PRIVACY SELF-HELP

Steven H. Hazel†

ABSTRACT

Today, millions of consumers practice privacy self-help. Some cover their laptop cameras; others communicate through encrypted messaging apps; still others delete sensitive documents. But while self-help has emerged as one of the primary ways that consumers manage privacy risks, it has attracted little scholarly attention.

To fill that gap, this Article offers a descriptive account of the relationship between privacy doctrine and self-help. As it turns out, privacy law relies on self-help to solve some of its most pressing problems. From the Fourth Amendment to the FTC's unfairness authority, courts and regulators look to self-help to decide which disputes deserve attention and to conserve scarce resources. The upshot is that harnessing self-help has become a pervasive feature of modern privacy law.

Turning from the descriptive to the normative, this Article asks how law should respond to privacy self-help. Too often, self-help exposes the data it promises to protect. When self-help backfires, the conventional wisdom holds that courts and regulators should install legal remedies to replace it. But displacing self-help would disable the doctrines that depend on it.

Challenging the conventional wisdom, this Article shows that legal institutions protect consumers best when they facilitate—rather than replace—self-help. By arming individuals with intelligence about self-help, courts and regulators can empower them to spot successful strategies and sidestep self-defeating ones. This approach promises to transform self-help from a popular yet unreliable practice into a potent weapon in the hands of millions of consumers. Ultimately, complementing self-help should be privacy law's first instinct, not its last resort.

DOI: https://doi.org/10.15779/Z382J68529

† J.D., 2019, University of Chicago Law School.

TABLE OF CONTENTS

I. INTRODUCTION 307
II. SELF-HELP IN PRACTICE 310

A. DEFINING SELF-HELP 311
B. SURVEYING SELF-HELP 312
1. Concealment Strategies 313
a) Concealing Identifying Information 314
b) Concealing Sensitive Information 315
c) Concealing Previously-Disclosed Information 316
2. Obfuscation Strategies 318
a) Obfuscating Identifying Information 318
b) Obfuscating Sensitive Information 319
c) Obfuscating Activity 320
3. Monitoring Strategies 321
a) Personal Monitoring 321
b) Monitoring Services 322
c) Monitoring Networks 323

III. THE PERILS OF SELF-HELP 324

A. PRIVACY-PRIVACY TRADEOFFS 325
1. Self-Help as Data Creation 326
2. Negative Inferences 327
3. Overreliance 328
B. SECURITY-PRIVACY TRADEOFFS 328
1. Confidentiality 329
2. Integrity 330
3. Availability 331
C. ARMS RACES 332
1. Surveillance Technologies 333
2. Data Brokers 334

IV. HOW PRIVACY LAW HARNESSES SELF-HELP 335

A. THE FOURTH AMENDMENT 336
B. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT 336
C. ARTICLE III STANDING IN DATA BREACH CASES 337
D. PRIVACY TORTS 338
E. DATA BREACH NOTIFICATION STATUTES 340

V. THE CASE FOR COMPLEMENTING SELF-HELP 341

A. HOW LAW CAN COMPLEMENT SELF-HELP 342

1. Revisiting Generally Applicable Laws That Exacerbate Asymmetries...342
2. Extracting Intelligence from Data Processing Firms.....345
3. Disrupting Invisible Arms Races.....347
B. COMPLICATIONS.....349
1. The Gap Between Information and Action.....349
2. The Social Costs of Self-Help.....350
3. The Market Alternative to Self-Help.....351
VI. CONCLUSION.....352

I. INTRODUCTION

Mark Zuckerberg, Facebook's founder and CEO, is not generally regarded as a privacy advocate. In 2010, for instance, he proclaimed that privacy is no longer "a social norm."[1] But photos indicate that Zuckerberg may be more concerned about privacy than his public statements suggest. Zuckerberg—a Harvard-trained computer scientist who employs thousands of engineers—covers his MacBook's camera with a piece of tape.[2] And Zuckerberg isn't the only one.[3] Next time you step into a classroom or conference room, look around. You're sure to spot a sea of taped-over laptop cameras.[4]

Millions of consumers embrace privacy self-help strategies like Zuckerberg's.[5] Some communicate through encrypted messaging apps;[6] others submit misleading information in response to marketing requests;[7] still others shred sensitive documents.[8] Indeed, a Pew Research Center survey reveals that

1. Bobbie Johnson, *Privacy No Longer a Social Norm, Says Facebook Founder*, THE GUARDIAN (Jan. 10, 2010), https://www.theguardian.com/technology/2010/jan/11/facebook-privacy.

2. Katie Rogers, *Mark Zuckerberg Covers His Laptop Camera. You Should Consider It, Too*, N.Y. TIMES (June 23, 2016), https://www.nytimes.com/2016/06/23/technology/personaltech/mark-zuckerberg-covers-his-laptop-camera-you-should-consider-it-too.html.

3. *See* Julian Hattem, *FBI Director: Coverup Your Webcam*, THE HILL (Sept. 14, 2016), https://thehill.com/policy/national-security/295933-fbi-director-cover-up-your-webcam.

4. *See* Kurt Opsahl, *How to Protect Against Laptop Webcam Hacking*, ELEC. FRONTIER FOUND. (Apr. 29, 2013), https://www.eff.org/deeplinks/2013/04/how-protect-against-laptop-webcam-hacking.

5. For a definition of privacy self-help, see *infra* Part II.A. Individuals also practice self-help to protect their data from friends, family members, and the government. But those forms of self-help take different forms and serve different purposes. Thus, this Article concentrates on consumer self-help strategies.

6. *See infra* Part 0.

7. *See infra* Part II.B.2.

8. *See infra* Part 0.

almost 90% of Americans practice at least one form of privacy self-help.[9] To put that figure in perspective, the Equifax data breach litigation—by far the largest privacy-related class action in U.S. history—covered 56% of American adults.[10]

The upshot is that self-help has emerged as one of the primary ways that consumers manage privacy risks. So far, however, it has attracted little attention from legal scholars.[11] To close that gap, this Article asks what the law should do about privacy self-help.

Courts and regulators cannot afford to ignore that question. Indeed, the same attributes that make self-help attractive to consumers also make it indispensable to legal institutions. First, self-help's *preference signaling* function tells adjudicators which types of data consumers see as sensitive.[12] By honoring consumers' self-help choices, courts and regulators empower individuals to decide what data to protect for themselves. Second, self-help's *resource conserving* function resolves low-value disputes that would otherwise consume scarce judicial and regulatory resources.[13] In doing so, self-help enables adjudicators to concentrate their limited resources on the most serious privacy threats. Over time, harnessing those functions has become a common move across many privacy doctrines.

But privacy law's reliance on self-help may be misplaced. Too often, self-help strategies expose the data they promise to protect.[14] Thanks to

9. *The State of Privacy in Post-Snowden America*, PEW RSCH. CTR. (Sept. 21, 2016), https://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/ ("Some 86% of internet users have taken steps online to remove or mask their digital footprints . . . .").

10. *See* Bryan Pietsch, *Factbox: Biggest U.S. Data Breach Settlements Before Equifax*, REUTERS (July 22, 2019), https://www.reuters.com/article/us-equifax-cyber-settlement-factbox/factbox-biggest-u-s-data-breach-settlements-before-equifax-idUSKCN1UH22P; Press Release, Off. of the Att'y Gen. for the D.C., 50 Attorneys General Secure $600 Million from Equifax in Largest Data Breach Settlement in History (July 22, 2019), https://oag.dc.gov/release/50-attorneys-general-secure-600-million-equifax.

11. *See generally* FINN BRUNTON & HELEN NISSENBAUM, OBFUSCATION: A USER'S GUIDE FOR PRIVACY AND PROTEST (2016) (endorsing obfuscation, a species of self-help); Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap: A Review*, 126 YALE L.J. 1180 (2017) (identifying the downsides of obfuscation); Douglas Gary Lichtman, *How the Law Responds to Self-Help* (John M. Olin Program L. & Econ. Working Article No. 232, 2004) (discussing briefly the relationship between privacy law and self-help).

12. *See, e.g.*, Lichtman, *supra* note 11, at 19 (explaining that self-help "distinguish[es] the bulk of normal business information from that special subset of information that warrants protection").

13. *See, e.g.*, Robert C. Ellickson, *Of Coase and Cattle*, 38 STAN. L. REV. 623, 686 (1986) (noting that self-help avoids the "cost[s of] carry[ing] out legal research and . . . engag[ing] in legal proceedings").

14. *See infra* Part III (documenting the many ways that self-help backfires).

information asymmetries, data subjects struggle to distinguish successful strategies from self-defeating ones. Absent accurate intelligence about various techniques and firms' responses to them, consumers cannot escape self-help's unintended consequences, including overexposure and overreliance.

When self-help backfires, the conventional wisdom holds that courts and regulators should develop legal remedies that substitute for self-help.[15] But that approach fails to appreciate the extent to which privacy law harnesses self-help's preference signaling and resource conserving functions. Displacing self-help would inadvertently disable the many doctrines that depend on those functions.

Instead, legal institutions protect consumers best when they complement—rather than replace—self-help. By supplying intelligence about self-help, this approach empowers data subjects to identify proven practices and avoid unreliable ones. By diminishing the asymmetries that distort consumers' self-help decisions, this approach strengthens the doctrines that rely on those decisions to discover data's value. And by repurposing pre-existing tools, this approach avoids the costs associated with implementing new legal rules.

More broadly, complementing self-help is appealing because it makes the most of regulators' limited resources. Thanks to self-help's popularity, even small decreases in asymmetries may translate into substantial improvements in individuals' ability to manage privacy risks. Ultimately, complementing self-help is a promising tool to promote consumer privacy that has been overlooked for too long.

To be clear, self-help is no substitute for legislative and regulatory efforts to protect consumers. Instead, self-help works best when used to address the kinds of privacy risks that more traditional tools overlook. When consumers seek to act on their own idiosyncratic preferences quickly and cheaply, self-help excels. When they face persistent and systemic risks, however, regulatory enforcement and civil litigation assume heightened importance. So, while complementing self-help represents an under-appreciated tool for advancing consumer privacy, it represents only one tool in a larger toolbox.

This Article's exploration of the promise and perils of self-help continues in Part II with a taxonomy of self-help strategies, including concealment, obfuscation, and monitoring. Marshalling evidence from a variety of disciplines, it shows that self-help has emerged as one of the main ways that consumers protect their data.

15. *See, e.g.*, Lichtman, *supra* note 11, at 26; *see also infra* Part V.

Part III shows that certain self-help strategies produce unintended consequences, including: (1) privacy-privacy tradeoffs, (2) security-privacy tradeoffs, and (3) arms races. Information asymmetries prevent consumers from appreciating or avoiding these unforeseen harms.

Part IV highlights privacy law's surprising dependence on self-help. From the Fourth Amendment to the Federal Trade Commission's (FTC) unfairness authority, courts and regulators harness self-help to identify disputes that warrant attention and to conserve scarce judicial and regulatory resources.

Part V outlines a novel regulatory strategy. Rather than replace self-help, as the conventional wisdom suggests, courts and regulators should facilitate it. To illustrate the virtues of complementing self-help, this Part identifies three ways that legal institutions can intervene to address information asymmetries. Each intervention mobilizes pre-existing tools to arm data subjects with intelligence about self-help.

II. SELF-HELP IN PRACTICE

Twenty-five years ago, the FTC gathered scholars, technologists, and policymakers to discuss what was then the "new high-tech, global marketplace."[16] In a white paper summarizing that session, the Commission predicted that "private initiatives" such as "technology-based consumer protections and self-help opportunities" would be the key to safeguarding privacy in the twenty-first century.[17]

Consistent with the FTC's early optimism, almost every organization that advises consumers about privacy endorses self-help. Advocacy groups, such as the Electronic Frontier Foundation (EFF), champion self-help technologies.[18] Similarly, leading newspapers—including the *New York Times*, *Wall Street Journal*, and *Washington Post*—recommend self-help strategies.[19] Popular

16. FED. TRADE COMM'N., ANTICIPATING THE 21ST CENTURY: CONSUMER PROTECTION POLICY IN THE NEW HIGH-TECH, GLOBAL MARKETPLACE (1996), https://www.ftc.gov/system/files/documents/reports/anticipating-21st-century-competition-policy-new-high-tech-global-marketplace/gc_v2.pdf.

17. *Id.* at 46.

18. Opsahl, *supra* note 4; *see also EPIC Online Guide to Practical Privacy Tools*, ELEC. PRIV. INFO. CTR., https://www.epic.org/privacy/tools.html (last visited July 18, 2021).

19. *See, e.g.*, Jonah Engel Bromwich, *Protecting Your Digital Life in 9 Easy Steps*, N.Y. TIMES (Nov. 16, 2016), https://www.nytimes.com/2016/11/17/technology/personaltech/encryption-privacy.html; Jennifer Valentino-DeVries, *How to Avoid the Prying Eyes*, WALL ST. J. (July 30, 2010), https://www.wsj.com/articles/SB10001424052748703467304575383203092034876; Hayley Tsukayama, *Must Have Gifts for Those Who Want to Protect Their Data*, WASH. POST (Nov. 16, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/11/16/must-have-gifts-for-those-who-value-their-privacy; Adam Levin, *8 Ways to Protect*

magazines, from *Consumer Reports* to *Wired*, follow suit.[20] Even public schools "teach the basics of 'cyberhygiene,' a kind of preventative care for the digital self."[21] The bottom line is that self-help has become "the dominant advice that privacy-conscious citizens encounter."[22]

This Part asks whether consumers act on that advice. After developing a definition of self-help, this Part catalogs the techniques that consumers currently practice. As quantitative and qualitative evidence attests, privacy self-help is pervasive, persistent, and varied. Though self-help is not the only way that consumers protect their personal data, it has become an important part of the picture.

