Michigan Technology Law Review

Article 4

2021

Individuals as Gatekeepers Against Data Misuse

Ying Hu
National University of Singapore

INDIVIDUALS AS GATEKEEPERS AGAINST DATA MISUSE

*Ying Hu**

ABSTRACT

This article makes a case for treating individual data subjects as gatekeepers against misuse of personal data. Imposing gatekeeper responsibility on individuals is most useful where (a) the primary wrongdoers engage in data misuse intentionally or recklessly; (b) misuse of personal data is likely to lead to serious harm; and (c) one or more individuals are able to detect and prevent data misuse at a reasonable cost.

As gatekeepers, individuals should have a legal duty to take reasonable measures to prevent data misuse where they are aware of facts indicating that the person seeking personal data from them is highly likely to misuse it or to facilitate its misuse. Recognizing a legal duty to prevent data misuse provides a framework for determining the boundaries of appropriate behavior when dealing with personal data that people have legally acquired. It does not, however, abrogate the need to impose gatekeeping obligations on big technology companies.

In addition, individuals should also owe a social duty to protect the personal data in their possession. Whether individuals have sufficient incentive to protect their personal data in a particular situation depends not only on the cost of the relevant security measures, but also on their expectation of the security decisions made by others who also possess that data. Even a privacy conscious individual would have little incentive to invest in privacy protective measures if he believes that his personal data is possessed by a sufficiently large number of persons who do not invest in such measures. On the flip side, an individual's decision to protect his personal data generates positive externalities—it incentivizes others to invest in security measures. As such, promoting the norm of data security is likely to lead to a self-reinforcing virtuous cycle which helps

* Lecturer, National University of Singapore. This article is part of my JSD thesis, written under the supervision of Professor Christine Jolls. I am tremendously grateful for her guidance and support. I am also indebted to Professors Jack Balkin, Simon Chesterman, Tom Tyler, Sandra Booysen, Damian Chalmers, Helena Whalen-Bridge, Dian Shah, Ernest Lim, and Mr. Brian Chang for their thoughtful comments and conversation. I would like to thank editors and staff of the *Michigan Technology Law Review*, especially Kimberly Parry, James Wang, Elizabeth McElvein, Marvin Shih, and Josh Zhao for their helpful suggestions and hard work editing this article. All mistakes are mine.

improve the level of data security in a given community.

Table of Contents

INTRODUCTION 116
I. INDIVIDUALS CAUSE DATA HARM TO OTHER INDIVIDUALS AND SOCIETY 120
A. *Revelation of Data Relating to Other Individuals* 120
B. *How Revelation of Data Leads to Harm* 121
II. INDIVIDUALS AS GATEKEEPERS OF DATA MISUSE 123
A. *Rationale for Imposing Gatekeeper Liability* 124
1. Direct Deterrence is Ineffective 124
2. Gatekeeper's Ability to Detect Misconduct 126
3. Gatekeeper's Ability to Prevent Misconduct 128
4. Gatekeeper's Ability to Provide Compensation to Victims 129
B. *Costs of Individual Gatekeeper Liability* 130
1. Costs of Gatekeeping 131
2. Is the Cost of Gatekeeping Lower Than Direct Enforcement? 135
C. *Alternatives to Imposing Gatekeeper Liability on Individuals* 135
1. Inadequate Private Gatekeeping Incentives 135
2. Ineffective Private Contracting for Gatekeeping Activities 137
3. Interaction with Other Gatekeepers 138
D. *A New Legal Duty to Prevent Data Misuse* 140
III. A SOCIAL DUTY TO SECURE PERSONAL DATA 142
A. *Interdependent Security* 144
B. *Explaining the Privacy Paradox* 146
C. *Policy Implications* 149
CONCLUSION 151

INTRODUCTION

Personal data is the fuel of the digital economy. In the wrong hands, however, it can cause significant harm to both individual data subjects and society at large.[1] Popular solutions to minimize data misuse generally fall

1. *See, e.g.*, Omri Ben-Shahar, *Data Pollution*, 11 J. LEGAL ANALYSIS 104 (2019); FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015); Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 737 (2018).

within two categories: (1) empowering data subjects by conferring them with more types of rights;[2] and (2) imposing new duties on persons that are better positioned to prevent data misuse.

