note 36, at 924.

38. *Romano v. Steelcase Inc.*, 907 N.Y.S.2d 650, 657 (Sup. Ct. 2010) (quoting Dana L. Fleming & Joseph M. Herlihy, *What Happens When the College Rumor Mill Goes Online? Privacy, Defamation and Online Social Networking Sites*, BOS. B.J. 16, 16 (Jan./Feb. 2009)).

istic and unattainable privacy ideal. This happens at the expense of engaging in the kind of calculus necessary to identify accurately significant privacy problems and balance legal and technical responses with other concerns and values.³⁹ Nissenbaum has elsewhere proposed a theory of privacy as “contextual integrity”⁴⁰ to provide more nuance to the notion of privacy, and this book further advances that goal.⁴¹

The concept of obfuscation represents an important challenge to myopic notions of privacy. It demonstrates that even perceived “weak” notions of privacy can still be valuable. We see the most significant contribution of *Obfuscation* as a lucid embrace of the centrality of the practical, cognitive, and financial limitations of surveillers and data collectors. The authors recognize that sometimes people must be visible to others in order to function in a modern society.⁴² Yet even when people are *necessarily visible*, it is possible to preserve some sense of privacy by leveraging the structural protections and the limited abilities of those who would watch us or collect our data.⁴³ Brunton and Nissenbaum spend much of the book demonstrating that even though obfuscation cannot provide absolute or robust privacy, in many circumstances it might be able to frustrate data collectors enough to give people the small amount of privacy they need.⁴⁴

In focusing on structural and practical privacy protections, *Obfuscation* joins the growing chorus of voices exploring concepts like obscurity, friction, inefficiency, and structural privacy rights, which look to the relative ease or difficulty of conducting privacy-protective activities.⁴⁵ These concepts are distinct yet ul-

39. See sources cited *supra* note 13.

40. NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 37, at 6-7; Nissenbaum, *Privacy as Contextual Integrity*, *supra* note 37, at 124; Nissenbaum, *Protecting Privacy*, *supra* note 37, at 581-82.

41. BRUNTON & NISSENBAUM, *supra* note 3, at 45 (“The house of privacy has many rooms. Some are concerned with the integrity of family life, some with state oppression (now or in the future), some with utility and value of data, and some with a true inner self that can only emerge in anonymity, and many have intersections and communicating doors.”).

42. *Id.* at 85.

43. *Id.* at 59 (“There are situations in which many people may periodically find themselves obligated to give things up, with uncertain consequences and without a clear mechanism for re-asserting control—moments when obfuscation can play a role, providing not a comprehensive military-grade data-control solution (though it may be usefully combined with such a solution) but an intuitive approach to throwing up a bit of smoke.”).

44. *Id.* (“Martyrdom is rarely a productive choice in a political calculus; as straightforward as the rational-actor binary of opting in or out may be, a choice between acceptance and dropping off the edge of the (networked) earth isn’t really a choice at all.”).

45. See Woodrow Hartzog & Evan Selinger, *Surveillance as Loss of Obscurity*, 72 WASH. & LEE L. REV. 1343, 1355 (2015) [hereinafter Hartzog & Selinger, *Surveillance*]; Woodrow Hartzog &

timately all look to the transaction costs associated with finding, understanding, using, or sharing information.

In economic theory, transaction costs refer to the kinds of expenses necessary to engage in market exchanges.⁴⁶ The concept is invaluable because our sense of privacy is in part a function of decisions made by corporations and government actors that have limited resources to spend on information collection and disclosure. The strategy of obfuscation is harmonious with the broader concept of obscurity, which is another way of using existing friction and other structural constraints to secure privacy.⁴⁷ Obscurity is the idea that when information is hard or unlikely to be found or understood, it is, to some degree, safe.⁴⁸ “Friction” is the idea that transaction costs can be used as a lever to make information more or less accessible, according to desired values of openness or privacy.⁴⁹ Finally, structural constraints are regulators of privacy-corrosive behavior that prevent surveillance and data collection or use through

Frederic Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV. 1, 4 (2013) [hereinafter Hartzog & Stutzman, *The Case for Online Obscurity*]; Woodrow Hartzog & Frederic Stutzman, *Obscurity by Design*, 88 WASH. L. REV. 385, 388 (2013) [hereinafter Hartzog & Stutzman, *Obscurity by Design*]; William McGeeveran, *The Law of Friction*, 2013 U. CHI. LEGAL F. 15, 18; Neil M. Richards, *The Perils of Social Reading*, 101 GEO. L.J. 689, 692 (2013); Evan Selinger & Woodrow Hartzog, *Obscurity and Privacy*, in ROUTLEDGE COMPANION TO PHILOSOPHY OF TECHNOLOGY (Joseph Pitt & Ashley Shew eds., forthcoming 2017), <http://ssrn.com/abstract=2439866> [<http://perma.cc/VN3R-FGBU>]; Harry Surden, *Structural Rights in Privacy*, 60 SMU L. REV. 1605, 1607 (2007); Woodrow Hartzog & Evan Selinger, *Obscurity: A Better Way To Think About Your Data Than ‘Privacy,’* ATLANTIC (Jan. 17, 2013) [hereinafter Hartzog & Selinger, *A Better Way*], <http://www.theatlantic.com/technology/archive/2013/01/obscurity-a-better-way-to-think-about-your-data-than-privacy/267283> [<http://perma.cc/FA9K-B2TQ>].

46. See, e.g., Alexandra Benham & Lee Benham, *The Costs of Exchange*, in THE ELGAR COMPANION TO TRANSACTION COST ECONOMICS 107, 107-08 (Peter G. Klein & Michael E. Sykuta eds., 2010); Douglas W. Allen, *Transaction Costs*, SIMON FRASER U. (1999), <http://www.sfu.ca/~allen/allentransactioncost.pdf> [<http://perma.cc/8UZS-6QN5>].
47. For sources exploring obscurity theory, see Hartzog & Selinger, *Surveillance*, *supra* note 45; Hartzog & Stutzman, *The Case for Online Obscurity*, *supra* note 45, at 4; Hartzog & Stutzman, *Obscurity by Design*, *supra* note 45, at 388; Selinger & Hartzog, *supra* note 45; and Hartzog & Selinger, *A Better Way*, *supra* note 45.
48. See sources cited *supra* note 47.
49. McGeeveran, *supra* note 45, at 18 (“In the physical world, too much friction can impede movement or even start fires, but too little would cause objects to slide off tables and cars off roads. The key to online disclosures also turns out to be the correct amount of friction, not its elimination.”); Richards, *supra* note 45, at 692 (“[S]ocial reading and frictionless sharing menace our intellectual privacy.”).

technological or physical barriers in the world.⁵⁰ Obfuscation is capable of being used to obscure through “noise,” to add friction through forced work on behalf of collection systems and recipients, and to leverage structural protections like limitations on automation capabilities. As such, it is a welcome contribution to the growing pragmatic approach to modern privacy, which is sensitive to the practical limitations of people and systems in identifying issues, assessing risk, and solving problems. One of *Obfuscation*'s greatest virtues is its recognition that pretty good privacy is often good enough.

3. *The Need for Privacy Outside Trustworthy Relationships*

Another strength of *Obfuscation* is that it equips people with another means of defense when safe relationships are not an option for sustainable data exchange. Although people need others to flourish, some data collectors are not trustworthy. The history of consumer protection is littered with scammers and others who would exploit us and our data.⁵¹ Electoral campaigns, advertisement networks, and other organizations that care more about short-term gains from data than long-term sustainable relationships also have little incentive to be trustworthy data stewards.⁵² Obfuscation, from this perspective, is a response to, and thus a product of, distrust.

Additionally, others that might collect people's personal information or surveil them have no relationships with the objects of their surveillance whatsoever. For example, many surreptitious surveillers like Peeping Toms, nosy neighbors, and government intelligence agents have no relationship with those they surveil. Data brokers usually do not have a direct relationship with the subjects of the data either.⁵³ Concepts like big data and open data presuppose downstream uses of data outside what we traditionally think of as information

50. Surden, *supra* note 45, at 1607 (“Structural constraints are regulators of behavior that prevent conduct through technological or physical barriers in the world. These barriers make certain conduct costly.”).

51. See generally CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW & POLICY (2016) (giving numerous examples of privacy scams investigated and punished by the Federal Trade Commission (FTC)).

52. See Ira S. Rubinstein, *Voter Privacy in the Age of Big Data*, 2014 WIS. L. REV. 861.

53. See Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595 (2004). These companies collect information from other data collectors that have a more direct relationship with the data subjects, such as government and social media. *Id.*

relationships.⁵⁴ It makes little sense to talk about the importance of relationships in these contexts. And it is here where obfuscation can matter most.

Obfuscation is most useful as a weapon when our backs are against the wall. In an increasingly nationalistic and paranoid world stage, governments are dramatically increasing surveillance, particularly of minority and vulnerable populations.⁵⁵ Obfuscation and more robust privacy strategies like using encryption will be invaluable for resistance. States are the ultimate dominant actors in asymmetrical power relationships. When the vulnerable are out of options, obfuscation is far better than resignation. The authors point out that obfuscation can also be a tool for protest and, if nothing else, a way to express displeasure, whether it ends up effectively protecting people or not. One of the most prominent examples of obfuscation in the wake of then-candidate Donald Trump's consideration of a Muslim registry was an organized effort by non-Muslims to register.⁵⁶ Doing so would add noise to the database and express protest and solidarity at the same time.