A. DEFINING SELF-HELP

Before surveying consumer strategies, it is essential to clarify what counts as privacy self-help. This Article defines privacy self-help as any action that: (1) safeguards personal data, (2) without resorting to the legal system, and (3) without relying on markets.

The first element concentrates on consumer activities that safeguard personal data. While scholars dispute how to define privacy, all agree that privacy has to do with protecting personal data.[23] By analyzing various practices in terms of their effect on personal data, rather than on privacy, this Article aims to be precise about what each practice accomplishes.

The second element, which excludes legal remedies, comports with every scholarly understanding of self-help. Indeed, even the broadest definitions of self-help do not include legal remedies.[24] Self-help is many things, but it is not law.

The final element distinguishes between self-help and market activity.[25] On first glance, the line between those categories may appear blurry, or even non-

Your Privacy Online, USA TODAY (Apr. 16, 2016), https://www.usatoday.com/story/money/personalfinance/2016/04/16/8-ways-protect-your-privacy-online/83056240.

20. *66 Ways to Protect Your Privacy Right Now*, CONSUMER REP. (Feb. 22, 2017), https://www.consumerreports.org/privacy/66-ways-to-protect-your-privacy-right-now; Lil Miss Hot Mess, *infra* note 78.

21. FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 53 (2015).

22. SARAH E. IGO, THE KNOWN CITIZEN: A HISTORY OF PRIVACY IN MODERN AMERICA 364–65 (2018).

23. *See, e.g.*, Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U.L. REV. 1814, 1835 (2011) (grappling with the various shortcoming of current legal models for defining personally identifiable information).

24. *See, e.g.*, Lichtman, *supra* note 11, at 25.

25. For a discussion of the similarities between self-help and market activity, see *infra* Part V.B.3.

existent. When a user buys an app that detects hidden cameras, for instance, is that an act of self-help, or a market transaction? To simplify matters, this Article defines market activity to encompass any practice where consumers switch between competing service providers. For example, an internet user who abandons Google in favor of DuckDuckGo (a search engine that emphasizes privacy) has engaged in market activity, not self-help.

Drawing the line here makes sense. In theory, whether competition protects privacy depends on factors, such as the structure of the market, the presence of competitors, and the non-privacy features of competing products, that are often irrelevant to self-help's success.[26] In practice, this definition of market activity has the advantage of ensuring that this Article does not repeat prior work, which extensively analyzes the relationship between competition and privacy while saying little about the strategies described below.[27]

To sum up, the best way to define self-help is by clarifying what it is not. Consumers who seek to protect their data have three types of precautions to choose from: self-help, market activity, and legal remedies. Table 1, below, outlines this menu of options. Privacy self-help describes those precautions that do not involve legal remedies or market activity.

Table 1: Precautions to Protect Personal Data

Self-Help	Market Activity	Legal Remedies
E.g., Submitting a false name, covering laptop cameras, or shredding credit cards.	*E.g.*, Deleting an account or reducing Facebook use in favor of a competitor.	*E.g.*, Joining a class action or filing a complaint with state or federal regulators.

B. SURVEYING SELF-HELP

Until now, scholars have paid little attention to privacy self-help. Though prior work has occasionally discussed specific strategies that fall within the definition introduced above, none surveys privacy self-help as a whole.[28] To

26. For an analysis of the considerations that influence self-help's effectiveness, see *infra* Part II.

27. *See, e.g.*, Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2060 (2004) (developing a model of how privacy law should regulate the "data trade"); ERIC A. POSNER & E. GLEN WEYL, RADICAL MARKETS: UPROOTING CAPITALISM AND DEMOCRACY FOR A JUST SOCIETY 205–49 (2018) (proposing the creation of a market for "data labor"); Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1883–88 (2013) (discussing the cognitive biases that limit individuals' ability to navigate privacy in the marketplace).

28. *See supra* note 11 (collecting prior works that touch on specific self-help strategies).

fill that void, this Section marshals evidence from a variety of disciplines—from computer science to sociology—that attests to self-help's popularity and diversity.

As the examples below illustrate, most self-help strategies share two features. First, popular techniques are invariably inexpensive; for example, common practices involve downloading free apps, covering phone cameras, and deleting files.[29] Such strategies enable individuals to avoid the fees that often accompany legal remedies.[30] Second, self-help "makes possible diverse, individuated judgments."[31] Put differently, self-help empowers individuals—not courts, regulators, or firms—to decide which data points warrant protection. Together, these features explain self-help's appeal.

To organize the diverse strategies that data subjects practice, this Section introduces a three-part taxonomy: (1) *concealment strategies* limit information disclosure, (2) *obfuscation strategies* share false information, and (3) *monitoring strategies* review others' access to personal data. Table 2, below, summarizes that taxonomy.

Table 2: Taxonomy of Self-Help Strategies

Category	Sub-Category	Example
Concealment	Identity data	Creating a temporary email address
	Sensitive data	Covering laptop and phone cameras
	Previously-disclosed data	Shredding sensitive documents
Obfuscation	Identity data	Using a fake name on social media
	Sensitive data	Submitting a fake address to avoid marketing requests
	Activity data	Generating fake social media "likes"
Monitoring	Personal monitoring	Using an app to detect hidden cameras
	Monitoring services	Hiring a reputation management service
	Monitoring networks	Writing app store reviews

1. Concealment Strategies

According to historian Sarah Igo, "[t]he most promising contemporary avenue for achieving [privacy]," involves "carefully designed practices for hiding one's tracks."[32] This Section describes three ways that data subjects

29. *See infra* notes 28–35.
30. *See* Ellickson, *supra* note 13, at 686.
31. Lichtman, *supra* note 11, at 7.
32. IGO, *supra* note 22, at 364–65.

cover their tracks: (1) concealing identifying information, (2) concealing sensitive information, and (3) retracting previously-disclosed data.

a) Concealing Identifying Information

Many practices prevent outsiders from discovering data subjects' identities. Common techniques include:

- **Creating Temporary Identifiers**: Data subjects routinely create temporary identities to safeguard their privacy.[33] About a quarter of consumers report using a temporary username or email address to conceal their identity, for instance.[34] Along the same lines, 18% of data subjects have employed public computers—for instance, workstations at a local library—to browse the internet without identifying themselves.[35] Another variant of this strategy is to pay with cash, not card. For example, *Time* instructs readers who "[d]on't want companies knowing [about] how much booze you're buying or other potentially embarrassing habits" to "[p]ay for things with cash."[36] And some individuals even obtain disposable "burner" phones or laptops to hide their identities—although this strategy is probably limited to journalists and spies.[37]

- **Employing Anonymization Technologies**: Some observers tout the benefits of anonymization technologies, such as "blind signatures, anonymous remailers, and encryption software."[38] Scholars call these tools Privacy Enhancing Technologies (PETs).[39] One example of a PET is The Onion Router, or Tor.[40] By hiding individuals' IP addresses, Tor permits them to browse the web without surveillance

33. In some cases, these practices may reflect motivations other than privacy. For example, some users may use fake email addresses to avoid spam, not to protect their anonymity. For the most part, this Article focuses on techniques for which privacy serves as the primary motivation.

34. Bruce Drake, *What Strategies Do You Use to Protect Your Online Identity?*, PEW RSCH. CTR. (Sept. 5, 2013), https://www.pewresearch.org/fact-tank/2013/09/05/what-strategies-do-you-use-to-protect-your-online-identity.

35. *Id.*

36. Christina DesMarais, *11 Simple Ways to Protect Your Privacy,* TIME (July 24, 2013), https://techland.time.com/2013/07/24/11-simple-ways-to-protect-your-privacy.

37. *See, e.g.*, Paul Sarconi, *Now's Probably the Time to Consider One of These Burner Phones*, WIRED (Feb. 3, 2017), https://www.wired.com/2017/02/7-great-burner-phones.

38. IGO, *supra* note 22, at 364–65.

39. *See* Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1410 (2011).

40. *See* WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 163 (2018).

by service providers or third parties. Unlike the other self-help strategies introduced in this Part, PETs have attracted sustained attention from scholars.[41] So far, however, consumers have not shown much interest in PETs. To take one example, just 2% of Americans employ anonymization software such as Tor.[42] The most plausible explanation is that only technologically-sophisticated consumers are able to take advantage of PETs.[43] So, while anonymization technologies deserve attention, concentrating on PETs alone would dramatically understate the popularity of privacy self-help.

b) Concealing Sensitive Information

Instead of hiding an individual's identity, some techniques conceal sensitive categories of information. Popular practices include:

- **Constructing Physical Barriers:** In many cases, consumers install physical coverings to conceal sensitive data. The best example of this approach involves using a sticker or tape to cover laptop and smartphone cameras.[44] This strategy has won the endorsement of the FBI.[45] The popularity of this technique reflects the sensitivity of the underlying data. Webcams collect pictures of users during their most intimate moments, an obvious threat to privacy. For similar reasons, some privacy-conscious consumers seal device microphones to thwart unauthorized listeners.[46] Going even further, more sophisticated

41. *See, e.g.*, Rubinstein, *supra* note 39, at 1417–21 (distinguishing between PETs that complement law and PETs that substitute for law). Even Brunton and Nissenbaum, who advocate for consumer obfuscation, primarily suggest technical strategies. *See* BRUNTON & NISSENBAUM, *supra* note 11, at 12 ("CacheCloak"); *id.* at 19 ("Tor relays"); *id.* at 21 ("Babble tapes").

42. Lee Rainie & Mary Madden, *Americans' Privacy Strategies Post-Snowden*, PEW RSCH. CTR. (Mar. 16, 2015), https://www.pewresearch.org/wp-content/uploads/sites/9/2015/03/PI_AmericansPrivacyStrategies_0316151.pdf.

43. *See, e.g.*, Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1673 n.383 (1999) ("Only those sophisticated enough to take advantage of public key encryption and anonymity filters may do so, with the rest of the population left defenseless due to ignorance.").

44. *See* Motherboard Staff, *The Motherboard Guide to Not Getting Hacked*, MOTHERBOARD (Nov. 14, 2017), https://motherboard.vice.com/en_us/article/d3devm/motherboard-guide-to-not-getting-hacked-online-safety-guide.

45. Violet Blue, *The FBI Recommends You Cover Your Laptop's Webcam, for Good Reason*, ENGADGET (Sept. 23, 2016), https://www.engadget.com/2016/09/23/the-fbi-recommends-you-cover-your-laptops-webcam-good-reasons.

46. *See, e.g.*, Kellen Beck, *Covering Your Webcam Isn't Enough: Here's How to Disable Your Computer's Microphone*, MASHABLE (June 22, 2016), https://mashable.com/2016/06/22/computer-microphone-hack/.

consumers erect screens around their property to prevent aerial surveillance, a tactic that may become more common as drones fill the skies.[47]

- **Blocking Online Trackers:** An army of digital trackers follows consumers around the web, recording the sites they visit and the searches they run.[48] So it is no surprise that tracker-blocking tools have widespread appeal. Indeed, more than a third (41%) of Americans "set their browser to disable or turn off cookies."[49] Many others (21.9%) employ apps or browser add-ins to block ads and web trackers.[50] In many cases, these technologies are free and easy to install. While these apps do not shield users' identities completely, they limit the amount of sensitive data third-party sites collect.

c) Concealing Previously-Disclosed Information

Once consumers disclose a piece of personal data, it usually passes out of their control forever.[51] That said, three techniques permit data subjects to retract data that they previously exposed but now wish to conceal:

- **Destroying Sensitive Data**: Consumer Reports recommends that readers shred any records that contain "social security number[s]," "birth date," "credit card numbers," "account numbers from financial institutions," and "medical insurance numbers."[52] This is not a new practice. As early as 2005, 51% of Americans claimed to "always" shred financial documents, such as credit cards and bills.[53] Today, advocates routinely advise consumers to wipe their computers of

47. *See, e.g.*, Carl Franzen, *The Anti-Drone Business Is About to Take Off*, POPULAR MECHANICS (May 1, 2015), https://www.popularmechanics.com/flight/drones/a15328/droneshield-anti-drone-business/; Heather Farmbrough, *Gatwick Fiasco Puts Anti-Drone Technology Under the Radar*, FORBES (Dec. 31, 2018), https://www.forbes.com/sites/heatherfarmbrough/2018/12/31/gatwick-fiasco-puts-anti-drone-technology-on-the-radar/#34cea2d37708.

48. *See* PASQUALE, *supra* note 21, at 33.

49. Drake, *supra* note 34.

50. *Privacy Goes Mainstream: People Take Action as Privacy Risks Increase*, DUCKDUCKGO (June 2, 2017), https://spreadprivacy.com/privacy-settings-survey.

51. *See* Solove, *supra* note 27, at 1902 (discussing the problem of unanticipated downstream uses of data).

52. CONSUMER REP., *supra* note 20.

53. ROBERT N. MAYER, AARP PUB. POL'Y INST., DEFENDING YOUR FINANCIAL PRIVACY: THE BENEFITS AND LIMITS OF SELF-HELP vi (2006), https://assets.aarp.org/rgcenter/consume/2006_06_privacy.pdf.

personal information before disposing of them.[54] In doing so, data subjects reduce the risk of identity theft—or that an unscrupulous firm will extract and resell their data.[55]

- **Asking Others to Delete Data:** Most of the time, other people control our data. For example, on social media, blogs, and photo-sharing sites, friends and family members routinely share data about one another. As a result, consumers may be able to conceal data by asking others to remove it. Indeed, one study found that more than 16% of respondents "have asked someone to remove or correct information about them that was posted online."[56]

- **Harnessing Ephemeral Communications Technologies:**[57] Another way to conceal previously disclosed data relies on ephemeral communication technologies.[58] The most prominent example is Snapchat, "a photo-sharing app in which images purportedly self-destruct after being viewed."[59] As a recent study confirms, data subjects employ Snapchat and other ephemeral software in an effort to "prevent[] the accumulation of meaningless and potentially embarrassing content."[60] Thanks to their ability to conceal personal data, ephemeral communications technologies have become

54. Tercius Bufete, *How to Wipe a Computer Clean of Personal Data*, CONSUMER REP. (Sept. 6, 2017), https://www.consumerreports.org/computers/how-to-wipe-a-computer-clean-of-personal-data.