This article focuses on the latter approach to preventing data misuse. A number of scholars have argued in favor of imposing additional duties on commercial data holders. According to Jack Balkin, digital media companies that collect and use our personal data should be classified as "information fiduciaries" and in turn, owe three basic duties towards their users: a duty of care, a duty of confidentiality, and a duty of loyalty.[3] Neil Richards and Woodrow Hartzog also draw on fiduciary law to impose similar duties on tech companies to curb harmful data processing.[4] Sarah Ludington advocates for a new tort of information misuse based on the Fair Information Practice Principles to hold data traders accountable for insecure data practices.[5]

However, few academic commentators have looked into what additional duties, if any, should be borne by the individual data subjects, who are often perceived as mere victims having little at their disposal to protect their own privacy.[6] This perception, while correct in many instances, is incomplete. When individuals disclose personal data to unscrupulous data collectors, they increase the risk of data harm to other people. Under existing law, each individual owes some duty with respect to personal data relating to others. For example, an individual owes a duty not to publicly disclose private facts about another and a duty not to disclose confidential information.[7] But should individuals owe additional duties, such as a more

---

2. *See, e.g.*, the new rights, such as the right to data portability, provided for under the European General Data Protection Regulation (GDPR). Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1. The GDPR also embraces the second approach by imposing additional duties on data controllers. *See*, *id.*

3. Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016) [hereinafter *Information Fiduciaries*]; Jack Balkin, *The First Amendment in the Second Gilded Age*, 66 BUFF. L. REV. 979, 1007–09 (2018) [hereinafter *Second Gilded Age*].

4. Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 457–71 (2016); Neil Richards & Woodrow Hartzog, *A Relational Turn for Data Protection?* 4 EUR. DATA PROT. L. REV. 492 (2020).

5. Sarah Ludington, *Reining in the Data Traders: A Tort for the Misuse of Personal Information*, 66 MD. L. REV. 140 (2006). This tort also targets "the use of personal data for purposes extraneous to the original transaction." *Id.* at 146.

6. *See, e.g.*, Cameron F. Kerry, *Why Protecting Privacy Is a Losing Game Today—and How to Change the Game*, BROOKINGS INST. (July 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game.

7. *See, e.g.*, RESTATEMENT (SECOND) OF TORTS § 652D (AM. L. INST. 1977); DANIEL J. SOLOVE & PAUL SCHWARTZ, INFORMATION PRIVACY LAW 108–42 (5th ed. 2015) (discussing public disclosure of private facts); Brian C. Murchison, *Reflections on Breach of Confidence from the U.S. Experience*, 15 MEDIA & ARTS L. REV. 295 (2010).

general duty to refrain from disclosing personal data to certain third parties, or a duty to secure the data in their possession?

This article builds upon the work of academic commentators who argue in favor of placing additional limits on individuals' power to disclose the personal data in their possession. For example, Mark MacCarthy points out that an individual's decision to share personal data can impose negative externalities on other people.[8] Where the use of data leads to substantial harm, he argues, there might be a case for disallowing individuals from disclosing that data in the first place.[9] Following MacCarthy, Joshua Fairfield and Christoph Engel also focus on the negative externalities caused by individual decisions to disclose personal data.[10] Their solution, however, lies in nudging individuals to make more privacy-seeking decisions. Drawing from insights from classical and behavioral economics, they recommend various coordination strategies based on individual payoffs, repeat play, reciprocity, and inequity aversion.[11] Implicit in Fairfield and Engel's recommendation is that individuals bear some social (as opposed to legal) duty to engage in privacy-seeking behavior, which can be enforced by social sanctions. More recently, Ben-Shahar has recommended imposing a data tax on individual data subjects to counteract the negative externalities that they impose on others.[12]