As a tool of expression and of last resort, obfuscation has much to commend it. But obfuscation can only be asked to do so much work. As we explain in greater detail below, it would be unwise to saddle it with heavy lifting. Technology alone cannot save us. Like the notion of obfuscation itself, privacy-friendly technologies unsupported by law and policy can only temporarily stave off the corrosive power of overreaching government and corporate surveillance. Technology is necessary to help create an environment for human flourishing.

54. See generally Symposium, *Privacy and Big Data*, 66 STAN. L. REV. ONLINE 25 (2013) (providing examples of big data uses outside information relationships).

55. Andrew D. Selbst, *Disparate Impact in Big Data Policing* (Aug. 5, 2016) (unpublished manuscript), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2819182 [<http://perma.cc/GK4C-F4GP>]; Clare Garvie, Alvaro M. Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, GEO. L. CTR. ON PRIVACY & TECH. (2016), <http://www.perpetuallineup.org/sites/default/files/2016-10/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law.pdf> [<http://perma.cc/CXT7-9YWG>]; Zack Whittaker, *Britain Has Passed the 'Most Extreme Surveillance Law Ever Passed in a Democracy'*, ZDNET (Nov. 17, 2016, 8:00 AM GMT), <http://www.zdnet.com/article/snoopers-charter-expansive-new-spying-powers-becomes-law> [<http://perma.cc/2XAV-X4VR>].

56. Heather Dockray, *There's Already a Plan To Fight Trump's Muslim Registry, and It's Brilliant*, MASHABLE (Nov. 17, 2016), <http://mashable.com/2016/11/17/ways-to-fight-muslim-registry> [<http://perma.cc/9NNL-QKBX>]; Taj James, *I Pledge To Register as Muslim If Trump Is Allowed To Take Power and Starts a Registry*, MOVEON PETITIONS, <http://petitions.moveon.org/sign/i-pledge-to-register> [<http://perma.cc/AX7F-RJ5S>]. But see *Stopping the 'Muslim Registry': A Serious Approach*, SAMIR CHOPRA (Nov. 17, 2016), <http://samirchopra.com/2016/11/17/stopping-the-muslim-registry-a-serious-approach> [<http://perma.cc/99UC-Y9YB>].

But it is not sufficient. The sustainable path to fixing a broken world is through social movements, participation in the democratic political process, and the rule of law.

B. Privacy Islands

Most American conversations about privacy follow a particular form, one that is followed in venues ranging from office water cooler chats to testimony before federal agencies: privacy is under threat because our modern digital society runs on human data. For example, the smartphones that most Americans carry with them are constantly collecting information about their location, reading habits, and contacts. Personal data has enormous potential to make the world a better place and has already become “the new oil,” the fuel on which much economic activity runs.⁵⁷ However, the subjective privacy preferences of individuals must be balanced against data-based innovation. But if people want to protect their data, the dominant theory argues that they should help themselves. They should choose to do business with companies who share their values, and they should read privacy policies and select privacy-protective options in online platforms. Control over data and surveillance is the paramount value and is often seen as the very definition of privacy.⁵⁸ Law has a role in this world, but it is limited to effectuating that control or protecting consumers

-
57. See generally Dennis D. Hirsch, *The Glass House Effect: Big Data, the New Oil, and the Power of Analogy*, 66 ME. L. REV. 373 (2014) (illustrating and exploring the consequences of the “privacy is the new oil” metaphor).
58. See ANNE WELLS BRANSCOMB, WHO OWNS INFORMATION? 3 (1994); DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 1, 24 (2007) (“One of the most predominant theories of privacy is that of control over personal information.”); ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967) (“Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.”); Randall P. Bezanson, *The Right to Privacy Revisited: Privacy, News, and Social Change 1890-1990*, 80 CALIF. L. REV. 1133, 1135 (1992) (“I will advance a concept of privacy based on the individual’s control of information . . .”); Charles Fried, *Privacy*, 77 YALE L.J. 475, 482-83 (1968) (“Privacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves.”); Ian Goldberg et al., *Trust, Ethics, and Privacy*, 81 B.U. L. REV. 407, 418 (2001) (defining “privacy” in terms of “a person’s ability to control the flow of his own personal information”); Oscar M. Ruebhausen & Orville G. Brim, Jr., *Privacy and Behavioral Research*, 65 COLUM. L. REV. 1184, 1189 (1965) (stating that the “essence of privacy” is the “freedom of the individual” to decide which personal information will be “shared with or withheld from others”).

against data practices that are “creepy” or demonstrably (usually financially) harmful.⁵⁹

This is the dominant rhetoric of privacy: a conflict between privacy and progress to be resolved through individual consumer choice. Like a lot of worldviews, this story does ideological and political work. The dominant view gave birth to the “notice and choice” regime that molded our current data protection regime.⁶⁰ It provides a justification for the maligned “third party doctrine” in Fourth Amendment law, which puts the risk of disclosure to the government on the person who shares information with others.⁶¹ It encourages us to think about information as being either “public” and known to all or “private” and known only to one person, rather than thinking about the variations between these two extremes that happen when information is shared in a relationship.⁶² The dominant narrative even underlies the “nothing to hide” fallacy used to excuse surveillance, as if the only relevant factor for surveillance were

59. Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy and Shifting Social Norms*, 16 YALE J.L. & TECH. 59, 60 (2013) (“[I]ntuitions and perceptions of how our social values should align with our technological capabilities are highly subjective. And, as new technologies strain our social norms, a shared understanding of that alignment is even more difficult to capture. The word ‘creepy’ has become something of a term of art in privacy policy to denote situations where the two do not line up.”).

60. For years, as long as the data subject was given notice of data collection but “chose” to disclose anyway, data collectors largely operated without restriction. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 592 (2014).

61. Under the third party doctrine, “information shared even with trusted ‘third parties’ loses a reasonable expectation of privacy under the Fourth Amendment, and with it, the protection of the warrant requirement.” Neil M. Richards, *The Third-Party Doctrine and the Future of the Cloud*, 94 WASH. U. L. REV. (forthcoming 2017) (manuscript at 3) (on file with authors). The doctrine has been a source of controversy. See, e.g., Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009) (arguing that critics of the third party rule overlooked its advantages and have overstated its weaknesses). But see Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1230 (2016) (arguing against the third party doctrine’s assumption that when people disclose information to a third party, the disclosers have “no reasonable expectation of privacy in the information” and proposing, instead, that many third parties “owe us fiduciary duties or duties of confidentiality”); Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611, 611, 616 (2015) (arguing that the third party doctrine should be limited where a person shares information with an “information fiduciary”); Richards, *supra* (manuscript at 4, 6) (arguing that the third party doctrine is inconsistent with both ancient principles and modern contexts of Fourth Amendment law).

62. See Woodrow Hartzog, *There Is No Such Thing as “Public” Data*, SLATE (May 19, 2016, 9:15 AM), http://www.slate.com/articles/technology/future_tense/2016/05/okcupid_s_data_leak_shows_there_s_no_such_thing_as_public_data.html [http://perma.cc/C443-6AGQ].

the bad secrets you may keep.⁶³ But at bottom, no matter how it is phrased, the responsibility for protecting our privacy under the dominant story ultimately rests upon each of us as individuals. Under this view, we are all privacy islands.

That individualism and isolationism are the dominant frame of privacy rhetoric and policy should come as no surprise. Privacy is only occasionally conceptualized as a group or even a social project.⁶⁴ Although the Anglo-American common law has a long history of protecting information in confidential relationships, privacy law in America as a self-conscious endeavor dates to Samuel Warren and Louis Brandeis's famous 1890 article *The Right To Privacy*.⁶⁵ That article, written to vindicate the particular injury of unwanted attention by the press, called for the recognition of a tort of invasions of privacy—emotional or dignitary injuries to the “inviolable personalit[ies]” of individual plaintiffs.⁶⁶ The article famously influenced the course of American privacy law, leading to the establishment of the four “privacy torts” by William Prosser⁶⁷ and the embedding of privacy rights in the core of Fourth Amendment protec-

63. See generally DANIEL J. SOLOVE, *NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY* (2011) (critiquing the “nothing to hide” fallacy).

64. There have been notable exceptions, however. See, e.g., EDWARD J. BLOUSTEIN, *INDIVIDUAL AND GROUP PRIVACY* (1978); JULIE E. COHEN, *CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE* (2012); Joshua A.T. Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 *DUKE L.J.* 385 (2015); Rafi M. Goldberg et al., *Trust in Internet Privacy and Security and Online Activity* (Nat'l Telecomm. & Info. Admin., Working Paper, Aug. 31, 2016), <http://ssrn.com/abstract=2757369> [<http://perma.cc/ZBG7-4ZZC>]; Robert H. Sloan & Richard Warner, “I’ll See”: How Surveillance Undermines Privacy by Eroding Trust (Mar. 14, 2016) (unpublished manuscript), <http://ssrn.com/abstract=2747435> [<http://perma.cc/M4ND-F59L>]. See generally SOCIAL DIMENSIONS OF PRIVACY: INTERDISCIPLINARY PERSPECTIVES (Beate Roessler & Dorota Mokrosinska eds., 2015) (offering interdisciplinary commentaries on the social aspects of privacy); Dennis D. Hirsch, *Privacy, Public Goods, and the Tragedy of the Trust Commons: A Response to Professors Fairfield and Engel*, 65 *DUKE L.J. ONLINE* 67 (2016) (expanding on the work of Professors Joshua Fairfield and Christoph Engel, *supra*); Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 *B.C. L. REV.* 741, 741 (2008) (applying freedom of association rights to the issue of network surveillance); Ari Ezra Waldman, *Privacy as Trust: Sharing Personal Information in a Networked World*, 69 *U. MIAMI L. REV.* 559, 561 (2015) (arguing that privacy law should protect “relationships of trust”).

65. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 *HARV. L. REV.* 193 (1890). But see Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 *GEO. L.J.* 123, 125 (2007) (arguing that, contrary to conventional wisdom, “Warren and Brandeis did not invent the right to privacy . . . but instead charted a new path for American privacy law”).

66. Warren & Brandeis, *supra* note 65, at 205; see RICHARDS, *supra* note 12, at 15-26.

67. William L. Prosser, *Privacy*, 48 *CALIF. L. REV.* 383, 388-89 (1960); see Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 *CALIF. L. REV.* 1887, 1924 (2010).

tions.⁶⁸ But by using a tort model of injury to individual plaintiffs as the essence of privacy law, Warren and Brandeis also helped move both the law and American notions of privacy away from the recognition of confidentiality—privacy in relationships of trust—and toward atomistic, individualistic conceptions of privacy outside recognized relationships.⁶⁹

This phenomenon becomes clearer when we look at the state of privacy law today. In modern American law, individual rights of privacy are at the center of virtually all privacy and surveillance laws, but such rights are largely agnostic about the relationship between the data subject and data collector.⁷⁰ Private rights of action created by statute are a major form of privacy enforcement in areas as wide-ranging as wiretapping law, government records, and video privacy.⁷¹ Although there is growing public enforcement of consumer privacy rights in the commercial context through investigations by the Federal Trade Commission (FTC) under its Section 5 Unfair and Deceptive Trade Practices authority, that authority is also premised upon injury to consumers or competition from deception or unfair trade practices.⁷² Similarly, one of the major obstacles to privacy regulation through litigation is the requirement that privacy plaintiffs demonstrate an individually traceable “injury in fact” to satisfy constitutional standing or related doctrines.⁷³ The imposition by courts of these requirements rooted in notions of individual rights and injuries cognizable only in individual terms have ossified privacy rights in areas as diverse as government surveillance of First Amendment-protected activities and privacy rights created by statute.⁷⁴

Missing from the individual view of privacy and security law is the more nuanced understanding that in a connected society, privacy is not just an individual concern, but a major building block for society as a whole. This is privacy’s trust gap. Our dominant legal framework is frequently insufficient or inca-

68. See RICHARDS, *supra* note 12, at 145.

69. See Richards & Solove, *supra* note 65.

70. See PRISCILLA M. REGAN, *LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY* (1995).

71. Privacy Act of 1974, 5 U.S.C. § 552a (2012); Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2012); Video Privacy Protection Act, 18 U.S.C. § 2710 (2012).

72. See HOOFNAGLE, *supra* note 51.

73. Julie E. Cohen, *Information Privacy Litigation as Bellwether for Institutional Change*, 66 DEPAUL L. REV. (forthcoming 2017), <http://ssrn.com/abstract=2833922> [<http://perma.cc/25HR-JCAS>]; see, e.g., *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016) (discussing statutory law); *Clapper v. Amnesty Int’l USA*, 133 S. Ct. 1138 (2013) (discussing constitutional law).

74. Cf. *Spokeo*, 136 S. Ct. at 1544–45; *Clapper*, 133 S. Ct. at 1142–43; *Laird v. Tatum*, 408 U.S. 1, 13 (1972) (imposing such requirements in the data-gathering context).

pable of comprehending the real and important injuries to the trust we need to flourish in our networked, digital society. If privacy is just a matter of individual concern, behaviors and forms of surveillance that breed suspicion raise no cognizable legal issues, even though they undermine our civil liberties or our willingness to connect to others in ways that produce social value. Privacy's trust gap thus contributes to the sense of fatalism dominating our rhetoric and hindering our policy, particularly as the law conceives of us all as individuals on our own privacy islands, rather than emphasizing our interconnections. While *Obfuscation* offers a useful weapon to those with little other power to avoid data collection and surveillance, the weapon is not only rooted in individual actions under the privacy islands model, but also reinforces and widens the trust gap.

II. OBFUSCATION REQUIRES TRUSTWORTHY ALLIES

Obfuscation is offered as a weapon of the weak, those on the “wrong” end of asymmetrical power relationships. But it is precisely the weak and vulnerable who need help from other people, organizations, and technologies in defending themselves. Thus, they cannot function effectively as islands in the way that the dominant individualistic theory of privacy would require.

While some examples of obfuscation that Brunton and Nissenbaum provide are entirely within an individual's control (such as speaking in general terms or planting false signals), few obfuscation attempts in the digital world, where most data is collected, are truly solitary affairs. Online attempts at obfuscation usually require the cooperation of (and thus, vulnerability to) at least one of two different kinds of parties: designers and confederates.

A. Obfuscation's *Call for a Lonely Revolution*

Unfortunately, the proposed obfuscation revolution looks to be a lonely one. *Obfuscation* accepts the framework of privacy individualism, and both obfuscation and privacy are conceived in individualistic terms, largely through the lens of self-defense. Obfuscation is proposed as an individual pursuit, a tactic to be employed by people seeking to create or preserve some notion of privacy for themselves.

The authors provide numerous examples of individual obfuscations, like poker players giving “false tells” to avoid being predictable and attorneys playing loud audio files of polyphonic “babbling” to confound eavesdropping.⁷⁵ They highlight how people can change out SIM cards to avoid being linked to

75. BRUNTON & NISSENBAUM, *supra* note 3, at 15, 21.

one specific phone or use deliberately vague language to frustrate data analytics.⁷⁶ As a revolution, obfuscation seems to merely ask that we each fight surveillance alone, even if sometimes we fight it alone, together.

What is missing from this account is the importance of other people and institutions in effectuating obfuscation. Brunton and Nissenbaum explicitly offer obfuscation to those on the weak end of asymmetrical power relationships. But they seemingly treat all asymmetrical power relationships as adversarial. That will not always be the case. For example, Apple aligned itself with its customers in fighting the FBI over the security of its phone.⁷⁷ Microsoft aligned itself with its customers in resisting search warrants for information stored outside the United States.⁷⁸

Adversarial attitudes within information relationships are not sustainable. If we all were to pollute the information economy, we would also counteract the usefulness of personal disclosure. Disclosing our health data to the right people can help us get and stay healthy. Disclosing our financial information can help us access credit and accumulate wealth. Agreeing to certain kinds of surveillance might gain us entry to places that require elevated levels of security. People and organizations need each other to participate in the modern world, which means they must work together.

Brunton and Nissenbaum recognize this reality in a section titled “The Fantasy of Opting Out.”⁷⁹ Credit, health insurance, jobs, travel and entertainment all require trust in other parties. Too often, the individualistic account of obfuscation glosses over the importance of these relationships. What would happen if people regularly obfuscated their health information to their doctors and their financial information to credit institutions? We would probably be less healthy and wealthy (and wise) because diagnosis and risk assessment would become very difficult for those seeking to work with us. While some surveillers and data collectors have little concern for people’s well-being, the costs of obfuscation vary wildly amongst different kinds of information relationships.

There is room for debate on the efficacy of obfuscation.⁸⁰ But our critiques concern the individualistic conceptualization of obfuscation itself. First, as we

76. *Id.* at 18-19, 30-31.

77. See *supra* note 15 and accompanying text.

78. *In re Warrant To Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197 (2d Cir. 2016).

79. BRUNTON & NISSENBAUM, *supra* note 3, at 53.

80. In addition to the authors themselves, other critics have noted the ethical issues inherent in obfuscation. See Rob Horning, *Hide and Seek: The Problem with Obfuscation*, L.A. REV. BOOKS (Nov. 10, 2015), <http://lareviewofbooks.org/article/hide-and-peek-the-problem-with-obfuscation> [<http://perma.cc/3JCJ-WSZC>]; Evan Selinger, *Internet Privacy: Stepping*

have seen with other regimes designed to give people “control” over their personal information, “empowerment” is often the positive spin placed upon the structural reallocation of privacy risks.⁸¹ Under this story, when we are “empowered” to exercise control over how our information is collected and used, we bear the responsibility of bad choices, even when our good options are limited or nonexistent. These situations can include being bound by voluminous, incomprehensible, and constantly changing privacy policies.⁸² Or they can include liability for harm resulting from our inability to manage a bewildering number of privacy settings or passwords,⁸³ or our failure to opt out of data collection by information brokers or online surveillance companies we may not have been aware even existed, a phenomenon Brunton and Nissenbaum themselves marvelously term “the fantasy of opting out.”⁸⁴ In these contexts, “empowerment” and “control” can be (and have been) used by the powerful to get their way while avoiding substantive legal obligations with respect to personal data. And they leave individuals alone and isolated to solve this problem themselves or bear its costs.

Up Our Self-Defense Game, L.A. REV. BOOKS (Nov. 10, 2015), <http://lareviewofbooks.org/article/internet-privacy-stepping-up-our-self-defense-game> [<http://perma.cc/MX73-TKHA>]. The authors themselves anticipate many of these objections, *see, e.g.*, BRUNTON & NISSENBAUM, *supra* note 3, at 71 (“Whether means [of obfuscating] are acceptable may rest on numerous ethical factors but, as often, may depend on the interaction of ends with various contingent and contextual factors, whose consideration resides in the zone of the political.”), and devote a substantial portion of the book to defending the ethics of obfuscation, *see id.* at 63-83.