55. Recognizing that data deletion reduces risk, the FTC tells consumers how to clean their drives. *See* FED. TRADE COMM'N., HOW TO PROTECT YOUR DATA BEFORE YOU GET RID OF YOUR COMPUTER (Jan. 2020), https://www.consumer.ftc.gov/articles/how-protect-your-data-you-get-rid-your-computer.

56. Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RSCH. CTR. 7 (Nov. 12, 2014), https://www.pewinternet.org/2014/11/12/public-privacy-perceptions.

57. As we shall shortly see, not all ephemeral communication technologies live up to their promise. *See infra* Part III.A.

58. Ephemeral communications technologies can be classified as a form of self-help, as a form of market activity, or both. By switching from one app to the other, consumers encourage firms to respect privacy. As this example suggests, some techniques combine the features of market activity and self-help.

59. DANAH BOYD, IT'S COMPLICATED: THE SOCIAL LIVES OF NETWORKED TEENS 64 (2014).

60. Bin Xu, Pamara Chang, Christopher L. Welker, Natalya N. Bazarova & Dan Cosley, *Automatic Archiving Versus Default Deletion: What Snapchat Tells Us About Ephemerality in Design*, PROC. 19TH ACM CONF. ON COMPUT. SUPPORTED COOP. WORK & SOC. COMPUTING 1662, 1663 (2016).

immensely popular; in 2020, for example, Snapchat reported an average of more than 260 million daily active users.[61]

2. Obfuscation Strategies

Another way that consumers protect their data is by producing "ambiguous, confusing, or misleading information to interfere with surveillance and data collection."[62] This Section outlines three ways that data subjects confound observers: (1) obfuscating identifying information, (2) obfuscating sensitive information, and (3) obfuscating activity.

a) Obfuscating Identifying Information

The best example of how consumers use obfuscation to shield their identities comes from a study of teens' Facebook use. To open an account, Facebook demands that users provide "the name you use in everyday life."[63] Needless to say, this policy makes it difficult for Facebook users to conceal their identities. In response, "many teens . . . offer[ ] up only their first name, preferring to select a last name of a celebrity, fictional character, or friend."[64] Indeed, about 26% of teen social media users "post fake information like a fake name . . . to help protect their privacy."[65] This practice shields teens' identities and retaliates against what they perceive as unnecessarily intrusive policies.[66]

As today's tech-savvy teens mature into adults, this variety of obfuscation is likely to grow even more popular. In fact, a 2013 survey revealed that 18% of Americans used a "fake name" or "untraceable username" online.[67] Since then, obfuscation techniques have become more sophisticated. For example, an app called MySudo "allows a user to create multiple email addresses and

61. Todd Spangler, *Snapchat Daily Users Pop 22% in Q4*, VARIETY (Feb. 4 2021), https://variety.com/2021/digital/news/snapchat-q4-2020-earnings-1234901096/.

62. BRUNTON & NISSENBAUM, *supra* note 11, at 1. Brunton and Nissenbuam were the first to use the term "obfuscation" to describe these types of techniques.

63. *Terms of Service*, FACEBOOK, https://www.facebook.com/terms.php (last visited Oct. 22, 2020).

64. BOYD, *supra* note 59, at 46.

65. Mary Madden, Amanda Lenhart, Sandra Cortesi, Urs Gasser, Maeve Duggan, Aaron Smith & Meredith Beaton, *Teens, Social Media, and Privacy*, PEW RSCH. CTR. (May 21, 2013), https://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/.

66. BOYD, *supra* note 59, at 46.

67. Lee Rainie, Sara Kiesler, Ruogo Kang & Mary Madden, *Anonymity, Privacy, and Security Online*, PEW RSCH. CTR. (Sept. 5, 2013), https://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/.

phone numbers for $1 a month."[68] According to MySudo's creators, switching phone numbers and emails "eliminate[s] the ability of advertisers, scammers, and other 3rd parties [to build] a detailed profile of [users'] personal information."[69] Similar apps have been downloaded over a million times.[70] In short, strategies that obscure users' identities have become surprisingly common.

b) Obfuscating Sensitive Information

Consumers practice obfuscation not just to shield their identities but also to protect particularly sensitive information. For instance, *Consumer Reports* warns parents not to submit accurate data when registering "connected kids' products" as it "essentially provides marketers and potential hackers with details about your children."[71] Instead, the magazine directs parents to "provid[e] fake information" such as inputting "Bart Simpson's [address]—742 Evergreen Terrace."[72] Though quantitative research on this topic is limited, the available evidence suggests that many consumers falsify sensitive data in certain circumstances.[73]

The appeal of obfuscating sensitive data—rather than obscuring one's identity altogether—is that it permits consumers to pick and choose which data points to protect. As a Pew interviewee explained, "[f]or any non-essential website . . . I choose to not share my real birthday. I understand the marketing and demographic component of why they collect birthday information so I choose a fake birthday [that] is similar to my real birthday."[74] By submitting information that is only partially misleading, savvy consumers capture disclosure's benefits while mitigating its dangers.

68. Joel Stein, *I Tried Hiding from Silicon Valley in a Pile of Privacy Gadgets*, BLOOMBERG (Aug. 8, 2019), https://www.bloomberg.com/news/features/2019-08-08/i-tried-hiding-from-silicon-valley-in-a-pile-of-privacy-gadgets.

69. *MySudo*, APPLE APP STORE, https://apps.apple.com/us/app/mysudo/id1237892621#?platform=ipad (last visited Jan. 10, 2020).

70. *See, e.g.*, *Burner*, GOOGLE PLAY STORE, https://play.google.com/store/apps/details?id=com.adhoclabs.burner&hl=en_US (last visited Jan. 10, 2020).

71. CONSUMER REP., *supra* note 20.

72. *Id.*

73. *See, e.g.*, Mayer, *supra* note 53, at 20 (summarizing survey evidence showing that between 24 and 34 percent of respondents had "supplied false personal information" to a website).

74. *Americans Conflicted About Sharing Personal Information with Companies*, PEW RSCH. CTR. (Dec. 30, 2015), https://www.pewresearch.org/fact-tank/2015/12/30/americans-conflicted-about-sharing-personal-information-with-companies.

c) Obfuscating Activity

Another obfuscation strategy involves manufacturing false activity to confuse observers. For example, web searches "end up acting as lists of [consumers'] locations, names, interests, and problems."[75] More often than not, "our identities can be inferred from these lists, and patterns in our interests can be discerned."[76] To address that problem, researchers developed TrackMeNot, an app 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."[77]

Not every variant of this strategy depends on sophisticated technologies (such as TrackMeNot) to generate false activity. Consider two examples:

- **Fabricating Social Media Inputs:** As *Wired* sees it, Facebook users should "throw[ ] the company off [their] scent" by hiding their "real interests within a sea of not-quite-real information."[78] To that end, the magazine urges readers to "lik[e]" random posts, "mis-tag[ ] photos of friends," and "click[ ] all of the ads."[79] What makes this type of activity attractive is that it promises "to confuse Facebook's facial recognition and computer vision algorithms."[80]

- **Swapping Loyalty Cards:** Another low-tech strategy involves retail store loyalty-card programs, which collect data on consumer purchasing habits.[81] In this strategy, practitioners "share[ ] cards . . . in *ad hoc* physical meetings, [and] with the help of mailing lists and online social networks, increasingly in large populations and over wide geographical regions."[82] By swapping loyalty cards, consumers create false purchasing data, confounding retailers' efforts to analyze their behavior.

75. BRUNTON & NISSENBAUM, *supra* note 11, at 13.

76. *Id.*

77. RICHARDS & HARTZOG, *supra* note 11, at 1190.

78. Lil Miss Hot Mess, *A Drag Queen's Guide to Protecting Your Privacy on Facebook by Breaking the Rules*, WIRED (Apr. 3, 2018), https://www.wired.com/story/opinion-facebook-privacy.

79. *Id.*

80. *Id.*

81. Lee Rainie & Maeve Duggan, *Scenario: Consumer Loyalty Cards and Profiling*, PEW RSCH. CTR. (Jan. 14, 2016), https://www.pewinternet.org/2016/01/14/scenario-consumer-loyalty-cards-and-profiling.

82. BRUNTON & NISSENBAUM, *supra* note 11, at 28–29.

3. Monitoring Strategies

By monitoring their data, consumers mitigate a wide range of privacy risks, from identity theft to phishing. The appeal of monitoring is that it multiplies the odds that consumers will detect privacy violations, deterring abuse by firms. At the same time, monitoring tells consumers when to engage in concealment and obfuscation, amplifying the effectiveness of other forms of self-help. This Section introduces three ways that data subjects monitor their data: (1) personal monitoring, (2) monitoring services, and (3) monitoring networks.

a) Personal Monitoring

"Carefully monitor [your] accounts for suspicious activity."[83] If there is one piece of self-help advice that consumers receive more than any other, this is it. Indeed, "[t]he FTC, the California Office of Privacy Protection, the Privacy Rights Clearinghouse, Consumer Reports, and various self-help guides" all instruct data subjects to monitor their accounts.[84] Consumers put that advice into practice in the following ways:

- First, after the typical data breach, 24% of affected individuals became "more diligent" in monitoring their accounts.[85] By stepping up monitoring activity, consumers uncover misbehavior by firms—including follow-on data breaches and violations of privacy policies.

- Second, as *Consumer Reports* recognizes, readers are interested in "ferreting out which companies are sharing [their] data."[86] To that end, the magazine suggests that subscribers "[t]ype '+' before the @ symbol [in an email] and add the website's name. Email[s] addressed to YourName+Websitename.com@gmail.com will go to the regular inbox for YourName@gmail.com. But now it will carry an extra crumb of data, and if you get spam from a company you've never heard of, you'll know whom to blame."[87]

83. Paul M. Schwartz, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 949 (2007).

84. *Id.*

85. LILLIAN ABLON, PAUL HEATON, DIANA CATHERINE LAVERY & SASHA ROMANOSKY, CONSUMER ATTITUDES TOWARDS DATA BREACH NOTIFICATIONS AND LOSS OF PERSONAL INFORMATION 30 (2016), https://www.rand.org/content/dam/rand/pubs/research_reports/RR1100/RR1187/RAND_RR1187.pdf.

86. CONSUMER REP., *supra* note 20.

87. *Id.*

- Finally, consumers download smartphone apps designed to detect hidden cameras positioned by employers, retailers, and hoteliers. For example, more than a million people have installed "Hidden Camera Detector," an app that analyses "magnetic activity" to pinpoint concealed webcams.[88] In the wake of national news coverage of a $100 million lawsuit alleging that a Hilton employee secretly recorded a hotel guest, camera-detection apps are likely to grow even more popular.[89]

b) Monitoring Services[90]

To defend their data, individuals enlist third-party services that offer the digital equivalent of home security monitoring. Examples abound:

- First, major companies—including Experian, Equifax, and TransUnion—offer credit monitoring services. Advocacy groups routinely urge consumers to make use of these services. Privacy Rights Clearinghouse, for instance, instructs readers to "monitor your credit reports on an ongoing basis" and request "one free credit report per year from each of the three credit bureaus."[91]

- Second, going beyond credit reporting, some consumers employ comprehensive monitoring services.[92] As Frank Pasquale reports, "[c]ontracting out reputation management to a private company is a growing 'market solution' to the emerging traffic in data."[93] Similar to a home security service, reputation managers "monitor an individual's online reputation . . . . [and] provide monthly reports to a client summarizing information about the client available online."[94] The most expensive options offer dedicated "lawyers to review [website] terms of service . . . and reputation managers to tend to . . . online

88. *See Hidden Camera Detector*, FUTUREAPPS (July 26, 2018), https://play.google.com/store/apps/details?id=hiddencamdetector.futureapps.com.hiddencamdetector&hl=en.

89. *See* Chris Boyette & Nicole Chavez, *A Woman Is Suing Hilton for $100M, Claiming She Was Secretly Filmed in the Shower and Blackmailed*, CNN (Dec. 5, 2018), https://www.cnn.com/2018/12/05/us/hilton-worldwide-hotel-hidden-camera-lawsuit/index.html.

90. These activities fall within this Article's definition self-help because monitoring services protect privacy even if consumers never switch (or threaten to switch) to competing providers. *See supra* Part II.A (distinguishing between market activity and self-help).

91. *Top 10 Tips to Protect Your Privacy*, PRIV. RIGHTS CLEARINGHOUSE (Jan. 24, 2013), https://www.privacyrights.org/blog/top-10-tips-protect-your-privacy.

92. *See, e.g.*, James Grimmelmann, *The Structure of Search Engine Law*, 93 IOWA L. REV. 1, 39 (2007) (describing search engine optimization (SEO) services as a form of "self-help directed at search engines").

93. PASQUALE, *supra* note 21, at 55.

94. Jacqueline D. Lipton, *Combating Cyber-Victimization*, 26 BERKELEY TECH. L.J. 1103, 1145–46 (2011).

profiles."[95] For those who can afford it, these services effectively outsource monitoring.[96]

c) Monitoring Networks

The most powerful form of monitoring depends on social networks, not service providers. In practice, consumers share privacy-related feedback through the following channels:

- **App stores:** The Google, Apple, and Microsoft app stores permit consumers to share their privacy concerns in the form of reviews. At best, the prospect of negative ratings may deter developers from using personal data in ways that diverge from users' expectations.[97] At a minimum, by complaining in app-store reviews, data subjects inform others about potential risks.[98]

- **Online communities:** Several popular online communities maintain dedicated channels for users to discuss privacy risks. For instance, Reddit hosts a page for privacy-concerned users to discuss vulnerabilities in consumer-facing technologies.[99] That forum boasts more than one million members.[100] Other social media platforms, such as Facebook or Twitter, also enable users to exchange information about privacy threats. By disseminating intelligence about negative privacy experiences (for example, an invasive ad or message), consumers may be able to discipline firms that violate privacy norms.