One of the few scholars arguing in favor of a duty not to disclose sensitive data about oneself is Anita Allen. She claims that such a duty is grounded in either self-respect or autonomy.[13] Similar to MacCarthy, Fairfield, and Engel, Allen points to negative externalities that an individual's decision to disregard his privacy can impose on other people.[14] The individual's duty not to harm others therefore entails a derivative duty to protect his own privacy.[15] Allen has not elaborated on what a duty to protect one's privacy requires. Indeed, she appears to suggest that there is

8. Mark MacCarthy, *New Directions in Privacy: Disclosure, Unfairness and Externalities*, 6 I/S: J.L. & POL'Y FOR INFO. SOC'Y. 425, 445–68 (2011). Information disclosed by that individual may, directly or through data analysis, enable inferences to be made about other individuals sharing certain characteristics with him. Such inferences might in turn be used to perpetuate various forms of discrimination (e.g., denial of access to employment) or to cause possible market dysfunctions. *Id*. at 456–68.

9. *Id.* at 430 ("If the harm done by negative privacy externalities is substantial, then individual choice might have to be restricted.").

10. Joshua A.T. Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 DUKE L.J. 385 (2016).

11. *Id*. at 433–48. Examples of such strategies include letting individuals control access to their data, enabling them to communicate and enforce their privacy expectations, social sanctions against privacy-reducing behavior. *Id.* at 448–56.

12. Ben-Shahar, *supra* note 1, at 138–43.

13. Anita L. Allen, *An Ethical Duty to Protect One's Own Information Privacy?*, 64 ALA. L. REV. 845, 853–54, 855–57 (2013).

14. *Id.* at 862.

15. *Id.*

very little that an individual can do to fulfill that duty in the big data era.[16] By contrast, this article argues that individuals should owe both legal and social duties to protect the personal data in their possession.

This article makes two main contributions. Firstly, drawing from the literature on gatekeeper liability, this article makes a new case for treating individual data subjects as gatekeepers against misuse of personal data. In particular, imposing gatekeeper responsibility on individuals is most useful where (a) the primary wrongdoers engage in data misuse intentionally or recklessly; (b) misuse of personal data is likely to lead to serious harm; and (c) one or more individual data subjects are able to detect and prevent that misuse at a reasonable cost. This article proposes that individuals should have a legal duty to take reasonable measures to prevent data misuse where they are aware of facts indicating that the person seeking personal data from them is highly likely to misuse it or to facilitate its misuse. Recognizing a legal duty to prevent data misuse provides a framework for determining the boundaries of appropriate behavior when dealing with personal data that people have legally acquired.

Secondly, this article argues that individuals should also owe a social duty to protect the personal data in their possession. Whether individuals have sufficient incentive to protect their personal data in a particular situation depends not only on the cost of the relevant security measures, but also on their expectation of the security decisions made by others who also possess that data. Even a privacy conscious individual would have little incentive to invest in privacy protective measures if he believes that his personal data is possessed by a sufficiently large number of persons that do not invest in such measures. On the flip side, an individual's decision to protect his personal data generates positive externalities: it incentivizes others to invest in security measures. As such, promoting the norm of data security is likely to lead to a self-reinforcing virtuous cycle which helps improve the level of data security in a given community.

This article proceeds as follows. Part I identifies various types of negative externalities flowing from disclosure of personal data. Part II argues in favor of treating individual data subjects as gatekeepers in appropriate circumstances to prevent data misuse and proposes a new legal duty on individuals to prevent data misuse. Part III makes an argument for promoting a social duty to protect the personal data in our possession.

16. Anita L. Allen, *Protecting One's Own Privacy in a Big Data Economy*, 130 HARV. L. REV. F. 71 (2016).

I. INDIVIDUALS CAUSE DATA HARM TO OTHER INDIVIDUALS AND SOCIETY

A. *Revelation of Data Relating to Other Individuals*

The phenomenon of "interdependent privacy," that is, situations in which personal data shared by one individual affects other people's privacy, has gained growing attention in recent years.[17] Let us consider a hypothetical example: an individual, let us call him Allen, can obtain control over data relating to another individual, let us call him Ben, in a myriad of ways. Allen might receive the information directly from Ben on a social occasion, or he might gain access to it in the course of his work. The relevant data might appear to relate only to Ben (as in the case of Ben's phone number) or relate to multiple parties, including Allen himself (as in the case of a group photo). If Allen retains a copy of Ben's data, either by memory or through other means, he might subsequently disclose that data, intentionally, recklessly, or negligently, to third parties. He might, for instance, upload an embarrassing photo of Ben on Facebook or tweet about Ben's chemotherapy even though Ben prefers to keep his medical condition private.