81. Woodrow Hartzog, *Website Design as Contract*, 60 AM. U. L. REV. 1635, 1636-37, 1652 (2011); Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control over Personal Information?*, 111 PA. ST. L. REV. 587, 588 (2007); Joel R. Reidenberg et al., *Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding*, 30 BERKELEY TECH. L.J. 39 (2015); Joel R. Reidenberg et al., *Privacy Harms and the Effectiveness of the Notice and Choice Framework*, 11 I/S 485, 487-88 (2015).
82. *See* McDonald & Cranor *supra* note 35, at 543, 565-68 (conceptualizing the time it takes a consumer to read a website's privacy policy as a “micropayment” and calculating the total annual costs consumers would incur should they read the privacy policy of each website they visit).
83. *See* Daniel J. Solove & Woodrow Hartzog, *Should the FTC Kill the Password? The Case for Better Authentication*, 14 Privacy & Security L. Rep. (BNA) 1353, at *1 (July 27, 2015) (arguing that passwords are a weak authentication method because “[p]eople select poor passwords, reuse them on many sites and have difficulty remembering them”); Maritza Johnson, Serge Egelman & Steven M. Bellovin, *Facebook and Privacy: It's Complicated*, SYMP. ON USABLE PRIVACY & SECURITY (SOUPS) 10 (2012), http://www.cs.columbia.edu/~smb/papers/a9_Johnson.pdf [<http://perma.cc/ZDZ8-J939>] (stating that Facebook users often fail to use the site's available privacy settings to achieve a stated desire to block profile content from certain members of their friend networks).
84. BRUNTON & NISSENBAUM, *supra* note 3, at 53-55.

We should be careful about an over-enthusiastic adoption of “privacy self-defense” because it places us in a defensive posture and allows third parties to escape responsibility for protecting and respecting people and their personal information. While Brunton and Nissenbaum explicitly emphasize at several points that obfuscation is only a small part of the privacy story and not a replacement for governance, markets, norms, and technological intervention,⁸⁵ ideas like obfuscation can take on a life of their own in our dialogue, norms, and policy. We should thus proceed cautiously and temper the rhetoric of an obfuscation “revolution.”

Second, and ominously, there is only so much that we can gain through a strategy of obfuscation. It is a defensive tactic to protect against overreaching by the already powerful. At best, it preserves the status quo, perhaps minimizing the exploitation of the powerless, but doing relatively little to upset the power differentials that constitute the status quo.

Additionally, as the authors themselves concede, obfuscation is available to the powerful as well as the relatively disempowered. It can be used by law enforcement and by corporate surveillance regimes as cloaks and countermeasures. Brunton and Nissenbaum give examples of each of these techniques, from the use of false signals by the police to trick automobile radar detectors into thinking there is a speed trap⁸⁶ to the intentional drafting of privacy policies to obscure the real ways in which personal data are being exploited.⁸⁷ Obfuscation can be a useful tactic, a “force multiplier” of sorts, but there is no evidence about whether its deployment will benefit the disempowered or the already powerful.⁸⁸ If obfuscation is simply about exploiting the practical limitations and resource cost of surveillance and data collection, the weak and vulnerable may be able to temporarily obfuscate effectively or obfuscate effectively against only some parties. But if a motivated adversarial party is willing to invest the resources to counteract obfuscation, the rich and powerful will eventually win. In addition to the powerless, the rich and powerful will also be motivated to find ways to use obfuscation to their own advantage. In a digital society, in which the control of code-based technologies generates ever-more useful social power, we fear that increased use of obfuscation across the board could worsen existing power imbalances rather than shrink them.

85. *See id.* at 97.

86. *See id.* at 26.

87. *Id.* at 30-31.

88. *See* David Brin, *Obfuscation: Protect Privacy by Destroying the Web!*, CONTRARY BRIN (Nov. 24, 2015), <http://davidbrin.blogspot.com/2015/11/obfuscation-protect-privacy-by.html> [<http://perma.cc/WNZ6-XJKW>] (“[W]hat has worked is not—and never has been—hiding. . . . In the future, elites will have all sorts of tools to defeat obfuscation.”).

If obfuscation is truly to be a revolution, it cannot be an individual pursuit that presumes all asymmetrical information-based power relationships are adversarial. Even if obfuscation is justified against some adversaries, people are likely going to need to trust others with whom they are at a power disadvantage. This is particularly true in the digital world, where the guts and inner workings of code, structure, and process are opaque.

Under the standard story we tell ourselves about digital privacy and security, individuals must take an adversarial position toward all those who would collect, use, and share their personal information. While we are certainly vulnerable online, privacy's trust gap means that this worldview can be wasteful and even destructive as the dominant story of privacy.

B. Obfuscation Requires Reliance on Designers

One common trait of many of the examples provided in *Obfuscation* is that they require the use of tools, most of which must be made by other people such as software developers or other designers. CacheCloak, for example, is a tool that obscures a mobile phone user's location by surrounding it with other users' paths.⁸⁹ The injection of that data noise makes any single user's location ambiguous.⁹⁰ Similarly, the Tor network facilitates anonymous Internet use by distributing a user's encrypted traffic through multiple "nodes" to obscure the origin of a data transmission.⁹¹ Vortex is a "proof-of-concept game" that "confuse[s] and misdirect[s] targeted advertising" through the use of "cookies and other identifying systems."⁹² FaceCloak generates false information for Facebook's profile fields and stores "real" or authentic data on a private server for authorized users.⁹³ Finally, another tool, TrackMeNot, developed in part by Nissenbaum, blends genuine and artificial searches to foil the profiling of users through their search results.⁹⁴

In the least, people must be able to understand how the tool works and trust that the tool works as it is supposed to. Every user creates a mental model about how a technology will work. Their expectations are created by the representations of the developers, the user's background knowledge, and the design

89. BRUNTON & NISSENBAUM, *supra* note 3, at 12-13.

90. *Id.* at 13.

91. *Id.* at 19-20.

92. *Id.* at 37.

93. *Id.* at 39-40.

94. *Id.* at 13-14.

of the technology itself.⁹⁵ When a user's mental model does not match the reality of how the technology works, they might think the technology protects them more than it does or accidentally misuse the technology in a way that exposes them to a range of privacy harms, from embarrassment to financial injury or even criminal penalties in the law enforcement context.

C. Obfuscation Requires Cooperation from Confederates

Many kinds of obfuscation also require ordinary people to put their trust in others just like them. Brunton and Nissenbaum provide several vivid examples. They recall the large group of Roman gladiators who called out "I am Spartacus" to protect the real Spartacus standing among them.⁹⁶ Or similarly, in *The Thomas Crown Affair*, the protagonist pulls off a spectacular caper with the help of many identically dressed people engaging in a blur of exchanges involving identical suitcases.⁹⁷ There are many real-world examples of obfuscation that require confederates as well. Brunton and Nissenbaum give the example of people who swap grocery store loyalty cards to obfuscate data collection about their shopping habits.⁹⁸ People can also exchange SIM cards and debit cards to muddy data trails and prevent accurate triangulations of people's whereabouts. But all of these examples share one critical factor—collective obfuscation usually requires us to trust our confederates. While this might not be a problem in contexts where enough people feel collectively and sufficiently repressed to fight back, this kind of solidarity is not always easy to locate.

Confederates must at least be reliable enough to engage faithfully in collective obfuscation. But often these confederates are entrusted with information, such as identifying information, incriminating information, location information, and more, that leaves the obfuscator vulnerable to a range of privacy injuries from embarrassment to criminal punishment. Spartacus and Thomas Crown were able to obfuscate effectively, but only by trusting in the solidarity of their confederates. The same gladiators who protected Spartacus from the Roman authorities could just as easily have identified him to those who would

95. See DON NORMAN, *THE DESIGN OF EVERYDAY THINGS* 26 (2013) ("Mental models, as the name implies, are the conceptual models in people's minds that represent their understandings of how things work Conceptual models are often inferred from the device itself. Some models are passed on from person to person. Some come from manuals. Usually the device itself offers very little assistance, so the model is constructed by experience.").

96. BRUNTON & NISSENBAUM, *supra* note 3, at 15.

97. *Id.* at 16.

98. *Id.* at 28-29.

kill him by shouting, “Here is Spartacus.” In short, many obfuscatory techniques require trusting allies.

Considering the role of developers and confederates, it seems clear that obfuscation is frequently not an individual activity but one that requires the assistance of others. This complicates our story of privacy and obfuscation as individual pursuits, as it requires us to trust obfuscators, even as we are sowing the seeds of distrust by obfuscating in the first place. After all, if we do not want to live like hermits, we have to place our trust somewhere. Recognizing the fact that other people are necessary complicates the standard privacy islands story, but as we will see in the next Part, obfuscation theory has a more serious trust gap of its own.

III. OBFUSCATION AS SECOND-BEST PRIVACY

The insight that we have to place our trust somewhere reveals a larger problem with obfuscation theory. Obfuscation, as we have discussed, is a product of distrust, a last resort for those who cannot otherwise resist their exploitation by the information economy. Instead of building bridges, obfuscators are compelled to burn them. By polluting the data stream to render it unreliable, obfuscation thus reveals itself as not just a creature of distrust, but also a creator of further distrust. In this Part, we examine obfuscation theory from an external critique and argue that it offers at best only a kind of second-best privacy—a privacy for those who have been disempowered and defeated rather than included as equals in the digital society.

There is a better alternative: a “first-best” form of privacy protection, which safeguards personal information via legal rules and social norms. Under this optimal solution, we could create the necessary incentives to protect sustainable, trusted information relationships between ordinary people and the corporations and governments with which they need to engage in order to participate fully in the digital society. This “first-best” privacy would be promoted through law rather than self-help, would be collective rather than individual, and would support building trust rather than undermining it.