- **In-person networks:** Consumers also distribute information about privacy risks through in-person networks. After having their data lost in a breach, for instance, 17% of affected users elected to "notify

95. PASQUALE, *supra* note 21, at 55.

96. *See* Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1383–97 (2017) (describing the burgeoning "pay-for-privacy model," where consumers pay third parties to protect their data).

97. *See, e.g.*, Muhammad Ikram, Narseo Vallina-Rodriguez, Suranga Seneviratne, Mohamed Ali Kaafar & Vern Paxson, *An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps*, https://www.icir.org/vern/papers/vpn-apps-imc16.pdf (identifying negative ratings that identified security vulnerabilities).

98. Admittedly, this example straddles the line between self-help and market activity. To the extent that product reviews prompt consumers to conceal or obfuscate their identity when using a particular app, those reviews qualify as a form of self-help. To the extent that reviews encourage consumers to switch from privacy-invasive to privacy-protective apps, those reviews qualify as a form of market activity.

99. *See, e.g.*, *r/privacy*, REDDIT, https://www.reddit.com/r/privacy (last visited Jan. 6, 2020).

100. *Id.*

> others."[101] Even so-called digital natives prefer to get information about privacy from their network of friends, parents, and teachers rather than online sources.[102] In short, sharing negative gossip helps other consumers protect themselves, rebukes firms by damaging their reputation, and discourages future violations.

From this survey of privacy self-help, two themes emerge. First, most strategies involve low-cost ways for consumers to express their preferences. Those attributes explain much of self-help's appeal. Second, different strategies reduce risk in different ways. Any investigation of how law should respond to self-help must account for the diversity of consumer practices. The bottom line is that self-help represents one of the primary ways that data subjects manage privacy risks. The next Part asks whether courts and regulators share consumers' enthusiasm.

III. THE PERILS OF SELF-HELP

Too often, self-help strategies backfire. First, privacy-privacy tradeoffs mean that self-help may expose the data it promises to protect. Common techniques generate new data, enable firms to draw negative inferences, and tempt consumers to disclose more data than they would have otherwise. Second, security-privacy tradeoffs occur when consumers' practices exacerbate security vulnerabilities, disrupting the confidentiality, integrity, and availability of data. Finally, self-help sometimes sparks wasteful arms races between firms and their customers.

To be clear, the diversity of consumer practices results in an unpredictable landscape. Although some strategies are self-defeating, others are not. So, while many techniques give rise to unintended consequences, consumers need not abandon all forms of self-help.

The problem is that data subjects struggle to predict which strategies trigger unforeseen harms. As economists warn, "consumers are often in a position of imperfect or asymmetric information regarding when their data is collected, for what purposes, and with what consequences."[103] While the scholarly literature concentrates on how information asymmetries disrupt market transactions, those asymmetries also distort individuals' ability to

101. ABLON ET AL., *supra* note 85, at 30.

102. *See* Madden, *supra* note 65 (showcasing teens' comfort with privacy settings).

103. Alessandro Acquisti, Curtis R. Taylor & Liad Wagman, *The Economics of Privacy*, 54 J. ECON. LITERATURE 442, 442 (2016).

identify successful self-help strategies.[104] The bottom line is that, absent accurate intelligence about which techniques backfire, data subjects cannot escape self-help's unintended consequences.

As it stands, privacy law does little to address this problem. As explained above, existing doctrines look to self-help to discern individual preferences and conserve scarce resources. At best, those doctrines do nothing to help data subjects distinguish successful techniques from self-defeating ones. At worst, by encouraging consumers to practice self-help before seeking legal remedies, privacy law may promote techniques that backfire.

This Part documents three unintended consequences of self-help: (1) privacy-privacy tradeoffs, (2) security-privacy tradeoffs, and (3) arms races between firms and consumers. Table 3 catalogs these problems.

Table 3: The Unintended Consequences of Self-Help

Category	Sub-Category	Example
Privacy-Privacy Tradeoffs	Self-Help as Data Creation	Firms collect data about who uses self-help apps
	Negative Inferences	Consumers who check their credit score may betray that they are a credit risk
	Overreliance	Users send sensitive messages because they trust Snapchat's ephemeral communications feature
Security-Privacy Tradeoffs	Confidentiality	Scammers promise free credit monitoring, only to compromise user data
	Integrity	When consumers submit false data, security technologies malfunction
	Access	Breached firms cannot warn customers who conceal their contact information
Arms Races	Surveillance Technologies	Firms "fingerprint" devices to identify the owner
	Data Brokers	Firms buy concealed or obfuscated data from data brokers

A. PRIVACY-PRIVACY TRADEOFFS

Proponents of self-help assume that consumer strategies obscure more data than they expose. But that is not always the case. This Section introduces

104. *See, e.g.*, Solove, *supra* note 27, at 1880, 1895 (documenting the "structural problems" and "information asymmetries" that bedevil privacy decision-making); Acquisti et al., *supra* note 103, at 447 ("[T]he data subject may not know what the data holder will do with their data . . . .").

three privacy-privacy tradeoffs: (1) some strategies inadvertently create new data, (2) other strategies enable observers to draw negative inferences, and (3) still other strategies tempt consumers to share more and more sensitive data than they would have otherwise.[105]

1. Self-Help as Data Creation

Consumers who practice self-help risk exposing their intentions or behavior. This tradeoff affects concealment, obfuscation, and monitoring strategies alike.

First, consumers who practice concealment signal that they have something to hide. For example, the FTC warns that "sites you visit may be able to determine that you are using a VPN app."[106] That information is valuable because VPN use correlates with other attributes. Indeed, lawyers, journalists, and political activists all rely on VPNs. Thus, VPN users are likely to have a job that requires them to handle sensitive information.[107] The upshot is that, by employing VPNs, consumers advertise that they have access to especially valuable data.

Second, obfuscation strategies suffer from a similar problem. To illustrate how obfuscation works, Professors Brunton and Nissenbaum give the example of a military aircraft that drops chaff (bundles of small metal pieces) to confuse enemy radar.[108] In that scenario, obfuscation distracts the enemy by generating additional targets. But dropping chaff has an obvious disadvantage: it broadcasts that at least one real target is present. In the same way, a data subject who practices obfuscation may attract extra scrutiny, either because she appears to be a security threat[109] or because she inadvertently discloses that she has access to information worth protecting.[110]

Finally, even monitoring strategies may inadvertently create new data. The best example involves credit monitoring services. When lenders or card issuers check a consumer's credit score, it signals that the consumer may be about to take on new debt. "In the Heisenberg-meets-Kafka world of credit scoring," Pasquale warns, "merely trying to figure out possible effects on one's score can

105. Professor David Pozen coined the term "privacy-privacy tradeoffs." *See* David E. Pozen, *Privacy-Privacy Tradeoffs*, 83 U. CHI. L. REV. 221, 222 (2016).

106. Andrea Arias, *Virtual Private Networks (VPN) Apps*, FED. TRADE COMM'N. (Feb. 22, 2018), https://www.consumer.ftc.gov/blog/2018/02/shopping-vpn-app-read.

107. *See* BRUNTON & NISSENBAUM, *supra* note 11, at 89–90 (discussing the motivations for political protesters and journalists to adopt obfuscation techniques).

108. *Id.* at 8.

109. *See infra* Part III.B.

110. *See infra* Part II.B.2.

reduce it."[111] Indeed, one individual who repeatedly checked the ownership of his mortgage note "reported . . . a 40-point hit on his credit score after his inquiry."[112]

Unfortunately, many consumers do not appreciate this tradeoff. Economists often emphasize "how invisible [data] collection is to the data subject."[113] And, as the FTC's warning about VPNs illustrates, data collection about self-help is no more visible than data collection about any other activity.[114] Without intelligence about which self-help techniques generate personal data, consumers may not be able to distinguish effective practices from self-defeating ones.

2. Negative Inferences

Even when self-help shields personal data from direct observation, firms may be able to draw inferences based on the absence of data. Game theorists recognize that when a data subject declines to disclose information, that choice reveals something about the subject.[115] For example, suppose that you decide not to share certain data on online financial forms. In response, banks may infer that you are hiding undesirable characteristics, such as unpaid debts. Because observers can draw inferences based on the absence of information, concealing one piece of data often exposes other, more sensitive data.

What scholars call "unraveling effects" exacerbate this problem.[116] As Scott Peppet explains, "[a]t first, those with positive private information … will disclose to seek discounts and economic benefit."[117] Next, "even those with the worst private information . . . may realize that they have little choice but to disclose to avoid the stigma of keeping information secret."[118] Ultimately, "privacy may unravel as those who refuse to disclose are assumed to be withholding negative information and therefore stigmatized and penalized."[119]

---

111. PASQUALE, *supra* note 21, at 24.

112. *Id.*

113. Alessandro Acquisti, *Privacy and Market Failures: Three Reasons for Concern, and Three Reasons for Hope*, 10 J. TELECOMM. & HIGH TECH. L. 227, 229 (2012).

114. *See* FED. TRADE COMM'N., *supra* note 106.

115. *See* DOUGLAS G. BAIRD, ROBERT H. GERTNER & RANDAL C. PICKER, GAME THEORY AND THE LAW 89–95 (1998).

116. Scott R. Peppet, *Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future*, 105 NW. U.L. REV. 1153, 1156 (2011). The concept of "unraveling" in repeated games is not unique to privacy, but it derives from game theory. *See* BAIRD, *supra* note 115, at 89–95; Ian Ayres, *Playing Games with the Law*, 42 STAN. L. REV. 1291, 1306 (1990).

117. Peppet, *supra* note 116, at 1176.

118. *Id.*

119. *Id.* at 1156.

Thanks to unraveling effects, firms' ability to draw inferences depends on the volume of personal data they possess. The more consumers who disclose personal data, the more likely that firms will be able to draw negative inferences about those who choose to conceal their data. But data subjects typically lack information about the size and quality of firms' data sets.[120] For that reason, consumers struggle to predict whether or to what extent self-help will permit firms to draw negative inferences.

3. Overreliance

In some cases, the availability of self-help encourages consumers to expose personal data that they would not have otherwise. Generally, "higher perceived control over information publication increased [data] subjects' propensity to disclose sensitive information."[121] For example, consider Snapchat, an app that promises to protect users' communications.[122] But Snapchat did not always live up to that promise. At one point, users could capture screenshots or use third-party apps to save each other's messages.[123] If every Snapchat user had realized that recipients could preserve their communications, many would have sent fewer messages—or none at all.

As this example suggests, overreliance is only an issue when practitioners overestimate the effectiveness of a particular strategy. In Snapchat's case, technically-proficient users were able to detect the problem years before the FTC intervened.[124] The more difficult it is for consumers to assess the effectiveness of a given strategy, the greater the risk of overreliance.

The result is that consumers cannot assume that self-help obscures more data than it reveals. Many self-help techniques invite privacy-privacy tradeoffs, exposing more data—or more sensitive data—than practitioners anticipate.

B. SECURITY-PRIVACY TRADEOFFS

Every day, cybercriminals attempt to access consumer data. Every day, corporate security experts try to stop them.[125] More specifically, corporate

120. *See* Solove, *supra* note 27, at 1889.

121. Acquisti, *supra* note 113, at 230.

122. Complaint at 8, *In re* Snapchat, Inc., FTC File No. 1323078, No. C-450 (Dec. 23, 2014), https://www.ftc.gov/system/files/documents/cases/141231snapchatcmpt.pdf.

123. *Id.* at 3.

124. *See* Kashmir Hill, *Snapchats Don't Just Disappear: Forensics Firm Has Pulled Dozens of Supposedly-Deleted Photos from Android Phones*, FORBES (May 9, 2013), https://www.forbes.com/sites/kashmirhill/2013/05/09/snapchats-dont-disappear/#2801d2192bdd.

125. *See* Kim S. Nash, *For Many Companies, a Good Cyber Chief Is Hard to Find*, WALL ST. J. (May 15, 2017), https://www.wsj.com/articles/for-many-companies-a-good-cyber-chief-is-hard-to-find-1494849600 ("About 65% of large U.S. companies now have a CISO position . . . .").

security teams safeguard the confidentiality, integrity, and availability of customer data—what experts call the "CIA triad."[126] *Confidentiality* prevents unauthorized access to data, *integrity* verifies that data is accurate, and *availability* ensures that authorized users can access their data.[127]

Too often, privacy self-help disrupts the CIA triad. Borrowing from David Pozen, the previous Section used the term "privacy-privacy tradeoffs" to describe situations where "preserving privacy along a certain axis may entail compromising privacy along another axis."[128] This Section introduces a parallel concept, security-privacy tradeoffs, to refer to practices that bolster privacy at the expense of security. By compromising confidentiality, integrity, and availability, some self-help strategies frustrate firms' attempts to protect personal data.

1. Confidentiality

Champions of self-help often endorse technology-dependent strategies, such as hidden camera apps and VPNs.[129] But trusting third-party technologies has a downside: it opens the door for malicious attackers. In many cases, harmful programs masquerade as self-help-style software.[130] But once a consumer clicks a link or downloads a file, the application steals their data. The FTC has identified two examples of this security-privacy tradeoff:

- First, take Scareware, a type of malware that "falsely claim[s] that scans ha[ve] detected viruses, spyware, and illegal pornography on consumers' computers."[131] The FTC explains that these programs "trick consumers into thinking their computers [a]re infected with malicious software" and then "s[ell] [the consumers] software to 'fix' the[] non-existent problem."[132] In this way, self-help provides an opportunity for cybercriminals to trick consumers into downloading applications that compromise their data.