Even where Allen discloses data that seems to relate only to himself, he may nevertheless reveal information about Ben.[18] Such revelation can happen in at least three ways. First, if a third party knows that either Allen or Ben displays certain characteristics or has done something (e.g., being recently divorced), once the data disclosed by Allen suggests that he does not or has not done so, then an inference can be made about Ben. In a similar vein, if Allen and Ben are known to share a certain characteristic, then Allen's disclosure could enable others to infer whether Ben possesses that characteristic. Second, if it is generally assumed that people who possess a certain trait (e.g., being heterosexual) would disclose that trait, and Allen's decision to disclose that trait reinforces this assumption, then one may infer from Ben's failure to disclose that he lacks this trait. Third, the data disclosed by Allen, when aggregated and analyzed with data about other individuals, may reveal previously unknown and non-obvious relationships between certain pieces of data (e.g., people who use non-

17. *See, e.g.*, Bernadette Kamleitner & Vince Mitchell, *Your Data Is My Data: A Framework for Addressing Interdependent Privacy Infringements*, 38 J. PUB. POL'Y & MKTG. 433 (2019); Gergely Biczók & Pern Hui Chia, *Interdependent Privacy: Let Me Share Your Data*, *in* FINANCIAL CRYPTOGRAPHY AND DATA SECURITY 338 (Ahmad-Reza Sadeghi ed., 2013); Solon Barocas & Karen Levy, *Privacy Dependencies*, 95 WASH. L. REV. 555 (2020); MacCarthy, *supra* note 8; Fairfield & Engel, *supra* note 10; Allen, *supra* note 13; Allen, *supra* note 16; Ben-Shahar, *supra* note 1.

18. For a more detailed discussion on how one can reveal information about others when disclosing his own information, see Barocas & Levy, *supra* note 17, at 562–605; MacCarthy, *supra* note 8, at 450–55; Fairfield & Engel, *supra* note 10, at 399–406.

standard browsers such as Firefox or Chrome are likely to perform better at work[19]). This new insight may then enable a third party who possesses certain information about Ben (e.g., that he uses Internet Explorer) to make predictions about him (e.g., that he is less likely to perform well).

B. *How Revelation of Data Leads to Harm*

The mere fact that Ben's data has been revealed does not mean that Ben has been or will be harmed. Somebody must use that data against Ben's interest or at least acquire the ability to do so (which may, in turn, provoke Ben's anxiety).

There are a number of ways that a third party can use data or inferences about Ben to his disadvantage. Certain uses warrant legal intervention. For example, criminals might use Ben's location data to stalk him, rob him, or injure him. Public disclosure of certain data (e.g., Ben's naked photo) might cause him to suffer embarrassment, humiliation, or even harassment.[20] Some information/inferences might be inaccurate or outright false, which could in turn cause Ben to suffer financial loss. For example, in *Robins v. Spokeo, Inc.*, the Ninth Circuit (on remand from the Supreme Court) concluded that the dissemination of inaccurate, and seemingly favorable, facts about an individual could cause him real harm.[21] Even where the relevant information /inference is accurate, it may be used to discriminate against Ben,[22] to exploit his vulnerabilities,[23] or to unjustifiably influence his behavior. For example, an employer might refuse to interview a prospective job candidate because that person has diabetes. A politician might send personalized

19. Eamon Javers, *Inside the Wacky World of Weird Data: What's Getting Crunched*, CNBC (Feb. 12, 2014, 2:06 PM), https://www.cnbc.com/2014/02/12/inside-the-wacky-world-of-weird-data-whats-getting-crunched.html.

20. Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 364–65 (2014).

21. Robins v. Spokeo, Inc., 867 F.3d 1108, 1117 (9th Cir. 2017). Spokeo, a website that compiles consumer information, falsely reported that "[Robins] is married with children, that he is in his 50s, that he is employed in a professional or technical field, that he has a graduate degree, and that his wealth level is higher than it is." Robins alleged that Spokeo's false report "caused actual harm to [his] employment prospects." *Id.*

22. Various legislation prohibits discrimination on the basis of race, color, religion, sex, national origin, age, disability, marital status, or genetic information. *See, e.g.*, Fair Housing Act, 42 U.S.C. §§ 3601–3619; Equal Credit Opportunity Act (ECOA), 15 U.S.C. §§ 1691–1691f; Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 881 (codified as amended in scattered sections of 26, 29, and 42 U.S.C.).

23. Scammers are known to rely on "sucker's list" to target individuals who have previously fallen victim to a scam. Caroline Mayer, *The Scam of All Scams: Sucker Lists*, FORBES (Feb. 18, 2014, 5:26 PM), https://www.forbes.com/sites/nextavenue/2014/02/18/the-scam-of-all-scams-sucker-lists/?sh=7bb043654393.

messages to prospective voters for the purpose of activating their "implicit attitudes and biases" and swaying their votes in an upcoming election.[24]

Whether legal intervention is justified in other situations is less obvious. For example, there are fears that information or inferences about Ben's preferences might result in him receiving more content that conforms to his existing views, causing him to live in a "filter bubble."[25] However, a number of recent studies suggest that fears over algorithmic filter bubbles might be exaggerated.[26] Another example concerns Ben's location data, which might enable retailers to charge him a higher price than they otherwise would. For instance, the Staples website allegedly displayed different prices to different online shoppers based on their locations and, in particular, their distance from a rival store, such as Office Depot.[27] But a company might have legitimate reasons for charging customers different prices based on their location: the cost of shipping might vary, or the company might face difficulty satisfying demand for its products in certain places. In any event, one might argue that displaying different prices in a website to customers based on their location does not cause any real harm, since if potential customers are unhappy with the price, they can simply search for cheaper alternatives elsewhere, a few clicks away.

Moreover, preventing Allen from disclosing the personal data in his possession on the basis that doing so might harm Ben can be objectionable on several grounds. First, one may argue that, even if Ben suffers harm as a result of an actual or expected misuse of personal data disclosed by Allen, Allen has not caused that harm in a legally significant way; rather, the harm is caused by the persons who have misused or may reasonably be expected to misuse Ben's data. Second, sometimes the data disclosed by Allen is aggregated with large amounts of data provided by other people; the dataset

---

24. Jacquelyn Burkell & Priscilla M. Regan, *Voter Preferences, Voter Manipulation, Voter Analytics: Policy Options for Less Surveillance and More Autonomy*, INTERNET POL'Y REV., Dec. 2019, at 1, 2. The most well-known example is Cambridge Analytica, a consulting firm that allegedly used Facebook data to manipulate voters on "an industrial scale". Carole Cadwalladr, *Fresh Cambridge Analytica Leak 'Shows Global Manipulation Is Out of Control'*, GUARDIAN (Jan. 4, 2020, 11:55 AM), http://www.theguardian.com/uk-news/2020/jan/04/cambridge-analytica-data-leak-global-election-manipulation.

25. ELI PARISER, THE FILTER BUBBLE: HOW THE NEW PERSONALIZED WEB IS CHANGING WHAT WE READ AND HOW WE THINK (2011).

26. *See, e.g.*, Mario Haim, Andreas Graefe & Hans-Bernd Brosius, *Burst of the Filter Bubble?*, 6 DIGIT. JOURNALISM 330 (2018); Richard Fletcher & Rasmus Kleis Nielsen, *Are News Audiences Increasingly Fragmented? A Cross-National Comparative Analysis of Cross-Platform News Audience Fragmentation and Duplication*, 67 J. COMMC'N 476, 485–93 (2017); Richard Fletcher, *The Truth Behind Filter Bubbles: Bursting Some Myths*, REUTERS INST. (Jan. 24, 2020), https://reutersinstitute.politics.ox.ac.uk/risj-review/truth-behind-filter-bubbles-bursting-some-myths.