A. Obfuscation Promotes Distrust

Obfuscation is a costly weapon. For it to work well, people must either deceive or damage a system or data set. Brunton and Nissenbaum defend obfuscation in these circumstances by arguing that “[d]ata pollution is unethical on-

ly when the integrity of the data flow or data set in question is ethically required.”⁹⁹ Fair enough, at least with respect to the data set.

But data are usually collected in the context of information relationships. Websites, Internet service providers, merchants, carriers, and members of our social networks all collect our personal information as part of a service or social exchange. Sabotage through obfuscation will breed distrust within these relationships. This is where obfuscation’s trust gap diminishes its own utility as a weapon of the weak.

As the authors note, it is essentially impossible to opt out of information relationships in the modern age. Unless we want to embrace the hermit lifestyle and go completely off the grid, we must share our information with others to get the things we need in order to live as integrated members of our society. It is thus not ideal to intentionally poison the online relationships we cannot do without—the technologies that help us get jobs, find partners, seek health treatment, recommend books and films, purchase goods and services, socialize, and travel.

While obfuscation can occasionally be useful, too much waste, damage, and dishonesty will render toxic any such useful information relationship. Consider social media. One obfuscation technique profiled by the authors is “Bayesian flooding,” a strategy in which Facebook users include so many false and implausible life events on their profiles that Facebook cannot accurately target advertisements to the user.¹⁰⁰ While this might be effective, a Facebook profile full of lies would be largely useless to everyone, including the owner of the profile. It might confuse one’s networked connections. Even if human audiences recognize the profile as a fake, the ostensible purpose of social media is to exchange legitimate communication with others. Why even use Facebook in the first place? Similar problems can be found in mapping, gaming, and recommendation apps that require geolocation to serve their purpose. Though such actions might help people obfuscate as a form of protest and collective action, they are mainly only useful when users are prepared to sacrifice the benefit of that information relationship.

The result is that obfuscation is best suited as a strategy for those within relationships that are expendable or those with whom we have no relationship. But in the context of a nonexpendable relationship, obfuscation promotes distrust. As information relationships continue to become more important to our networked lives, this issue is likely to become more problematic.

99. *Id.* at 69.

100. *Id.* at 38-39.

B. Legal Reform Is Not Hopeless

A defender of obfuscation theory might respond at this point that while the tactic is neither practically nor ethically perfect, it can still be good enough. From the perspective of a powerless individual, obfuscation might well be the best option. But as we have already explained, looking at privacy questions from an individual perspective is limiting. Once we expand our frame from the individual perspective to a social perspective, other options become available.

One promising option is collective action through the legal system (e.g., class actions or government enforcement) or the political process (e.g., new laws). As lawyers, these options may seem obvious to us, but we believe that they should not be underestimated. Brunton and Nissenbaum explicitly consider the possibility of regulation as an alternative to a strategy of obfuscation, but they are dismissive of law's potential to resolve the problems of the digital age, and they are suspicious of large corporate and government institutions that run on personal data.¹⁰¹ They argue:

Our laws probably will be the eventual site of the conversation in which we answer, as a society, hard questions about the harvesting and stockpiling of personal information. But they operate slowly, and whatever momentum propels agents of government and law in the direction of protecting privacy in the public interest it is amply counterbalanced by opposing forces of corporations and other institutional actors, including government itself The rate of progress doesn't inspire great optimism.¹⁰²

We agree with Brunton and Nissenbaum's observation that our law has taken a long time to wrestle with the problems created by the information revolution and the processing of personal data. We are sympathetic to the sincere frustration that Brunton and Nissenbaum undoubtedly feel about the lag between social change and legal regulation. Moreover, we are also ideologically sympathetic to their call to the barricades of obfuscatory self-help. But we disagree with the proposition that the inherent conservatism of legal change should lead us to abandon the law as a primary means of dealing with these problems.¹⁰³

^{101.} See *id.* at 61.

^{102.} *Id.*

^{103.} See Neil M. Richards, *Digital Laws Evolve*, WIRED WORLD 2015, at 83-84 (2015), <http://ssrn.com/abstract=2523748> [<http://perma.cc/4RUP-DMQC>] (predicting that privacy-related challenges will increasingly be met with legal and regulatory solutions).

An obfuscation-first strategy for the information age is a concession that the battle is lost, conceding that the best hope for individuals is a kind of guerrilla war against the powerful. Depending upon one's politics, these strategies can have just as powerful an emotional appeal as the obfuscation strategy does for us. But when it comes to the strategy of obfuscation, while we feel its romantic appeal, we harbor no hopeful illusions about such a last-resort strategy's efficacy over time. Instead, we believe that the strategy of trust building will be more effective. Such a strategy works with government and corporate interests to show the long-term value that digital trust can create and plays those interests against each other where necessary to promote the interests of the humans who constitute our digital society.

Contrary to both popular and legal rhetoric about the "death of privacy" and the privacy pessimism *Obfuscation* exhibits, there is substantial evidence that the legal campaign for privacy rights can be effective.¹⁰⁴ Consider the numerous examples from the past few years of instances in which privacy law has advanced human interests over those of the government or corporations. Examples of this phenomenon abound, but some of the most salient include the expiration of the PATRIOT Act,¹⁰⁵ the passage of the California Electronic Communications Privacy Act (CalECPA)¹⁰⁶ and state social media protection laws,¹⁰⁷ the expansion of FTC enforcement of privacy and security rules,¹⁰⁸ the

104. See Richards, *supra* note 16, at 33.

105. Erin Kelly, *Patriot Act Provisions Expire as Senate Compromise Comes Late*, USA TODAY (June 1, 2015), <http://www.usatoday.com/story/news/nation/2015/05/31/nsa-cia-data-collection/28259481> [<http://perma.cc/XQ3M-SZQV>].

106. CAL. PENAL CODE § 1546 (West 2016). See generally *California Electronic Communications Privacy Act (CalECPA) - SB 178*, ACLU N. CALIF. [hereinafter *CalECPA*], <http://www.aclunc.org/our-work/legislation/calecpa> [<http://perma.cc/LKQ4-A8JJ>] (discussing how CalECPA protects cloud-stored data with a warrant requirement).

107. In response to public outcry, at least twenty-five states have passed laws restricting the ability of employers to, among other things, access employees' social media accounts. See generally *State Social Media Privacy Laws*, NAT'L CONF. ST. LEGISLATURES (July 6, 2016), <http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-prohibiting-access-to-social-media-username-and-passwords.aspx> [<http://perma.cc/BBX5-6AU3>] (listing such laws).

108. See generally HOOFNAGLE, *supra* note 51, at 67 ("The FTC . . . changed its structure in 2006 in order to formalize its privacy role, and started hiring technologists to advise the lawyers about technology."); Solove & Hartzog, *supra* note 60, at 666 ("Until recently, the FTC has largely limited itself to the four corners of privacy policies The implications of the FTC's expansion of enforcement and shift to consumer expectations over company representations are profound.").

effect of European privacy regulation on American data practices,¹⁰⁹ and the efforts to foster data security by state attorneys general.¹¹⁰ In each of these recent cases, law has been successfully marshaled to protect people's privacy (whether in their capacities as citizens, consumers, or employees) against powerful corporate or government entities.

These privacy-protective legal developments cover a wide range of regulatory possibilities. For example, the Supreme Court has started to expand the Fourth Amendment to reflect digital technologies, holding that the police must obtain a warrant before they use thermal imaging to search houses,¹¹¹ deploy GPS trackers on cars,¹¹² and search cell phones incident to an otherwise valid arrest.¹¹³ At the federal regulatory level, the FTC has, over the past two decades, used its limited authority to police unfair and deceptive trade practices, and to secure consent decrees against many of the largest Internet companies as well as dozens of other companies. These agreements typically require the companies to cease specified acts alleged to be unfair or deceptive, to create "comprehensive privacy and data security programs," and if those companies violate the consent agreements, to be liable to the government for potentially devastating damages.¹¹⁴ Moreover, a federal court recently reaffirmed the FTC's authority to regulate information security.¹¹⁵ At the state level, the California legislature recently passed CalECPA, a comprehensive digital privacy law that

109. European law has affected American privacy law in a number of ways, most directly in the self-regulatory "Safe Harbor" program that American companies have had to use if they wished to process data about European citizens. In connection with FTC oversight of this voluntary program, the Safe Harbor agreement has had a major effect on the privacy work done in many American companies. See generally KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, *PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE* 60, 188 (2015) (documenting that corporations view European privacy laws as establishing a "floor" that shapes compliance-oriented measures); Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1966 (2013) ("The [European Union] has played a major role in international decisions involving information privacy, a role that has been bolstered by the authority of EU member states to block data transfers to third party nations, including the United States.").

110. Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747 (forthcoming 2017).

111. *Kyllo v. United States*, 533 U.S. 27 (2001).

112. *United States v. Jones*, 132 S. Ct. 945 (2012).

113. *Riley v. California*, 134 S. Ct. 2473 (2014).

114. See HOOFNAGLE, *supra* note 51; Solove & Hartzog, *supra* note 60.

115. *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

requires the police to get a warrant before they access emails, cloud-stored documents, or cell phone metadata.¹¹⁶

The battle to secure privacy is by no means won, but as these numerous cases illustrate, progress is being made. Seeking change and shelter through the legal and political process is a proven strategy recognized by previous revolutions like the civil rights movement and the struggle for safe and equal workplaces.¹¹⁷ We worry that a strategy of increased obfuscation could, by corroding trust in our digital future and by keeping our focus on the individual rather than the social dimensions of privacy issues, undermine this promising trend in a way that might make us all worse off.