126. Kristen E. Eichensehr, *Giving up on Cybersecurity*, 64 UCLA L. REV. DISCOURSE 320, 324 (2016).

127. *See* BRUCE SCHNEIER, CLICK HERE TO KILL EVERYBODY: SECURITY AND SURVIVAL IN A HYPER-CONNECTED WORLD 78 (2018) (explaining that the CIA triad aims to prevent outsiders from "steal[ing] a copy of [data], modify[ing] it, or delet[ing] it.").

128. Pozen, *supra* note 105, at 222.

129. *See supra* Part 0.

130. *See How to Spot, Avoid and Report Tech Support Scams*, FED. TRADE COMM'N. (Feb. 2019), https://www.consumer.ftc.gov/articles/0263-free-security-scams [https://perma.cc/QYV9-8NY9].

131. *Operator of Deceptive "Scareware" Scheme Will Pay More than $8 Million to Settle FTC Charges*, FED. TRADE COMM'N. (Jan. 27, 2011), https://www.ftc.gov/news-events/press-releases/2011/01/operator-deceptive-scareware-scheme-will-pay-more-8-million.

132. *Id.*

- Second, experts warn that some VPNs exacerbate security vulnerabilities.[133] "[W]hen you use a VPN app," the FTC says, "you are giving the app permission to intercept all of your internet traffic."[134] As security researchers caution, some "VPN apps . . . expose users to serious privacy and security vulnerabilities, such as use of insecure VPN tunneling protocols."[135]

Information asymmetries prevent consumers from discerning these unintended consequences. According to one survey, for instance, "only a marginal number of . . . users" recognize that VPN apps may reveal personal data.[136] If consumers cannot distinguish applications that protect personal data from ones that expose it, self-help may do more harm than good. At a minimum, by encouraging data subjects to take privacy into their own hands, self-help opens the door for Scareware and unreliable VPNs.

2. Integrity

Self-help also threatens the second component of the CIA triad: data integrity. To see why, it is helpful to have a basic understanding of anomaly-based intrusion detection systems (IDS).[137] Firms rely on these systems to "detect intrusion attempts by comparing current account activities against a 'normal activity profile.' "[138] "When the IDS detects abnormal activity (outside normal boundaries as identified in the baseline)," cybersecurity expert Darril Gibson explains, "it gives an alert indicating a potential attack."[139] In doing so, these systems safeguard customer data from hackers and other threats.

The problem with practices that ask users to act "outside normal boundaries" is that they risk triggering false IDS alerts.[140] Obfuscation strategies may be the worst offender. By definition, submitting large volumes of false searches or clicks will be "abnormal" compared with consumers'

133. Andrea Arias, *Shopping for a VPN app? Read this.*, FED. TRADE COMM'N. (Feb. 22, 2018), https:// www.consumer.ftc.gov/blog/2018/02/shopping-vpn-app-read.

134. *Id.*

135. Ikram et al., *supra* note 97, at 1.

136. *Id.* at 6 ("Only less than 1% of the negative reviews relate to security and privacy concerns, including the use of abusive or dubious permission requests and fraudulent activity . . . .").

137. *See, e.g.*, Arnt Brox, *Signature-Based or Anomaly-Based Intrusion Detection: The Practice and Pitfalls*, SC MEDIA (May 1, 2002), https://www.scmagazine.com/home/security-news/features/signature-based-or-anomaly-based-intrusion-detection-the-practice-and-pitfalls.

138. Michael Lee, Sean Park, Tae Kim, David Lee, Aaron Schapiro & Tamer Francis, *Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory Proposal*, 14 BERKELEY TECH. L.J. 839, 853 (1999).

139. Darril Gibson, COMPTIA SECURITY+ GET CERTIFIED GET AHEAD 181 (2014).

140. *Id.*

baseline. If a user starts submitting random searches in Vietnamese, for example, an IDS may not be able to tell whether the sudden behavior change is the product of an obfuscation strategy or a hacker's intrusion. In other words, IDS technologies may interpret obfuscation as a sign that a malicious attacker has gained access to customer accounts. The sad reality is that, because obfuscation produces false positives, it confuses the security systems designed to protect consumer data.

Few data subjects appreciate this tradeoff. As Pew Research complains, "many [Americans] struggle with more technical cybersecurity concepts."[141] If consumers do not understand security basics, they cannot identify which self-help techniques are likely to interfere with companies' security efforts.

3. Availability

In addition to threatening confidentiality and integrity, self-help also endangers the availability of data, the final component of the CIA triad. Consider three examples:

- First, imagine that you run a data processing firm. Your security team discovers that a data breach has occurred. In turn, your lawyers recommend that you notify affected users about the breach.[142] To do so, you need access to valid names, email addresses, or phone numbers for each user. On reviewing the relevant records, however, you discover that many customers have concealed their contact information. As this example illustrates, strategies that shield consumers from unwanted communications from firms may inadvertently prevent them from receiving essential notifications.

- Second, Facebook assumes that accounts with fake names involve "malicious intent to violate [their] policies."[143] Accordingly, the social media giant promises to "remove" the accounts of users who practice obfuscation.[144]

141. Aaron Smith, *What the Public Knows About Cybersecurity*, PEW RSCH. CTR. (Mar. 22, 2017), https://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity.

142. *See* CAL. CIV. CODE § 1798.29 (West 2006).

143. *Fake Accounts*, FACEBOOK, https://transparency.fb.com/data/community-standards-enforcement/fake-accounts/facebook/ (last visited Aug. 15, 2021).

144. *See Community Standards Enforcement Preliminary Report*, FACEBOOK, https://transparency.facebook.com/community-standards-enforcement#fake-accounts (last visited Oct. 30, 2020) (reporting that Facebook disabled 583 million fake accounts in the first quarter of 2018 alone).

- Third, suppose that you practice obfuscation by submitting false names, email addresses, and security questions. The simple fact that it can be more difficult to remember many different lies than it is to recall a single truth may mean that consumers who practice obfuscation ultimately struggle to authenticate their identities and regain access to their accounts.

Again, data subjects do not always take this tradeoff into account when deciding whether to engage in self-help. Indeed, a recent survey found that "a significant share of online adults are simply not sure of the correct answer on a number of cybersecurity knowledge questions."[145] Without an understanding of security basics, consumers may struggle to predict which self-help strategies will cause them to lose access to their data.

To be clear, not every strategy undermines security. Indeed, some low-tech strategies shield both privacy and security. Covering laptop cameras, for example, protects data from both firms and hackers. The trouble is that, if consumers do not appreciate security tradeoffs, they cannot tell which strategies endanger data security.

C. ARMS RACES

Consumers do not have a monopoly on self-help. To the contrary, "self-help can initiate wasteful 'arms races' between providers and consumers."[146] These arms races are distinct from the privacy-privacy tradeoffs introduced above. Section III.A argued that some self-help strategies are self-defeating because they create new data, permit negative inferences, and induce over-reliance. During an arms race, by contrast, firms counter consumer self-help with strategies of their own.

The best-documented example of an arms race between consumers and firms involves copyright protection.[147] At the start of the race, consumers share content in violation of copyright restrictions through tools like LimeWire. Then creators respond by "develop[ing] more secure, tamper-resistant management systems."[148] At the end of the day, consumers and content creators would be better off cooperating.[149] But because they are trapped in a

145. Smith, *supra* note 141.

146. Lee Kovarsky, *A Technological Theory of the Arms Race*, 81 IND. L.J. 917, 918 (2006).

147. Dan L. Burk, *Muddy Rules for Cyberspace*, 21 CARDOZO L. REV. 121, 167 (1999).

148. *Id.*

149. *See* Stephen J. Majeski, *Arms Races as Iterated Prisoner's Dilemma Games*, 7 MATHEMATICAL SOC. SCI. 253, 253 (1984) ("[I]ndividually rational behavior does not lead to a cooperative, group preferred outcome.").

prisoner's dilemma, rational decisions on each side lead to "wasteful investment[s]" in "hacking and protection technology."[150]

Privacy arms races follow a similar pattern. When consumers practice self-help, the economics of personal data encourage firms to respond with strategies of their own. As *The Economist* observes, personal data is the new oil.[151] It follows that when self-help strategies reduce the quantity of data available, firms have a powerful incentive to circumvent those strategies.[152] To do so, firms either: (1) install surveillance technologies, or (2) buy personal data from brokers.

1. Surveillance Technologies

The most obvious way to circumvent self-help is through surveillance technologies. Imagine, for instance, that customers start refusing to fill out forms on a company's website. In response, that company may decide to deploy trackers that follow the customer around the internet. Today, such counterattacks by firms are commonplace.[153]

For the most part, firms prefer surveillance technologies that consumers cannot detect. Take "fingerprinting," a technique that "uniquely identif[ies] computers" by reference to details such as "clock setting, different fonts, [and] different software."[154] As the *Wall Street Journal* reports, "fingerprinting is largely invisible" to consumers.[155] Indeed, "[i]t's tough even for sophisticated Web surfers to tell if their gear is being fingerprinted."[156]

For another example, consider a recent study that attempted to identify all of the ways that Facebook gathers personal data. The researchers found that the social media giant consolidates data from the Facebook Messenger app, phone contact lists, and data uploaded to user accounts for "two-factor

150. Burk, *supra* note 147, at 167.

151. *Regulating the Internet Giants: The World's Most Valuable Resource Is No Longer Oil, but Data*, ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

152. *See* Imanol Arrieta Ibarra, Leonard Goff, Diego Jimenez Hernandez, Jaron Lanier & E. Glen Weyl, *Should We Treat Data as Labour? Moving Beyond "Free"*, AEA ARTICLES. & PROC. 2 (May 2018) (stressing the importance of accurate data for machine learning); POSNER & WEYL, *supra* note 27, at 221 (observing that insufficient data can preclude the development of working algorithms).

153. *See* PASQUALE, *supra* note 21, at 53.

154. Julia Angwin & Jennifer Valentino-DeVries, *Race Is on to 'Fingerprint' Phones, PCs*, WALL ST. J. (Nov. 30, 2010), https://www.wsj.com/articles/SB10001424052748704679204575646704100959546.

155. *Id.*

156. *Id.*

authentication."[157] Even data "obtained without a user's knowledge, such as by some other user syncing their phone contacts . . . is used for PII-based advertising."[158]

As these examples indicate, firms identify creative ways to collect personal data without alerting consumers.[159] The appeal of these invisible data collection technologies is obvious: consumers cannot respond to a counterattack they cannot detect in the first place.

2. Data Brokers

Not all firms have access to the same surveillance technologies as Facebook. But they all have access to data brokers.[160] These entities "collect and maintain data on hundreds of millions of consumers."[161] Thanks to brokers, "[h]uge databases of usernames, credit card numbers, and social security numbers already exist online."[162] By selling access to those databases, brokers offer a cost-effective way to circumvent self-help.

Indeed, data brokers thrive because they enable counterattacking firms to avoid detection. To that end, many brokers refuse "to identify the specific sources of their data or the [firms] who purchase it."[163] In doing so, brokers make it "impossible for a consumer to determine the originator of a particular data element."[164] To understand which self-help strategies fall victim to data brokers, data subjects need information about the types of data that brokers sell and who they sell it to. Otherwise, consumers cannot predict when brokers will enable firms to circumvent self-help.[165]

Of course, not every self-help strategy sparks an arms race. While data brokers and surveillance technologies are powerful, their reach does not

157. Giridhari Venkatadri, Elena Lucherini, Piotr Sapiezynski & Alan Mislove, *Investigating Sources of PII Used in Facebook's Targeted Advertising*, SCIENDO: PROC. ON PRIV. ENHANCING TECHS. 227 (2018).

158. *Id.* at 240. PII stands for personally-identifiable information.

159. *See, e.g.*, Acquisti, *supra* note 113, at 229 (commenting on "how invisible such collection is to the data subject").

160. *See* Steven H. Hazel, *Personal Data as Property*, 70 SYRACUSE L. REV. (forthcoming 2020).

161. S. COMM. ON COM., SCI., & TRANSP., A REVIEW OF THE DATA BROKER INDUSTRY: COLLECTION, USE, AND SALE OF CONSUMER DATA FOR MARKETING PURPOSES i (Dec. 18, 2013) [hereinafter A REVIEW OF THE DATA BROKER INDUSTRY].

162. PASQUALE, *supra* note 21, at 53.

163. *Id.* at iii.

164. FED. TRADE COMM'N., DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 14 (May 2014).

165. *See id.* at iii.

extend to every person and every type of data.[166] But consumers struggle to distinguish strategies that are vulnerable to arms races from those that are not. Firms exacerbate this problem by engaging in invisible arms races. Unaware of hidden counterattacks, data subjects fail to adopt alternative strategies that could better protect their data. At the same time, consumers continue to waste resources implementing unsuccessful strategies, harming social welfare.

Taken together, privacy-privacy tradeoffs, security-privacy tradeoffs, and arms races threaten self-help's appeal. In an ideal world, consumers would avoid strategies that backfire and prioritize ones that succeed. But information asymmetries limit consumers' ability to discern which strategies produce unforeseen harms. So, absent accurate intelligence about various strategies and firms' responses, consumers cannot escape self-help's unintended consequences.

IV. HOW PRIVACY LAW HARNESSES SELF-HELP

What, if anything, should privacy law do about self-help? To answer that question, it is first necessary to understand the relationship between existing privacy doctrines and self-help. For the most part, the same attributes that make self-help appealing to consumers also make it useful to legal institutions. First, self-help's *preference signaling* function helps adjudicators discern which types of data consumers view as sensitive.[167] Second, self-help's *resource conserving* function resolves low-value disputes that would otherwise consume scarce judicial and regulatory resources.[168] Over time, privacy law has come to depend on these functions.