27. Jennifer Valentino-DeVries, Jeremy Singer-Vine & Ashkan Soltani, *Websites Vary Prices, Deals Based on Users' Information*, WALL ST. J. (Dec. 24, 2012), http://www.wsj.com/articles/SB10001424127887323777204578189391813881534.

is then analyzed to generate insights which are subsequently used to harm Ben. In such cases, Allen's contribution to Ben's harm is arguably negligible. In fact, as long as a significant number of people disclose similar types of data, Ben may suffer harm irrespective of whether Allen discloses his data. Third, even if Allen's disclosure results in harm to Ben, the disclosure may also generate significant benefits to Ben or other people, producing an overall net gain to society. For example, granting various entities and the government access to Ben's location data to facilitate contact tracing during the Covid-19 outbreak is arguably justified by the public interest in alleviating the public health crisis. Similarly, it may be easier to assess whether a particular use (e.g., the government using Ben's health data for Covid-19 research), as opposed to a particular disclosure (e.g., disclosing Ben's health data to the government, who may use that data for a myriad of purposes), of personal data produces a net gain to the society. Therefore, it may be more appropriate to regulate the use, as opposed to the distribution, of personal data. Finally, restricting Allen's right to disclose the personal data in his possession could, under certain circumstances, unduly interfere with his right to free speech.[28] Some of these objections will be considered in greater detail in Parts II and III when we consider the extent of an individual's duty, if any, with respect to the personal data in his possession.

II. INDIVIDUALS AS GATEKEEPERS OF DATA MISUSE

In this article, gatekeepers are defined broadly as persons "who are able to disrupt misconduct by withholding their cooperation from wrongdoers."[29] Traditional analysis of gatekeeper liability generally focuses on a limited group of persons that provide special goods or services, such as lawyers and accountants.[30] In comparison, individual data subjects seem to be far too broad of a group to be considered gatekeepers. Nevertheless, Reinier H. Kraakman's gatekeeper analysis framework provides a useful tool to determine whether, and to what extent, any duty should be imposed on

28. For a summary and a critique of the argument that attempts to regulate the flow of personal data would conflict with the First Amendment, see Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149 (2004).

29. Reinier H. Kraakman, *Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy*, 2 J.L. ECON. & ORG. 53, 53 (1986).

30. *See, e.g.*, *id.* at 54 (noting that the support provided by gatekeepers are usually in the form of "a specialized good, service, or form of certification that is essential for the wrongdoing to succeed"); John C. Coffee, Jr., *Gatekeeper Failure and Reform: The Challenge of Fashioning Relevant Reforms*, 84 B.U. L. REV. 301, 308–09 (2004); Andrew F. Tuch, *The Limits of Gatekeeper Liability*, 73 WASH. & LEE L. REV. ONLINE 619, 619 (2017) ("As conventionally understood, [gatekeeper] strategy involves imposing liability on 'gatekeepers'—actors such as lawyers, investment bankers, and accountants—for the wrongs of their corporate clients . . . .").

individual data subjects.[31] Moreover, individual data subjects are sometimes able to prevent data misuse by withholding personal data in their possession from wrongdoers and as such may be viewed as gatekeepers.