We cannot know what the future will hold. As Justice Holmes wisely reminded us in his great dissent in *Abrams v. United States*, “[A]ll life is an experiment. Every year, if not every day, we have to wager our salvation upon some prophecy based upon imperfect knowledge.”¹¹⁸ Holmes was writing about an earlier revolution—the industrial one—and dealing with the prosecution of an activist who had quite literally called his fellow workers to the barricades to protect human interests against government and corporate ones.¹¹⁹ Yet Holmes’s wisdom is as relevant to the information revolution of the twenty-first century as it was to the industrial revolution of the twentieth: we do not know what the future will hold, but we have to do the best we can with the limited knowledge we possess. We cannot know for certain whether a strategy of obfuscation or one of trust is the best way to deal with the disruptive consequences of the information revolution. But we remain hopeful that trust is the better strategy. If we must have a conceptual revolution about how we think about privacy and security, we should fight that revolution for trust and relationships rather than sabotage and individualism. Instead of a revolution of sabotage, a guerilla war of obfuscation against powerful interests, we should

116. CAL. PENAL CODE § 1546 (West 2016). See generally *CalECPA*, *supra* note 106 (explaining both CalECPA and the ACLU’s work in shepherding it through the California legislative process).

117. E.g., MARY DUDZIAK, *COLD WAR CIVIL RIGHTS: RACE AND THE IMAGE OF AMERICAN DEMOCRACY* (2011) (discussing civil rights); MICHAEL J. KLARMAN, *FROM JIM CROW TO CIVIL RIGHTS: THE SUPREME COURT AND THE STRUGGLE FOR RACIAL EQUALITY* (2004) (discussing civil rights); JOHN MENDELOFF, *REGULATING SAFETY: AN ECONOMIC AND POLITICAL ANALYSIS OF OCCUPATIONAL SAFETY AND HEALTH POLICY* (1979) (discussing workplace safety); Daniel B. Rodriguez & Barry R. Weingast, *The Positive Political Theory of Legislative History: New Perspectives on the 1964 Civil Rights Act and Its Interpretation*, 151 U. PA. L. REV. 1417, 1427 (2003) (discussing civil rights).

118. 250 U.S. 616, 630 (1919) (Holmes, J., dissenting).

119. See RICHARD POLENBERG, *FIGHTING FAITHS: THE ABRAMS CASE, THE SUPREME COURT, AND FREE SPEECH* 218-28 (1987).

have a conceptual revolution about the way we think and talk about privacy that pushes past the limitations of the privacy islands approach. At bottom, we believe there are encouraging signs that the battle for privacy has not been lost and that a strategy that promotes trust in information relationships is a better way forward than doubling down on obfuscation and distrust.

IV. THE POTENTIAL OF TRUST

In this Review, we have argued that the major weakness of obfuscation is that it subscribes to the individualism that dominates modern privacy rhetoric and policy. There is, however, a better way to think about privacy, security, and the role of information in a digital age. Rather than thinking about the ways in which we are isolated like islands, we can think instead about the ways in which we are connected. These connections frequently occur through what we have been calling *information relationships*. Thinking about privacy in these terms will allow us to move past the privacy islands model and close privacy's trust gap.

In this final Part, we sketch out how a trust-based model of privacy policy can work. First, we explain what we mean by trust, what its constituent parts are, and how it can serve as a conceptual foundation for privacy. Second, drawing on our trust theory of privacy, we show how looking at privacy problems from a trust perspective rather than a privacy islands perspective changes legal and policy questions.

A. A Theory of Privacy and Trust

Trust is an incredible force. Here and in other work, we use the term to mean a willingness to expose our vulnerabilities to others.¹²⁰ In the privacy context, trust allows us to develop long-term, sustainable information relationships by sharing meaningful but often sensitive information and having sincere exchanges with the confidence that what we share will be used for our benefit and not come back to haunt or harm us.¹²¹

120. Richards & Hartzog, *supra* note 10 (manuscript at 36-48); Neil M. Richards & Woodrow Hartzog, *Trusting Big Data Research*, DEPAUL L. REV. (forthcoming 2017), <http://ssrn.com/abstract=2717868> [<http://perma.cc/YYJ6-6BTJ>]; Neil Richards & Woodrow Hartzog, *Facebook's New Digital Assistant 'M' Will Need To Earn Your Trust*, GUARDIAN (Sept. 9, 2015), <http://www.theguardian.com/technology/2015/sep/09/what-should-we-demand-of-facebook-new-digital-assistant> [<http://perma.cc/BV78-W8RS>].

121. See, e.g., RUSSEL HARDIN, TRUST AND TRUSTWORTHINESS 3 (2004); J. David Lewis & Andrew Weigert, *Trust as a Social Reality*, 63 SOC. FORCES 967, 968 (1985).

How should we promote trust in the context of personal information? Trustworthy data stewards have four characteristics that promote trust: they are honest, discreet, protective, and loyal.¹²² Each of these values requires some elaboration. First, trustworthy stewards are *honest* because they explain to us the terms under which they hold and use our data. Honesty places the obligation of being understood on the steward, rather than on our ability to scrutinize the dense, vague, and protean language of privacy policies and terms of service. Second, they are *discreet* because they treat our data as presumptively confidential and do not disclose it in ways contrary to our interests or expectations. Third, trustworthy stewards are *protective* because they hold the data securely against third parties, doing everything within reason to protect us from hacks and data breaches. Fourth, and most fundamentally, those we trust are *loyal* because they put our interests ahead of their own short-term potential for gain. This means, among other things, that they do not engage in unreasonable self-dealing when collecting, using, or sharing our data.

We have argued elsewhere at length how these four principles can serve as the foundation for our modern notions of privacy, thereby encouraging us to engage in online commerce, social relationships, and political discussion.¹²³ The four foundations of trust are already familiar to us instinctually and in our policy. They are implicit in some existing notions, such as confidentiality, transparency, loyalty, and data security. They can be seen in the law of protective relationships like fiduciaries.¹²⁴ However, we have not typically used the idea of trust to unify these concepts as an alternative frame to individual-centric mindsets. Nor have we used them to place substantive rather than procedural obligations on those who hold our data—our digital lives and identities—on their servers. However, change is starting to happen here as well. A small but growing number of other scholars are also moving beyond the limitations of the privacy islands approach and exploring the promise of thinking about privacy problems in trust terms.¹²⁵

122. Richards & Hartzog, *supra* note 10 (manuscript at 36-48).

123. *Id.* (manuscript at 27-34).

124. See Balkin, *supra* note 61, at 1205-09; Ethan J. Leib, *Friends as Fiduciaries*, 86 WASH. U. L. REV. 665, 672 (2009).

125. For additional perspectives on the relationship between privacy and trust, see Balkin, *supra* note 61, at 1205-09; Brennan-Marquez, *supra* note 61; Hirsch, *supra* note 64; Waldman, *supra* note 64, at 561; and Kirsten Martin, *Transaction Costs, Privacy, and Trust: The Laudable Goals and Ultimate Failure of Notice and Choice To Respect Privacy Online*, 18 FIRST MONDAY (Dec. 2013), <http://firstmonday.org/ojs/index.php/fm/article/view/4838/3802> [<http://perma.cc/SY9L-YFHT>].

The most sustainable solution to the problems raised by personal data is to promote trust between humans and the corporate and government institutions that hold and process data about them. Rather than doubling down on obfuscation, which fosters distrust, we should promote a privacy policy based upon trusted, sustainable, long-term relationships. For corporations, where market incentives exist to create these kinds of relationships, we should embrace them, and where markets fail or incentives conflict, we should use the full range of legal and policy tools to promote trust in our information relationships. For governments, we should use the range of public law tools—constitutional, statutory, and regulatory—to encourage our public officials to act in trustworthy ways. Given the important roles that corporations play in holding our personal data, we should also encourage corporations to fight the government to earn and maintain the trust of their customers, as Apple notably did in its battle with the FBI over the San Bernardino shooter's iPhone.¹²⁶ We believe that when it comes to the battles over personal information in a time of rapid technological, social, and commercial change, a trust-based equilibrium for personal information will be normatively superior to an obfuscation-based equilibrium. Trust, properly understood, holds the potential for a kind of first-best privacy.

B. Privacy Problems from a Trust Perspective

One of the chief virtues of a trust-based approach to privacy is that it allows us to better understand privacy problems and formulate privacy solutions. Legal and policy questions surrounding privacy are transformed when we move from a privacy islands perspective to a trust perspective.

Consider, for example, the problem of government surveillance. Secret government surveillance of journalists and activists, in addition to being difficult to prove in court, might not rise to the level of an individual injury under current law. This was the Supreme Court's holding in *Clapper v. Amnesty International USA*, which rejected the plaintiffs' individual claims of injury from surveillance as too speculative.¹²⁷ From a privacy islands perspective, journalists who could not allege a legal injury might want to turn to obfuscation. However, a focus on relationships enables us to perceive one of the real harms of secret, thoroughgoing, and unchecked surveillance. Such surveillance threatens relationships and chills expressive freedoms because the fear of that surveil-

^{126.} See *supra* note 15 and accompanying text.