To illustrate how existing doctrines harness self-help, this Part introduces five disparate examples: the Fourth Amendment, the Electronic Communications Privacy Act (ECPA), Article III standing, privacy torts, and state data breach notification laws. Each doctrine depends on self-help to identify disputes that warrant attention and to husband judicial and regulatory resources.

166. *See* DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? 218 (1998) (positing that firms are less likely to circumvent unpopular strategies).

167. *See* Lichtman, *supra* note 11, at 19 (explaining that self-help "distinguish[es] the bulk of normal business information from that special subset of information that warrants protection").

168. *See, e.g.*, Ellickson, *supra* note 13, at 686 (noting that self-help avoids the "cost[s of] carry[ing] out legal research and . . . engag[ing] in legal proceedings").

A. THE FOURTH AMENDMENT

The Supreme Court's "reasonable expectation of privacy test" may be the best-known rule in privacy law. In *Katz v. United States*, the Court held that whether government activity counts as a Fourth Amendment search hinges on the searched citizen's "reasonable expectation of privacy."[169] In a concurrence, Justice Harlan set out the two-pronged test that courts continue to apply today. Under Harlan's test, the Fourth Amendment applies when: (1) the defendant exhibits a "subjective" expectation of privacy, and (2) that expectation is "one that society is prepared to recognize as 'reasonable.' "[170]

In elaborating the first prong, Justice Harlan warned that, "objects, activities, or statements that [a citizen] exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited."[171] This "knowing exposure" requirement clarifies that citizens who do not engage in reasonable self-help measures forfeit the Fourth Amendment's protection.[172] In *Katz*, for example, it was essential that the defendant had "shut[ ] the door" to the phone booth that the government surveilled.[173] Closing the door signaled that the defendant regarded his conversations within that booth as private. The same logic explains why citizens who fail to engage in reasonable forms of self-help—such as installing fencing,[174] affixing roof panels,[175] or securely disposing of garbage[176]—forfeit constitutional protection. Ultimately, *Katz*'s "knowing exposure" test looks at self-help to divine whether a given data point deserves protection.

B. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

Similar reasoning guides courts' analyses of the Electronic Communications Privacy Act (ECPA). That statute prescribes criminal and civil penalties for those who intercept electronic, oral, and wire communications.[177]

---

169. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

170. *Id.* at 361.

171. *Id.*

172. *Id.*

173. *Id.*

174. *See* United States v. Dunn, 480 U.S. 294, 303 (1987) (holding that respondent's interior fencing did not indicate a reasonable expectation of privacy).

175. *See* Florida v. Riley, 488 U.S. 445, 450 (1989) (declining to recognize a reasonable expectation of privacy in part because the defendant left "the sides and roof of his greenhouse . . . partially open").

176. *See* California v. Greenwood, 486 U.S. 35, 40–41 (1988) ("[S]ociety would not accept as reasonable respondents' claim to an expectation of privacy in trash left for collection in an area accessible to the public . . . .").

177. 18 U.S.C. § 2511.

In defining ECPA's scope, Congress imported *Katz*'s "knowing exposure" test. By its terms, the Act applies when plaintiffs "[exhibit] an expectation that such communication is not subject to interception under circumstances justifying such expectation."[178] To decide whether this requirement is satisfied, courts look to self-help. Indeed, ECPA only protects plaintiffs who take "common-sense precautions . . . to preserve their expectation of privacy," as the Fifth Circuit has observed.[179]

Consider *Huff v. Spaw*, where the chair of a corporate board pocket-dialed a colleague.[180] Though the colleague quickly realized that the chair had called her by accident, she stayed on the line for over an hour, listening in on an embarrassing conversation between the chair, the chair's spouse, and a third-party. In denying the chair's ECPA claim, the Sixth Circuit faulted him for failing to engage in any of the "simple and well-known measures [to] prevent pocket-dials."[181] For example, the plaintiff could have "lock[ed] the phone, set[ ] up a passcode, [or] us[ed] one of many downloadable applications that prevent pocket-dial calls."[182] The court even cited a magazine article that recommended self-help-style apps that reduce the risk of pocket dials.[183]

Huff illustrates how courts harness self-help's preference signaling function to reduce the cost of discerning data's value. Because the plaintiff failed to take self-help measures that would have protected his information, the Sixth Circuit was able to infer that his privacy interest was minimal.[184] At the same time, by requiring that plaintiffs practice "simple and well-known measures" before resorting to ECPA, the *Huff* court conserved judicial resources.[185] The bottom line is that, without ECPA's self-help requirement, courts would need to wrestle with many more low-value cases than they do today.

C. ARTICLE III STANDING IN DATA BREACH CASES

To satisfy Article III's standing requirement, plaintiffs must show an injury-in-fact that is "concrete and particularized" and "actual or imminent."[186] In recent years, courts have struggled to apply this standard to data breach

178. 18 U.S.C. § 2510(2) (defining an "oral communication").

179. Kee v. City of Rowlett, Texas, 247 F.3d 206, 216–17 (5th Cir. 2001).

180. *See* Huff v. Spaw, 794 F.3d 543, 545–46 (6th Cir. 2015).

181. *Id.* at 552. The Sixth Circuit determined that the Chairman's wife, Bertha Huff, may have had a viable ECPA claim. *See id.* at 554.

182. *Id.* at 552.

183. *See id.* (citing Will Verduzco, *Prevent Unwanted Butt Dialing with Smart Pocket Guard*, XDADEVELOPERS (Apr. 15, 2014), https://www.xdadevelopers.com/android/prevent-unwanted-butt-dialing-with-smart-pocket-guard).

184. *See id.*

185. *Id.*

186. *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548 (2016).

claims. During a breach, hackers gain access to consumer data but do not inevitably use that data in ways that harm consumers. Thus, whether a given data breach threatens "imminent" injury is not always apparent.[187]

Although not dispositive on its own, self-help assists courts in determining whether a data breach creates sufficient risk to satisfy Article III standing. In *Remijas v. Neiman Marcus*, for instance, the Seventh Circuit confronted a breach of a major retailer's customer records.[188] The retailer confirmed that a breach had occurred, acknowledged the risk, and even recommended that customers implement credit monitoring.[189] In those circumstances, the court reasoned that "[a]n affected customer, having been notified by Neiman Marcus that her card is at risk, might think it necessary to subscribe to a service that offers monthly credit monitoring."[190] Because many consumers did engage in self-help, and because those decisions were reasonable, the Seventh Circuit determined that the risk of harm was sufficient to support standing under Article III.[191]

As *Neiman Marcus* illustrates, consumers' self-help decisions provide a shortcut to gauge the threat posed by a given data breach. If few members of a putative class practice credit monitoring or other self-help strategies, it is unlikely that they see the breach as a substantial threat. But if many class members embrace those strategies, then the "risk of harm" may be "sufficiently substantial" to establish standing.[192] In this way, self-help enables courts to focus their resources on the data breaches that pose the greatest risk.[193]

D. PRIVACY TORTS

Thanks to Samuel Warren and Louis Brandeis's famous law review article, *The Right to Privacy*, most states recognize privacy-related torts.[194] To adjudicate

187. Beck v. McDonald, 848 F.3d 262, 274 (4th Cir. 2017).

188. *See* Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 694 (7th Cir. 2015).

189. *Id.* ("It is telling in this connection that Neiman Marcus offered one year of credit monitoring and identity-theft protection . . . .").

190. *Id.*

191. The Seventh Circuit is not alone in harnessing self-help to decide whether plaintiffs in data breach cases have demonstrated standing. *See, e.g.*, Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388 (6th Cir. 2016).

192. *Id.*

193. An analysis of the risk posed by a data breach remains relevant even after the Supreme Court's decision in *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021). *TransUnion* observes that a "mere risk of future harm" does not establish Article III standing when a plaintiff seeks damages. *Id.* at 2211. But the decision makes clear that "a person exposed to a risk of future harm may pursue forward-looking, injunctive relief." *Id.* at 2210.

194. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 219 (1890).

those claims, courts usually must decide whether a given piece of information is sufficiently "private" to merit protection.[195] Though courts examine many factors in this analysis, the outcome often turns on whether the plaintiff engaged in self-help to conceal, obscure, or monitor her data.

Take the public disclosure of private facts tort.[196] To prevail on such a claim, a plaintiff must show that the defendant gave "publicity to matters concerning the private, as distinguished from the public, life of the individual."[197] This element "seeks to differentiate between those facts whose disclosure promotes intimacy and those whose disclosure does not."[198] Generally, courts sort private facts from public ones by asking whether the plaintiff engaged in self-help. Consistent with that approach, courts recognize "no liability for giving further publicity to what the plaintiff himself leaves open to the public eye."[199]

For example, in *Gill v. Hearst Publishing Co.*, a couple objected to the dissemination of a photograph that showed them "seated in an affectionate pose" in a restaurant.[200] But the couple did nothing to block the camera's view or to discourage the photographer.[201] The court therefore rejected the couple's claim, emphasizing that the picture "was not surreptitiously snapped . . . but rather was taken of plaintiffs in a pose voluntarily assumed in a public market place."[202] By displaying their affection where other people could observe them, the plaintiffs signaled that their information was not sensitive enough to warrant judicial protection.

Just like the doctrines described above, privacy torts harness self-help. To distinguish private and public information, courts must make difficult decisions about what data deserves protection. Self-help offers a way out. By honoring consumers' self-help choices, courts allow individuals to decide which data to protect for themselves.

195. Restatement (Second) of Torts § 652D (1977).

196. The application of the intrusion upon seclusion tort also turns on whether the plaintiff practices self-help. *See id.* § 652B ("The defendant is subject to liability under the rule stated in this Section only when he has . . . invaded a private seclusion that the plaintiff *has thrown about* his person or affairs.") (emphasis added).

197. Restatement (Second) of Torts § 652D.

198. Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 930 (2005).

199. Restatement (Second) of Torts § 652D.

200. Gill v. Hearst Pub. Co., 40 Cal. 2d 224, 226 (1953).

201. *Id.* at 230–31.

202. *Id.*

E. DATA BREACH NOTIFICATION STATUTES

Today, a significant number of U.S. states have enacted legislation requiring firms to notify affected consumers about data breaches.[203] In general, these statutes specify which incidents require notification and prescribe the content of those communications. Such statutes serve many purposes, from "impos[ing] a reputational sanction on breached entities" to creating a private right of action for consumers.[204]

But the primary goal of notification laws is to encourage consumers to practice self-help. Consider California's statute, which has emerged as a model for other states.[205] As the state's Office of Privacy Protection explains, mandatory notifications are "intended to give individuals early warning when their personal information has fallen into the hands of an unauthorized person, so that they can take steps to protect themselves."[206] To that end, California requires that notification letters specifically tell consumers about "What [They] Can Do" to mitigate risks.[207] The premise is that, if notification letters prompt consumers to practice self-help, there will be less demand for the involvement of state or federal regulators. Like the doctrines introduced above, data breach notification statutes use self-help to preserve regulators' resources.

In sum, privacy law depends on self-help to solve two of its most pressing problems. First, self-help's preference signaling function helps adjudicators discern whether a given piece of data deserves protection. By honoring consumers' self-help choices, courts and regulators empower individuals to decide what data to protect for themselves.[208] Second, self-help's resource conserving function filters out the many low-value privacy disputes that might otherwise overwhelm the legal system. In doing so, self-help enables adjudicators to concentrate their limited resources on the most serious privacy threats.

In the future, self-help's preference signaling and resource conserving functions may grow even more essential. According to one estimate, modern

---

203. Taryn Elliott, *Standing a Chance: Does Spokeo Preclude Claims Alleging the Violation of Certain State Data Breach Laws?*, 49 SETON HALL L. REV. 233, 242 (2018) (observing that all fifty states have passed data breach notification statutes).

204. Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 917, 925 (2007).

205. *See* CAL. CIV. CODE § 1798.29 (West Supp. 2006).

206. CAL. DEP'T OF CONSUMER AFF., OFF. OF PRIV. PROT., RECOMMENDED PRACTICES ON NOTICE OF SECURITY BREACH INVOLVING PERSONAL INFORMATION 5 (2007).

207. CAL. CIV. CODE §§ 1798.29, 1798.80, 1798.82 (as amended, 2016).

208. *See* Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 929 n.25 (2005) (observing that individuals are generally "in a better position than government officials to make decisions about sharing personal information").

society "create[s] as much information in two days . . . as we did from the dawn of man through 2003."[209] The more data consumers create, the more often that adjudicators will need to decide what to protect. For that reason, reliance on self-help is likely to remain a common feature of privacy doctrines. Turning from the descriptive to the normative, the remainder of this Article asks how the law should respond to privacy self-help.

V. THE CASE FOR COMPLEMENTING SELF-HELP

Courts and regulators can respond to self-help in one of two ways. The first option is to develop legal remedies that substitute for self-help. The second option is to complement self-help by addressing the information asymmetries that undermine it.

The conventional wisdom endorses the first approach. In this view, privacy law and self-help are substitutes. As Douglas Lichtman maintains, "privacy law might be explained simply on th[e] notion that the law obviates the need for costly self-help measures."[210] Along the same lines, Woodrow Hartzog and Neil Richards posit that "first-best privacy [sh]ould be promoted through law rather than self-help."[211] Channeling Annie Oakley, the traditional view is that anything self-help can do, law can do better.

But the conventional wisdom misses the mark. As an initial matter, it is far from obvious that legislators could devise legal remedies that are sufficiently low-cost such that they present consumers with a meaningful alternative to self-help. For the most part, self-help and legal remedies specialize in different types of privacy risks: self-help enables consumers to vindicate their preferences quickly and cheaply, while litigation addresses persistent, systemic risks. Even in the best of circumstances, bringing a privacy-related lawsuit costs money, takes many months or even years, and yields uncertain results. By contrast, most of the self-help techniques surveyed in Part II promise instant results at almost no expense. Under those circumstances, it is difficult to see how even the most potent privacy legislation could convince consumers to abandon self-help.