A. *Rationale for Imposing Gatekeeper Liability*

An oft-cited rationale for imposing gatekeeper liability is that direct deterrence is impractical or ineffective.[32] This may be so, for example, where the wrongdoer cannot be easily identified or located, lacks the capacity to make self-interested decisions (e.g., they are intoxicated), or is otherwise unresponsive to punishment (e.g., they have limited assets).[33] Gatekeeper liability may provide an ex-ante incentive for gatekeepers to dissociate themselves from misconduct and to exercise reasonable care to prevent its occurrence. Ineffective direct deterrence is but one of several prerequisites for the imposition of gatekeeper liability. As Kraakman has pointed out, other requirements include (1) inadequate private gatekeeping incentives; (2) the ability of gatekeepers to detect misconduct at a reasonable cost; and (3) the ability of gatekeepers to reliably prevent misconduct.[34] This article will examine each of these prerequisites in the context of data misuse and propose that it is sometimes appropriate to impose gatekeeper liability on individuals to prevent them from disclosing certain types of personal data in their possession. In addition to deterrence, gatekeeper liability also serves a secondary function of providing compensation to victims who are otherwise unable to seek relief against the wrongdoers.

1. Direct Deterrence is Ineffective

Imposing liability directly on the party misusing personal data is likely more effective where that party is an established organization, such as a public company. Such an organization will likely suffer significant reputational harm if it is found to engage in data misuse. Thus, it has a strong incentive to refrain from such misuse in the first place. Moreover, such an organization likely employs a number of workers and/or external

---

31. *See* Kraakman, *supra* note 29, at 61–66. Indeed, Kraakman himself suggests that the theory of gatekeeper enforcement is useful for analyzing antifraud doctrines, such as section 12(2) of the Securities Act of 1933, which imposes liability on "any person who offers or sells a security." *Id.* at 83–85. Over the years, the definition of "sellers" has been relaxed to reach "a wide range of intermediaries in securities sales." *Id.* at 85. As such, section 12(2) imposes liability on a fairly large group of persons, though perhaps not as large a group as "individual data subjects."

32. *See, e.g.*, Doug Lichtman & Eric A. Posner, *Holding Internet Service Providers Accountable*, 14 SUP. CT. ECON. REV. 221, 222–23 (2006); Assaf Hamdani, *Gatekeeper Liability*, 77 S. CAL. L. REV. 53, 65 (2003).

33. Kraakman, *supra* note 29, at 56–57.

34. *Id.* at 61.

service providers who might become whistleblowers, providing more opportunities to detect and report data misuse. Once data misuse is detected, victims and regulators are also more likely to bring actions against an established organization that presumably has relatively deep pockets.

By contrast, direct deterrence is less likely to be effective against wrongdoers who intentionally exploit other people's personal data for illegal purposes. For instance, criminals who use personal data to defraud or harass people will likely use countermeasures to avoid detection, making them harder to trace.[35] Even if the criminals can be located, there may be jurisdictional concerns. Since criminal law is generally territorial, if the criminals are located outside of the relevant jurisdiction, then it may be difficult for prosecutors to bring proceedings against them.[36] Even in the exceptional circumstances where criminal laws apply extraterritorially, there have been relatively few prosecutions due to both practical and legal complications.[37] To start, criminal investigations in another country often require cooperation from authorities in that country,[38] which may not be available. Furthermore, there may not be an extradition treaty between the United States and the country where a particular criminal resides.[39] In any event, prosecutors have limited time and resources and are often unable to bring charges against all criminals.[40] The victims of data misuse are also likely to experience various difficulties bringing civil actions against the wrongdoers. To begin with, a victim may not know the identity of the person who disclosed or misused his personal data, particularly where there has not been any criminal proceeding brought against the wrongdoer.[41] A victim might also lack the means or skills to track down the relevant wrongdoer even if he wants to do so. If the wrongdoer happens to reside overseas, the victim is faced with the additional burden of persuading a

35. *See, e.g.*, Scott Charney & Kent Alexander, *Computer Crime*, 45 EMORY L.J. 931, 943 (1996) (noting "[a] primary goal of every criminal scheme is to avoid getting caught").

36. Kraakman has focused on the cost of raising expected penalties against wrongdoers and, in particular, identified two contributing factors: (1) the misconduct may be expensive to detect or prosecute; (2) constraints on actual penalty levels. *See* Kraakman, *supra* note 29, at 56–57. He has not, however, discussed the practical difficulties of pursuing an overseas wrongdoer or highlighted the different obstacles faced by prosecutors and victims in criminal and civil proceedings respectively.