^{127.} 133 S. Ct. 1138, 1143 (2013).

lance fosters suspicion that thwarts the building of trust.¹²⁸ A trust-based perspective also reveals the fallacy of the government's reading of the Fourth Amendment to suggest that when we disclose data to a trusted "third party" like our cloud provider, we lose the protection of the Fourth Amendment for that data.¹²⁹

Away from government surveillance, a trust-based perspective can also help us better understand private law problems in personal information. Consider the issue of data breaches. Focusing on individual harm in cases involving data security breaches, the aggregation of information by data brokers, and the downstream disclosure of information shared on social networking websites often gets law and policy no closer to keeping personal data secure, digital dosiers compliant with the fair information practices, and socially-shared information obscure.¹³⁰ By contrast, trust supplies the missing ingredient to these problems by treating betrayal of trust as actionable in the absence of an otherwise quantifiable, visceral harm. Similar to theories of promissory estoppel and detrimental reliance, breach of trust should be taken more seriously in privacy law because people change their positions to become more vulnerable because of it.¹³¹

Thinking about privacy in terms of trust also helps us avoid many of the shortcomings and blind spots of the dominant individualistic view of privacy. That view takes as a given that individuals must take primary responsibility for their digital privacy and security. Thus, in most sectors of the economy, as long as companies offer notice of their privacy practices and a choice to opt out of those practices, they have complied with the law.¹³² This is the case even when the "notice" is vague legal text buried in a privacy policy that few consumers read, and the "choice" is nothing more than the choice not to use that compa-

128. Cf. Richards, *supra* note 1 (describing how uncontrolled surveillance regimes distort relationships by facilitating blackmail and subversive persuasion).

129. See Richards, *supra* note 61 (manuscript at 3-6).

130. See M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1158 (2011); Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2277 (2015); Strahilevitz, *supra* note 36, at 948-53; Daniel Solove, *When Is a Person Harmed by a Privacy Violation? Thoughts on Spokeo v. Robins*, LINKEDIN (May 17, 2016), <http://www.linkedin.com/pulse/when-person-harmed-privacy-violation-thoughts-spokeo-v-daniel-solove> [<http://perma.cc/5KDC-2W2T>].

131. See Woodrow Hartzog, *Promises and Privacy: Promissory Estoppel and Confidential Disclosure in Online Communities*, 82 TEMP. L. REV. 891 (2009); Waldman, *supra* note 64, at 615 (noting the role of trust in good faith and fair dealing assumed in contractual exchange).

132. See WOODROW HARTZOG, *PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES* (forthcoming 2017) (manuscript at 7) (on file with authors).

ny's services.¹³³ If we are all privacy islands left to fend for ourselves, this approach seems innocuous, even though the American approach is an outlier compared to the laws of virtually every other advanced economy.¹³⁴ Moreover, fending for ourselves would lead logically to a strategy of obfuscation.

A focus on trust changes this calculus. Moving beyond fictive notions of trust and blunt concepts of consent as the essence of privacy law, a trust perspective would go further. It would ask whether the notice was sincere and reasonable (i.e., whether it was *honest*). It would ask whether the choice was meaningful and gave the data subject the opportunity for *discretion* in the way their data was held. More generally, it would ask whether the data were *protected* and whether the institution holding personal data acted in ways that were *loyal* to the data subject. In this context, loyalty might mean the company took the data subject's substantive interests into account so that the data subject did not need to engage in pragmatic privacy self-help, whether of the notice-and-choice or of the obfuscatory varieties. The main effect of the shift in perspective is to keep the party entrusted with personal information from shifting the risk of loss back onto the trusting party. It thus places obligations on the powerful entities best able to protect against loss, rather than blaming the powerless individuals who are often at their mercy.

Consider, for example, how this shift in perspective might work in the context of a social network like Facebook. Large technology companies competing with each other for long-term relationships with human customers already have substantial market incentives to promote trust. However, one of the criticisms that Facebook has confronted is the argument that because its human users do not pay any money to use the service, its real customers are the paying advertisers on whose behalf Facebook users are served up for marketing purposes.¹³⁵ Meaningful legal incentives to be honest (in terms of better notice of data practices and data breaches), discreet (in terms of never selling data to third parties, at least by default), and secure (greater liability for data breaches) could generate greater trust than the mixed feelings many people have about large technology companies. But the real virtue of trust theory is the duty of loyalty, putting the interests of the human user first over the short- and medium-term interests of the company, so that both the user and the company benefit over the long term. A meaningful duty of loyalty to human users could

133. Richards & Hartzog, *supra* note 10 (manuscript at 8).

134. RONALD J. KROTOSZYNSKI, JR., PRIVACY REVISITED: A GLOBAL PERSPECTIVE ON THE RIGHT TO BE LEFT ALONE xvi (2016).

135. E.g., Olivia Solon, *You Are Facebook's Product, Not Customer*, WIRED UK (Sept. 21, 2011), <http://www.wired.co.uk/article/doug-rushkoff-hello-etsy> [<http://perma.cc/XCG7-GCUY>] (quoting an argument by the media theorist Douglas Rushkoff).

eliminate the ambiguity over Facebook's duties to its human users, and promote further investment in the platform by both sides.¹³⁶

We harbor no illusions that trust is a panacea for all problems of information policy. It is hard for us to trust those whose interests are opposed to ours, or parties of whose existence we are unaware. Another limitation of trust is the problem of misplaced trust—a party that pretends to be trustworthy but then betrays those that trust them can sow massive amounts of distrust. As we conceive of it, trust works best in relationships in which there is the potential for mutual gain and in which there are multiple opportunities to deepen the relationship. We can have such relationships with our cloud provider, our social network, or our spouse, but one-time transactions standing alone are more prone to distrust. Relationships like these are the economic or literal equivalent of a “one-night stand.” To guard against this problem, companies in the “sharing economy” like Airbnb and other online intermediaries have built trust-promoting structures like peer rating systems into their platforms.¹³⁷ But we believe that trust retains enormous potential, particularly for consumers in the digital economy who must live their lives in connection with large technology companies who share the consumers' economic interests in a long-term, sustainable information relationship that can be beneficial (and profitable) to both parties.

Similarly, we believe that there is much insight to be gained when we look at the world from the perspective of trust. For example, trust allows us to see other problems with the dominant view, such as the implicit zero-sum game of individualistic notions of privacy. When the individual is pitted against the world, we should not be surprised when the individual's gain is seen as the company's or government's loss.¹³⁸ If we think about privacy as the antithesis of profitability or national security, we should not be surprised when companies choose to maximize profits or governments engage in widespread surveil-

136. For a more extensive discussion of this topic in the context of Facebook's proposed digital assistant technology, see Richards & Hartzog, *supra* note 120.

137. *E.g.*, Jason Tanz, *How Airbnb and Lyft Finally Got Americans To Trust Each Other*, WIRED (Apr. 23, 2014), <http://www.wired.com/2014/04/trust-in-the-share-economy> [<http://perma.cc/QBC5-VMSA>].

138. Consider in this regard the definition of an “unfair trade practice” under federal law, which requires exactly this kind of direct tradeoff to be actionable. *See* Federal Trade Commission Act § 5, 15 U.S.C. § 45(n) (2012) (preventing the Federal Trade Commission from “declar[ing] unlawful an act or practice” on the basis of unfairness “unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition”). Or consider the commonly held belief that privacy and national security are zero-sum. *See generally* SOLOVE, *supra* note 63 (debunking this myth).

lance. But privacy is frequently something corporations can use for their long-term benefit, and something free societies can cherish while also being secure.¹³⁹ However, looking at privacy in negative, individualistic terms can cause us to lose sight of this very important insight.

Perhaps most interestingly, even obfuscation is transformed into something more useful when we look at privacy through the lens of trust. As an isolated concept, obfuscation is destructive. Brunton and Nissenbaum speak of “sand in the gears” and of frustrating adversaries.¹⁴⁰ The entire point of sabotage is wreckage. However, the wisdom motivating obfuscation—that data collectors’ limited resources can be used to protect our privacy—can be leveraged for constructive purposes as well. Consider instead a broader notion of obscurity as privacy. Obscurity is a concept focused on the creation or preservation of transaction costs to finding and accessing personal information. Obscurity protections are based around the notion that making (or keeping information) “hard but possible” to find or use is often good enough for many purposes.¹⁴¹ Whereas the examples in *Obfuscation* largely taint data, obscurity looks to more generally minimize the risk of identification, which could include limitations on searchability, storage, or other increases in transaction costs that keep the data safe, but useful.¹⁴² While it is hard to imagine companies saying “please obfuscate against us” or “please taint our data,” they might be open to preserving the obscurity of data subjects within relationships of trust. They might not need to know (or store) many kinds of identified sensitive data in order to carry out their functions and might deliberately collect less data than is possible in order to protect and be loyal to their trusting customers.

C. Promoting Trust in a Digital Society

At a practical level, how do we promote trust in the relationships that constitute our digital society? Our proposal for first-best, trust-promoting privacy rules is twofold. First, we should encourage the further development of existing trust norms as a business practice in the technology industry. Second, we

139. Richards, *supra* note 16.

140. BRUNTON & NISSENBAUM, *supra* note 3, at 2, 57.

141. For more insight on the privacy advantages of making information “hard but possible” to find, see Paul Ohm, *Good Enough Privacy*, 2008 U. CHI. LEGAL F. 1, 49-50. For a discussion of the virtues of Ohm’s account, see also Woodrow Hartzog, *The Value of Modest Privacy Protections in a Hyper Social World*, 12 COLO. TECH. L.J. 333, 347-49 (2014).

142. See Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 WASH. L. REV. 703 (2016) (advocating for an approach to protecting data that focuses on procedural safeguards and “minimizing risk of reidentification”).

should develop legal rules to provide additional incentives for trustworthiness and to punish companies that act in ways that are trust-corrosive or disloyal. Third, we should place meaningful checks on government surveillance and government access to information held by companies on behalf of their customers.