And even if policymakers could achieve that improbable result, it would produce unexpected—and unwelcome—consequences. As Part IV explained, privacy law has come to rely on self-help's preference signaling and resource

209. MG Siegler, *Eric Schmidt: Every 2 Days We Create as Much Information as We Did up to 2003*, TECHCRUNCH (Aug. 4, 2010).

210. Lichtman, *supra* note 11, at 26.

211. RICHARDS & HARTZOG, *supra* note 11, at 1207.

conserving functions.[212] Displacing self-help would disable the many doctrines that depend on those functions.

Compared with the conventional wisdom, complementing self-help has many virtues.[213] By arming data subjects with intelligence about self-help, this approach empowers them to select successful strategies and sidestep self-defeating ones. By diminishing the asymmetries that distort consumers' self-help decisions, this approach supports the doctrines that rely on those decisions to discover data's value. And by repurposing familiar tools, this approach avoids the costs associated with formulating new legal rules.

Above all, complementing self-help makes the most of regulators' limited resources. Thanks to self-help's popularity, even small decreases in information asymmetries may translate into big improvements in consumers' ability to manage privacy risks. That means that complementing self-help is a promising tool to promote privacy that has been overlooked for too long.

A. HOW LAW CAN COMPLEMENT SELF-HELP

Just as law depends on self-help, self-help also depends on law. This Section identifies three ways that courts and regulators can reduce the information asymmetries that undermine self-help: (1) revisiting generally applicable laws, (2) extracting intelligence about self-help from data processing firms, and (3) disrupting invisible arms races that perpetuate asymmetries.

1. Revisiting Generally Applicable Laws That Exacerbate Asymmetries

On a regular basis, privacy and security researchers shed light on self-help.[214] For example, computer scientists have called attention to the security-privacy tradeoffs associated with VPNs.[215] In a similar vein, experts recently revealed that firms track users' devices in an attempt to circumvent concealment strategies.[216] By identifying the strategies and circumstances that

212. *See, e.g.*, Ellickson, *supra* note 13, at 686 (explaining that self-help avoids the "cost[s of] carry[ing] out legal research and . . . engag[ing] in legal proceedings").

213. Two decades ago, David Brin identified a "class of solutions to privacy issues, whose approach is not to close down information flows, but rather to compensate by opening them wider." BRIN, *supra* note 166, at 81. Complementing self-help falls into that class: by supplying consumers with intelligence about self-help, legal institutions help them protect their personal data.

214. *See, e.g.*, *The Computer Fraud and Abuse Act Hampers Security Research*, ELEC. FRONTIER FOUND. (Feb. 13, 2013), https://www.eff.org/document/cfaa-and-security-researchers ("Computer scientists are studying how advertisers and other companies track consumers' activities online . . . ."); Ikram et al., *supra* note 97, at 2 (finding that certain VPN apps amplify rather than resolve security vulnerabilities).

215. *See* Ikram et al., *supra* note 97, at 2.

216. *See, e.g.*, ELEC. FRONTIER FOUND., *supra* note 214.

produce unforeseen harms, this sort of research reduces the information asymmetries that plague self-help.

But many generally applicable laws discourage this vital research.[217] Commercial contracts prevent data brokers from sharing their clients' secrets, non-disclosure agreements stop employees at data processing firms from speaking with researchers, and trade secret law shields details about new surveillance technologies.[218] Though these generally applicable laws serve important functions, they have the unfortunate side effect of exacerbating the information asymmetries that plague self-help.

The Computer Fraud and Abuse Act (CFAA) may be the worst offender. That Act establishes criminal and civil penalties for individuals that access a computer "without authorization" or who "exceed[ ] authorized access."[219] In interpreting the CFAA, "most courts . . . have held that a conscious violation of a website's terms of service/use will render the access unauthorized and/or cause it to exceed authorization."[220] In practice, terms of service usually forbid activities—such as creating fake accounts or engaging in automated monitoring—that scientists use to gather intelligence about self-help.[221] So, by criminalizing terms of service violations, the CFAA inadvertently discourages research that sheds light on self-help's unintended consequences.

This is not a theoretical concern. Consider *Sandvig v. Sessions*, where scientists petitioned the court to issue a declaratory injunction shielding them from CFAA liability.[222] In *Sandvig*, the plaintiffs' proposed project would have studied employment discrimination, not privacy self-help. But the scientists planned to use the same methods as privacy and security researchers, such as

217. *See, e.g.*, A. Michael Froomkin, *"PETs Must Be on a Leash": How U.S. Law (and Industry Practice) Often Undermines and Even Forbids Valuable Privacy Enhancing Technology*, 74 OHIO ST. L.J. 1, 2 (2013) ("[L]egal rules and corporate policies . . . block . . . privacy self-help in the form of Privacy Enhancing Technologies . . . .").

218. *See* SCHNEIER, *supra* note 127, at 41 (2018) (noting that the Digital Millennium Copyright Act "includes a prohibition against security research").

219. 18 U.S.C. § 1030(a)(2).

220. United States v. Drew, 259 F.R.D. 449, 460 (C.D. Cal. 2009).

221. For example, Facebook demands that users "[p]rovide accurate information about yourself" and "[c]reate only one account." *See Terms of Service*, FACEBOOK, https://www.facebook.com/terms.php (last revised Oct. 22, 2020). Similar provisions are commonplace. *See, e.g.*, *Terms and Conditions*, THE ATLANTIC, https://www.theatlantic.com/terms-and-conditions (last updated Oct. 5, 2020) (warning users not to "[f]orge headers or otherwise intentionally disguis[e] the origin of any content or communication"); *Apple Website Terms of Use*, APPLE, https://www.apple.com/legal/internet-services/terms/site.html (last updated Nov. 20, 2009) (stating that users should not "manipulate identifiers in order to disguise the origin of any message or transmittal you send to Apple").

222. Sandvig v. Sessions, 315 F. Supp. 3d 1, 14 (D.D.C. 2018).

"misrepresenting their identities to target websites" and "[s]craping data."[223] In the end, the District Court concluded that "it would be credible [for researchers] to fear a future [CFAA] prosecution" for engaging in those activities.[224]

There is no doubt that the CFAA discourages research on privacy self-help. For example, take the "Persons You May Know (PYMK) Inspector," an app that helps users monitor how Facebook collects data and circumvents self-help.[225] As the app's developers explain, "Facebook won't discuss the input it uses, [so] the alternative is to study the output it produces: to track your friend suggestions and see how they change from day to day."[226]

Soon after the researchers released the app, "a Facebook spokesperson . . . told [them] that the tool violated Facebook's terms of service."[227] Threatened with liability under the CFAA, the researchers reluctantly agreed to modify the tool.[228] As this example illustrates, the Act chills research that could provide consumers with intelligence about self-help strategies and firms' responses to them.

But while the CFAA currently amplifies information asymmetries, it need not do so. Fortunately, legislative action is not necessary to fix the problem. Indeed, it would be easy for courts and regulators to ensure that the CFAA does not chill privacy and security research. First, courts should read the CFAA not to criminalize violations of a website's terms of service.[229] Rather, liability should only attach to defendants who undertake code-based hacking, a

223. *Id.* at 15–16.

224. *Id.* at 19.

225. Kashmir Hill & Surya Mattu, *Keep Track of Who Facebook Thinks You Know with This Nifty Tool*, GIZMODO (Jan. 10, 2018), https://gizmodo.com/keep-track-of-who-facebook-thinks-you-know-with-this-ni-1819422352.

226. *Id.*

227. Kashmir Hill & Surya Mattu, *Facebook Wanted Us to Kill This Investigative Tool*, GIZMODO (Aug. 7, 2018), https://gizmodo.com/facebook-wanted-us-to-kill-this-investigative-tool-1826620111.

228. *Id.* ("Facebook is happy to have users hand over lots of data about themselves, but doesn't like it when the data flows in the other direction.").

229. How far the Supreme Court's recent interpretation of the CFAA goes towards accomplishing this result remains unclear. *See generally Van Buren v. United States*, 141 S. Ct. 1648 (2021). Though the Court held that liability under the CFAA's "exceeds authorization" provision implicates "a gates-up-or-down inquiry," *id.* at 1658, it declined to decide whether that "inquiry turns only on technological . . . limitations on access, or instead also looks to limits contained in contracts or [website] policies," *id.* at 1659 n.8. So, whether a researcher's violation of a website's terms of service would trigger CFAA liability is a question the appellate courts must resolve. *See infra* note 230 (collecting cases).

conclusion that the Second and Fourth Circuits already embrace.[230] Second, prosecutors should promise not to bring charges against privacy and security researchers. The Department of Justice (DOJ) has already taken a step in this direction. In 2014, it released an "Intake and Charging Policy for Computer Crime Matters" that instructs prosecutors to consider "[t]he extent to which the activity was in furtherance of a larger criminal endeavor or posed a risk of bodily harm."[231]

Of course, creating a safe harbor in the CFAA is just one example of how revisiting generally applicable laws can complement self-help. Other doctrines, including the Digital Millennium Copyright Act, are also interpreted and enforced in ways that discourage privacy and security research.[232] By establishing safe harbors in such laws, policymakers can promote research that provides consumers with vital information about self-help.

2. Extracting Intelligence from Data Processing Firms

Another way for courts and regulators to reduce information asymmetries is by encouraging data processing firms—the institutions that know the most about self-help—to share that intelligence with consumers. This approach does not require policymakers to develop new statutes or promulgate new rules. Instead, regulators already have access to an array of familiar tools that are designed to encourage disclosure.

Most important, the FTC has statutory authority to monitor data processing firms.[233] In establishing the Commission, Congress gave it "[the] power . . . to gather and compile information concerning, and to investigate from time to time the organization, business, conduct, practices,

230. *See, e.g.*, United States v. Valle, 807 F.3d 508, 528 (2d Cir. 2015); WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 204, 206 (4th Cir. 2012). In these cases, the Second and Fourth Circuits held that the CFAA does not hinge on a website's terms of use but rather on whether an individual violates technical barriers—that is, whether the defendant engages in hacking. By contrast, the First, Fifth, Seventh, and Eleventh Circuits concluded that whether defendants act without authorization or exceed authorized access depends in part on the policies and terms of the computer owner. *See* EF Cultural Travel BV v. Explorica Inc., 274 F.3d 577, 583 (1st Cir. 2001); United States v. John, 597 F.3d 263, 272 (5th Cir. 2010); Int'l Airport Ctrs. LLC v. Citrin, 440 F.3d 418, 421 (7th Cir. 2006); United States v. Rodriguez, 628 F.3d 1258, 1263–64 (11th Cir. 2010).

231. OFF. OF THE ATT'Y GEN., MEMORANDUM TO THE UNITED STATES ATTORNEYS AND ASSISTANT ATTORNEY GENERALS FOR THE CRIMINAL AND NATIONAL SECURITY DIVISIONS 2 (2014), https://www.justice.gov/criminal-ccips/file/904941/download.

232. *See, e.g.*, SCHNEIER, *supra* note 127, at 41 (explaining how the Digital Millennium Copyright Act discourages security research and proposing improvements).

233. *See* Thomas Pahl, *Your Cop on the Privacy Beat*, FED. TRADE COMM'N. (Apr. 20, 2017), https://www.ftc.gov/news-events/blogs/business-blog/2017/04/your-cop-privacy-beat.

and management of any…corporation engaged in…commerce."[234] Also, Congress "empowered [the FTC] to make public the information obtained, except trade secrets and names of customers."[235] As scholars of consumer protection law observe, agency monitoring powers of this kind are ideally suited to address "information asymmetries."[236]

But the Commission rarely employs its monitoring authority to protect consumer privacy.[237] Instead, the FTC "decides whether to open an investigation by relying mostly on publicly available information and consumer complaints."[238] That information comes from "industry conferences, online consumer complaints, or litigators watching television in search of deceptive ads."[239] So, despite the agency's extensive monitoring powers, FTC investigators may suffer from the same information asymmetries as the consumers they protect.

By activating its dormant monitoring authority, the FTC could level the informational playing field. For example, the agency might decide to investigate the secretive data broker industry.[240] Through its monitoring authority, the Commission could identify "specific sources of [broker] data" and "the [firms] who purchase it."[241] At best, publishing that information would discourage firms from dealing with brokers in the first place. At a minimum, consumers would know not to rely on self-help when transacting with firms that buy data from brokers.

This is not to say that the FTC needs to limit its monitoring activities to data brokers. The Commission could also gather intelligence about firms' security measures, educating users about which self-help strategies disrupt those systems.[242] Or the FTC could study the circumstances in which missing data enables firms to draw negative inferences.[243] The bottom line is that by engaging its pre-existing monitoring powers, the FTC can equip data subjects with intelligence about which self-help strategies succeed and when.

---

234. 15 U.S.C. § 46(a) (West 2006); *see also* Kenneth Culp Davis, *The Administrative Power of Investigation*, 56 YALE L.J. 1111, 1118 (1947) (describing the history of this provision).

235. *Id.*; *see also* 15 U.S.C. § 46(f).

236. Rory Van Loo, *Regulatory Monitors: Policing Firms in the Compliance Era*, 119 COLUM. L. REV. 369, 404 (2019).

237. Rory Van Loo, *Helping Buyers Beware: The Need for Supervision of Big Retail*, 163 U. PA. L. REV. 1311, 1379 (2015) ("[U]nlike financial regulators, the FTC does not exercise these powers.").

238. *Id.* at 1380.

239. Van Loo, *supra* note 236, at 411.

240. *See supra* Part III.C.2.

241. *See* A REVIEW OF THE DATA BROKER INDUSTRY, *supra* note 161, at iii.

242. *See supra* Part III.B.2.

243. *See supra* Part III.A.2.

3. Disrupting Invisible Arms Races

When data subjects practice self-help, firms respond in kind, sparking arms races. Unsurprisingly, firms prefer to undermine self-help with strategies—such as data brokers and surveillance technologies—that consumers cannot detect.[244] Unaware of these hidden counterattacks, data subjects fail to adopt alternative strategies that could better protect their data.

Though regulators cannot prevent all arms races, they can ensure that when firms counterattack, they do so openly. To disrupt invisible arms races, the FTC has a powerful tool at its disposal: the authority to block unfair practices.[245] The agency's three-part unfairness test requires: (1) a "substantial injury to consumers," (2) "which is not reasonably avoidable by consumers themselves," and (3) is "not outweighed by countervailing benefits."[246] As it turns out, most invisible arms races satisfy all three of those elements.

First, counterattacks that undo self-help generally cause "substantial injury" to data subjects.[247] The reason is that consumers usually use self-help to safeguard data they consider sensitive.[248] Second, when consumers cannot detect firms' responses to self-help, the harm is—almost by definition—not "reasonably avoidable."[249] After all, the purpose of hidden surveillance technologies and undisclosed data broker agreements is to prevent consumers from avoiding them.[250] Finally, counterattacks typically lack countervailing consumer benefits. At a minimum, this element requires firms to explain why invisible arms races benefit consumers—and many practices will be difficult to justify.

To see how unfairness claims can complement self-help, consider the Commission's complaint against DesignerWare, "a company that licensed software to rent-to-own stores to help them track and recover rented computers."[251] Unbeknownst to users, DesignerWare's software, called PC

244. *See supra* Part III.C.

245. Because more than forty states have passed consumer protection laws modeled on the FTC Act, state regulators have the ability to bring unfairness claims as well. *See* John A. Rothchild, *Against Notice and Choice: The Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online (or Anywhere Else)*, 66 CLEV. ST. L. REV. 559, 638–39 (2018) ("Some but not all of these state laws are interpreted according to the FTC's unfairness standard.").

246. 15 U.S.C. § 45(n).

247. *Id.*

248. As noted above, some legal doctrines adopt that presumption explicitly. *See, e.g.*, *supra* Part IV.A–B.

249. *See* 15 U.S.C. § 45(n).

250. *See supra* Part III.C.

251. Press Release, Fed. Trade Comm'n., FTC Halts Computer Spying (Sept. 25, 2012), https://www.ftc.gov/news-events/press-releases/2012/09/ftc-halts-computer-spying.

Rental Agent, "log[ged] key strokes, capture[d] screen shots and t[ook] photographs using a computer's webcam."[252] By hiding these surveillance tools, DesignerWare ensured that consumers could not engage in self-help to defeat them. As the FTC cautioned, "[c]onsumers cannot reasonably avoid [the harms stemming from data collection] because PC Rental Agent is *invisible* to them."[253] Soon after the FTC filed suit, DesignerWare agreed to stop selling its tracking software.[254]

Despite the benefits of shutting down invisible arms races, however, the FTC rarely does so.[255] One explanation is that the agency's unfairness authority may rest on a shaky foundation. For years, critics have complained that unfairness authority is so broad that regulated entities lack notice about what conduct counts as unfair.[256] Validating those concerns, the Eleventh Circuit recently held that FTC remedial orders in unfairness cases must direct defendants "to stop committing a specific act or practice."[257]

But when unfairness claims target invisible arms races, concerns about specificity and notice lose much of their force. Regarding specificity, when a firm employs a surveillance technology to circumvent self-help, the natural response is for the FTC to forbid that "specific . . . practice."[258] As for notice, after DesignerWare, firms are on notice that invisible arms races may give rise to unfairness claims.[259] So, even if some unfairness claims raise concerns about notice and specificity, claims that target invisible arms races do not. By

252. *Id.*

253. Complaint at 19, *In re* DesignerWare, LLC, FTC File No. 123151, No. C-4390, 5 (Apr. 15, 2013), https://www.ftc.gov/enforcement/cases-proceedings/112-3151/designerware-llc-matter (emphasis added).

254. *See FTC Halts Computer Spying*, *supra* note 251 (outlining the terms of the proposed settlement orders).

255. Apart from *DesignerWare*, my research only uncovered two cases that targeted invisible arms races. *See* Complaint, *In re* Lenovo (USA) Inc., FTC File No. 1523134, No. C-4636, 6 (Dec. 20, 2017), https://www.ftc.gov/system/files/documents/cases/1523134_c4636_lenovo_united_states_complaint.pdf (explaining that pre-installed software blocked access to VPNs); Complaint for Permanent Injunction and Other Equitable and Monetary Relief, Fed. Trade. Comm'n. v. Vizio, Inc., No. 2:17-cv-00758, 2017 WL 7000553, (D.N.J. Feb. 6, 2017), https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf.

256. Most criticism of the FTC's unfairness authority has arisen in data security cases. *See, e.g.*, Fed. Trade. Comm'n. v. Wyndham Worldwide Corp., 799 F.3d 236, 255 (3d Cir. 2016) (rejecting the defendant's claim that they lacked fair notice that their conduct violated 18 U.S.C. § 45).

257. LabMD, Inc. v. Fed. Trade Comm'n., 894 F.3d 1221, 1236 (11th Cir. 2018).

258. *Id.* at 1233.

259. *See* Complaint, *supra* note 253, at 5 (emphasis added).

stepping up unfairness enforcement, regulators can help data subjects figure out which strategies fall victim to arms races and which do not.

This Article began by asking how the law should respond to self-help. The conventional wisdom, which favors displacing self-help, fails to recognize that many privacy doctrines depend on it. Complementing self-help holds more promise. By disseminating intelligence about self-help, courts and regulators increase the odds that consumers will embrace proven practices while avoiding unreliable ones.

B. COMPLICATIONS

This Section acknowledges three objections that complicate the case for complementing self-help. The first objection contends that facilitating self-help is not feasible, while the second and third posit that it is not desirable. Though none of these objections are fatal, they underscore that self-help is an imperfect tool for advancing consumer privacy. Even if courts and regulators eliminate information asymmetries, they cannot transform self-help into a cure for every privacy problem. So, while policymakers should devote more resources to supporting self-help than they do today, legal remedies and market activity will remain essential tools for protecting personal data.

1. The Gap Between Information and Action

The interventions introduced above assume that consumers will act on the intelligence that regulators and researchers disseminate. But disclosures do not always influence consumer behavior. As quantitative research attests, data subjects rarely review or understand privacy policies.[260] Should consumers ignore intelligence about self-help, they may continue to practice strategies that backfire.[261]

260. *See, e.g.*, Lior Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?*, 45 J. LEGAL STUD. S69, S92 (2016) ("[D]ifferences in [privacy] policy language that are quite salient to lawyers are essentially irrelevant to consumers."); Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 543, 565 (2009) ("We estimate that reading privacy policies carries costs in time of approximately 201 hours a year, worth about $ 3,534 annually per American Internet user.").

261. A related problem is that educated, wealthy consumers may be better equipped to implement effective self-help strategies. *See generally* Mary Madden, *Privacy, Security, and Digital Inequality: How Technology Experiences and Resources Vary by Socioeconomic Status, Race, and Ethnicity*, DATA & SOC'Y. (Sept. 27, 2017), https://datasociety.net/pubs/prv/DataAndSociety_PrivacySecurityandDigitalInequality.pdf. That raises a real concern that the availability of self-help may exacerbate distributional differences in access to privacy. At the same, other privacy protection mechanisms—such as class-action lawsuits—may well suffer from similar problems, so the broader distributional effects of complementing self-help remain far from clear.

Of course, empirical evidence is the only way to conclusively determine the extent to which data subjects act on intelligence about self-help.[262] That said, consumers are far more likely to read and apply intelligence about self-help than other privacy information. Privacy policies, after all, supply information that is unimportant to most readers. By contrast, data subjects only practice self-help when they believe that a given piece of data is worth protecting. For this reason, consumers may be particularly likely to pay attention to—and act on—intelligence about which self-help strategies succeed and which fail.

2. The Social Costs of Self-Help

It is no secret that some self-help strategies inflict social costs.[263] To take one example, Facebook users who create "many false and implausible life events on their profiles . . . might confuse networked connections."[264] In turn, that may lead to lost friendships, or, at a minimum, wasted time. Worse still, self-help may deprive firms of data that ultimately benefits consumers.

And, while complementing self-help does not raise social costs itself, it does not reduce them either. That is because individuals generally overlook social costs when making decisions.[265] So, even if consumers enjoy perfect information about such costs, they may still decide to pursue strategies that inflict them. Thus, if the magnitude of social costs is large, self-help may cause serious problems that the interventions introduced above do nothing to solve.

Two considerations mitigate this concern. First, many popular self-help strategies do not impose social costs. For instance, while taping over laptop cameras creates some private costs—no one wants sticky camera lenses—it has no obvious social costs. To the contrary, if installing camera covers inspires other consumers to do the same, it may generate social benefits. Second, while some unusual techniques inflict substantial social costs, existing legal doctrines generally deter those techniques. If, for example, an individual hacks into a

262. One possibility is that behavioral biases will prevent consumers from acting. *See, e.g.*, Solove, *supra* note 27, at 1883–88 (examining how cognitive biases interfere with individuals' privacy decision-making); Sasha Romanosky & Alessandro Acquisti, *Privacy Costs and Personal Data Protection: Economic and Legal Perspectives*, 24 BERKELEY TECH. L.J. 1061, 1096 (2009) ("[R]esearch in behavioral economics and behavioral decision making [sic] provides ample evidence that consumers are unable to conceive of all possible outcomes and risks of data disclosures.").

263. *See* RICHARDS & HARTZOG, *supra* note 11, at 1207–08 (raising the issue of social costs in the context of obfuscation strategies.).

264. *Id.*

265. *See, e.g.*, Carl J. Dahlman, *The Problem of Externality*, 22 J.L. & ECON. 141, 141 (1979) ("[W]e say that when an externality is present there is a divergence between private and social cost.").

firm's network as a form of self-help, that firm can bring a civil claim or even press criminal charges.[266]

So, for the most part, self-help strategies either do not impose substantial social costs or are adequately deterred by existing criminal and civil penalties. To the extent that some strategies inflict social costs without triggering liability, new legal remedies may be necessary to discourage those strategies or mitigate their effects. Thus, while courts and regulators generally should facilitate self-help, it may sometimes be necessary to displace particularly wasteful strategies.

3. The Market Alternative to Self-Help

In a competitive market, consumers need not resort to self-help to protect their interests. Instead, they can exit, taking their business—and their data—to another firm. In this way, market activity replicates self-help's ability to express individual preferences and to do so cheaply. At the same time, market activity encourages firms to compete by enhancing privacy features.[267] So, when exit is an option, self-help may be a second-best solution.

As a result, it is tempting to conclude that the law should ignore self-help and instead encourage consumers to manage privacy risks through market activity. But data subjects routinely encounter problems that exit cannot solve. For one thing, some platforms may be so ubiquitous that consumers cannot disentangle themselves without incurring substantial costs.[268] For another thing, markets do not always permit consumers to address granular privacy risks. Recall, for instance, the Pew interviewee who revealed most personal data but concealed her birthday.[269] Even firms that tout dashboards that

266. For example, in one case, a group of individuals allegedly created thousands of fake accounts on LinkedIn, degrading the value of that social network. In response, LinkedIn brought a variety of federal and state law claims, including some under the CFAA. *See* Complaint, LinkedIn Corp. v Does, No. 5:15-cv-04463, (N.D. Cal. Aug. 8, 2016), https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2261&context=historical.

267. *See* Frank Pasquale, *Privacy, Antitrust, and Power*, 20 GEO. MASON L. REV. 1009, 1009 (2013) ("Within a neoclassical economic framework, the relationship between Internet privacy and competition is direct and positive.").

268. *See, e.g.*, Dina Srinivasan, *The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy*, 16 BERKELEY BUS. L.J. 39, 81 (2019).

269. *See Americans Conflicted About Sharing Personal Information with Companies*, PEW RSCH. CTR (Dec. 30, 2015), https://www.pewresearch.org/fact-tank/2015/12/30/americans-conflicted-about-sharing-personal-information-with-companies.

purportedly give users control over their data[270] rarely permit such granular choices.[271]

Because markets cannot solve every problem that consumers encounter, self-help is likely to remain a popular tool to protect privacy. So, while courts and regulators should facilitate competitive markets, they must also complement self-help.

VI. CONCLUSION

Today, privacy self-help is endorsed by journalists, championed by advocates, and embraced by consumers. Too often, however, self-help exposes the data that it promises to protect. In an ideal world, consumers would avoid strategies that backfire and adopt ones that succeed. But information asymmetries prevent data subjects from discovering which strategies and circumstances produce unforeseen harms.

While displacing self-help falls short because it disrupts existing doctrines, complementing self-help succeeds because it works with them. This approach preserves individuals' ability to decide what data deserves protection, strengthens the many doctrines that depend on self-help, and harnesses familiar regulatory tools. Ultimately, complementing self-help promises to transform a popular but unreliable practice into a potent weapon in the hands of millions of consumers.

270. For example, Google states that its privacy settings permit users to control how data is used across Google. *Privacy Controls*, GOOGLE, https://safety.google/privacy/privacy-controls (last visited Nov. 25, 2020); *see also* Paddy Underwood, *Privacy Checkup Is Now Rolling Out*, FACEBOOK (Sept. 4, 2014), https://newsroom.fb.com/news/2014/09/privacy-checkup-is-now-rolling-out.

271. *See* Fred Stutzman, Ralph Gross & Alessandro Acquisti, *The Silent Listeners: The Evolution of Privacy and Disclosure on Facebook*, 4 J. PRIV. & CONFIDENTIALITY 7, 23 (2012) ("Choosing Facebook privacy settings to correctly match one's preferences can be difficult.").