The first part of our strategy involves encouraging trust norms. There are already numerous market incentives for companies to promote these kinds of relationships. Consider in this regard Apple's high-profile standoff with the FBI over the security of iPhones and its lobbying in favor of strong encryption before Congress.¹⁴³ Or consider Microsoft Corporation's lawsuits against the federal government, seeking to prevent extraterritorial use of search warrants and the use of search warrants accompanied by gag orders.¹⁴⁴ Consider also the trend among large technology companies to issue "transparency reports," data-rich compendia of government requests and orders to access the data of their users.¹⁴⁵ Or consider the vast sums that big technology and cloud companies expend in order to protect the data they store on behalf of their customers.¹⁴⁶ These are recent examples, but this phenomenon is hardly new. In 2006, for example, Google successfully convinced the government to narrow a subpoena of its search engine records in order to protect the trust of its users and the confidentiality of their search results.¹⁴⁷ These cases illustrate that it will often be in the immediate and long-term interest of companies to protect the privacy

143. See Elizabeth Weise, *Apple v FBI Timeline: 43 Days that Rocked Tech*, USA TODAY (Mar. 30, 2016, 10:46 AM), <http://www.usatoday.com/story/tech/news/2016/03/15/apple-v-fbi-timeline/81827400> [<http://perma.cc/W2MQ-N6XC>] (providing a timeline of events from February 16, when a judge issued the initial order for Apple to help the FBI access a suspect's iPhone, to March 29, when the judge vacated her original order).

144. Nora Ellingsen, *The Microsoft Ireland Case: A Brief Summary*, LAWFARE (July 15, 2016, 10:34 AM), <http://www.lawfareblog.com/microsoft-ireland-case-brief-summary> [<http://perma.cc/DN6Y-VJ5A>] (summarizing *Microsoft v. United States* as holding that "the government cannot compel Microsoft . . . to turn over customer emails stored on servers outside the United States").

145. See, e.g., Jon Russell, *Google's Latest Transparency Report Shows Record Government Data Requests*, TECHCRUNCH (July 19, 2016), <http://techcrunch.com/2016/07/19/googles-latest-transparency-report-shows-record-government-data-requests> [<http://perma.cc/U5J7-2BBX>] (describing the transparency reports as "provid[ing] a glimpse at how international governments and states are trying to use and access our data" and "an indicator as to how much information Google . . . gives up in these cases").

146. E.g., *Companies To Spend \$130 Billion on Cybersecurity in 2011*, CONSUMER REP. (July 26, 2011, 9:08 AM), <http://www.consumerreports.org/cro/news/2011/07/companies-to-spend-130-billion-on-cybersecurity-in-2011/index.htm> [<http://perma.cc/73BQ-5XNN>] (discussing efforts by U.S. companies to improve their cybersecurity).

147. *Gonzales v. Google, Inc.*, 234 F.R.D. 674, 678-79 (N.D. Cal. 2006).

of their users. More generally, as Internet business models mature, it will be in the interest of companies to be honest, discreet, protective, and loyal to their customers, in order to develop long-term relationships that create real value for the companies as well as their users.

We harbor no illusions, however, that all companies will take this long view. Bad actors exist throughout our economy and seek short-term gain at the expense of their users, a phenomenon we have elsewhere called “data strip mining.”¹⁴⁸ Similarly, there will also be instances in which companies have financial or other incentives to betray or act disloyally with respect to the privacy of their users or other people. The shadowy and largely unregulated data broker industry is one salient example here, but there are many others. In these cases, in which the market fails to adequately promote or protect trust, we offer the second prong of our privacy strategy, which is overtly regulatory. In cases where the market fails to provide adequate incentives to promote trust, we believe that the law should step in to regulate in trust-protective ways and require companies to be honest, discreet, protective, and loyal toward those people whose data they hold, process, and exploit for gain. In this way, the law could recognize a kind of constructive information relationship between a person and a large commercial entity that trades in large quantities of information about them. Such examples are further afield than our core case of a close information relationship, however.

We should also continue to use law to provide additional incentives for trustworthiness and to punish companies that act in ways that are trust-corrosive or disloyal. For example, while the FTC has used its long standing jurisdiction over unfair and deceptive trade practices to become the de facto American privacy and data protection regulator, it could go further.¹⁴⁹ The FTC already promotes the honesty norm to some extent through its unfair and deceptive trade practices work, but we could imagine the FTC treating indiscreet or disloyal trade practices within its unfairness authority. The agency could continue its trend of holding data collectors, instead of data subjects, responsible for ensuring that consumer expectations match reality.¹⁵⁰ Congress could

¹⁴⁸. Richards & Hartzog, *supra* note 10 (manuscript at 6).

¹⁴⁹. HOOFNAGLE, *supra* note 51, at xiii-xvi.

¹⁵⁰. See *In re Goldenshores Techs., LLC*, No. 132-3087, 2014 WL 1493611 (Fed. Trade Comm'n Mar. 31, 2014) (alleging failure to disclose the collection of geolocation information to be an unfair and deceptive trade practice); *In re Sears Holdings Mgmt. Corp.*, No. 082-3099, 2009 WL 2979770 (Fed. Trade Comm'n Aug. 31, 2009) (alleging deception by failure to adequately disclose surveillance practices in a privacy policy); Solove & Hartzog, *supra* note 60, at 617 (“The FTC often required companies to make modifications to their privacy policies to better notify users that their personal information is being collected, used, and shared. If com-

empower the FTC with additional authority in this area, and it could join the rest of the industrialized West by passing a baseline privacy law for commercial data—one that places real incentives on companies to treat personal data in trustworthy ways. This could take the form of the traditional, top-down regulation that every industrial Western democracy but the United States has, or it could take the form of the “Digital Millennium Privacy Act” proposed by Jack Balkin and Jonathan Zittrain, under which companies could agree to act as trust-promoting “information fiduciaries” in exchange for immunity from uncertain liability.¹⁵¹

An entirely different approach could be for courts to reinvigorate the languishing tort of breach of confidentiality to reinforce expectations of nondisclosure and protection within intimate relationships and those that involve significant personal disclosure. In other work, we have explored the ways in which American tort law has failed to fully embrace the idea of a duty of confidentiality that protects information disclosed in relationships.¹⁵² By encouraging *discretion* and *loyalty* in particular in these relationships, tort law could be leveraged to promote digital trust as well.

The third part of our proposed strategy deals with government surveillance. All citizens of digital societies are in information relationships with their governments, who collect data on them from cradle to grave and beyond. The dangers of government databases were a stimulus for the passage of federal and state laws placing limits on government data usage like the Federal Privacy Act of 1974 and its state law equivalents.¹⁵³ But as noted above, as modern technology has marched on, new dangers of government recordkeeping and surveillance have emerged, whether by direct surveillance or by obtaining personal data from companies that hold it on behalf of their customers.¹⁵⁴ The revelations of Edward Snowden shattered the trust of many ordinary and law-abiding Internet users in the privacy and confidentiality of their communica-

panies did not have a privacy policy, the FTC might require them to create one, perhaps under its authority to order corrective advertising.” (internal citations omitted)).

151. See Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain To Make Tech Companies Trustworthy*, ATLANTIC (Oct. 3, 2016), <http://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346> [<http://perma.cc/K7EP-BX9C>].

152. See Woodrow Hartzog, *Chain-Link Confidentiality*, 46 GA. L. REV. 657 (2012); Woodrow Hartzog, *Reviving Implied Confidentiality*, 89 IND. L.J. 763 (2014); Richards & Solove, *supra* note 65, at 124, 151-52.

153. See, e.g., Privacy Act of 1974, 5 U.S.C. § 552a (2012); Virginia Government Data Collection and Dissemination Practices Act, VA. CODE ANN. § 2.2-3801 (1976).

154. See also Richards, *supra* note 1, at 1937-41 (giving examples of some of these practices).

tions and online activities.¹⁵⁵ Law can (and should) be used to rebuild trust between citizens and their government, whether by explicitly extending Fourth Amendment law to digital communications and evidence,¹⁵⁶ or by using statutory law to achieve similar goals.¹⁵⁷ There are a variety of ways to rebuild trust between governments and citizens; our argument does not depend upon any particular form, but we believe more generally that the information relationships each of us have with our governments will benefit from the trust that clear legal rules can create. In particular, the governments that democratic citizens create to govern their societies must be honest, discreet, protective, and loyal.

There will no doubt be difficult cases to regulate, but we believe that trust-promoting regulation is a superior alternative to doubling down on obfuscation. More fundamentally, if we think about personal information in terms of trust, we start to ask better regulatory questions, ones that focus on the kind of sustainable digital future we want to build, rather than on fictive notions of consent or illusions of consumer choice. This, we believe, is the policy path forward to a first-best kind of privacy.

CONCLUSION

In *Obfuscation*, Brunton and Nissenbaum have done us an enormous service by identifying obfuscation as a strategy, describing its potential, and engaging deeply with many of its ethical pitfalls. They also powerfully remind us that, when it comes to protecting our data, pretty good protection is frequently good enough. Our understanding of the strategies of privacy and security is substantially richer as a result of their work.

Obfuscation may well be one of the most appealing strategies of the digital age, but we must resist the full force of its siren call to “revolution.” While the practices of obfuscation will certainly have their uses, a full embrace of obfuscation will lead to distrust at a time when there is good evidence to believe that a strategy of market and regulatory trust building can produce meaningful benefits in our struggles over personal information in the digital society. The deployment of legal and policy tools to promote trust in sustainable information relationships certainly has less romantic appeal than obfuscation, but there is

155. RICHARDS, *supra* note 12, at 185-86.

156. See Richards, *supra* note 61 (making an extended argument along these lines).

157. *E.g.*, CAL. PENAL CODE § 1546 (West 2016) (requiring the government of California to get a warrant before it accesses, *inter alia*, data stored in the cloud).

good reason to believe that trust, not obfuscation, is the way toward a better digital future.