37. For a summary of these legal and practical difficulties, see CHARLES DOYLE, CONG. RSCH. SERV., 94-166, EXTRATERRITORIAL APPLICATION OF AMERICAN CRIMINAL LAW (2016).

38. *Id.* at 23.

39. *See id.* at 31–33.

40. *See* Adam M. Gershowitz & Laura R. Killinger, *The State (Never) Rests: How Excessive Prosecutorial Caseloads Harm Criminal Defendants*, 105 NW. U. LAW REV. (2011) (discussing the ramifications of excessive prosecutorial caseloads).

41. *See, e.g.*, Ying Hu, *The Role of Public Enforcement in Investor Compensation: A Hong Kong Perspective*, 46 COMMON L. WORLD REV. 216, 222–23 (2017) (discussing this "naming, blaming" problem in the context of financial misconduct).

court to exercise jurisdiction over the wrongdoer and allow service outside the jurisdiction against him.[42] In the event that a victim succeeds in bringing an action against a wrongdoer, he may not be able to enforce a judgment or award obtained in his favor if the wrongdoer has few assets within the jurisdiction.[43]

2. Gatekeeper's Ability to Detect Misconduct

Where an individual directly transfers personal data to a person who uses it to inflict unjustifiable harm on other people (hereinafter referred to as a "primary wrongdoer"), the individual sometimes knows or ought to know that the primary wrongdoer would subsequently misuse that data. It may be because the individual discloses personal data intending it to be misused. One obvious example is doxing, where a doxer discloses someone's personal data in the hopes that others will use that data to harass the person being doxed.[44] It may be because the primary wrongdoers have made it clear that they seek personal data for an illegal purpose. For example, a primary wrongdoer might seek DNA samples from the public expressly for the purpose of cloning a human organ, to conduct unapproved clinical trials, or even to develop genetically targeted weapons.[45] Alternatively, the circumstances under which the wrongdoer solicits personal data might be such that a reasonable person would be under a duty to satisfy himself that the relevant data would not be misused before providing it. It may be because the type of data sought is particularly sensitive—a notorious example was the website "Is Anyone Up," which encouraged men to upload nude pictures of women without their consent.[46] It may also be because the primary wrongdoer is seeking data that is clearly unrelated to or unnecessary for the services provided. For example, after the Cambridge

42. For a discussion of the requirements for a U.S. court to exercise in personam jurisdiction over foreign nationals and the difficulty of satisfying those requirements for victims of information technology and intellectual property theft, see Andrew F. Popper, *In Personam and Beyond the Grasp: In Search of Jurisdiction and Accountability for Foreign Defendants*, 63 CATH. U.L. REV. 155, 177–79 (2013).

43. For a discussion of the legal and practical difficulties of enforcing U.S. judgments overseas, see Samuel P. Baumgartner, *Understanding the Obstacles to the Recognition and Enforcement of U.S. Judgments Abroad*, 45 N.Y.U. J. INT'L L. & POL. 965 (2013).

44. A number of commentators consider existing legal protections against doxing unsatisfactory. *See, e.g.*, Alexander J. Lindvall, *Political Hacktivism: Doxing & the First Amendment*, 53 CREIGHTON L. REV. 1, 6–8 (2019).

45. *See, e.g.*, Sarah Knapton, *World Must Prepare for Biological Weapons That Target Ethnic Groups Based on Genetics, Says Cambridge University*, TELEGRAPH (Aug. 13, 2019, 12:01 AM), https://www.telegraph.co.uk/science/2019/08/12/world-must-prepare-biological-weapons-target-ethnic-groups-based.

46. BAILEY POLAND, HATERS: HARASSMENT, ABUSE, AND VIOLENCE ONLINE 114 (2016).

Analytica saga, an individual arguably should be more wary of quiz or gaming apps that seek access to his private mailbox messages.[47]

Even where an individual merely transfers personal data to an intermediary who does not directly use it to harm people, the individual may nevertheless know or ought to know that the data disclosed will likely be misused. The intermediary may be a high-risk recipient who will very likely cause the data to be transferred to a wrongdoer (hereinafter referred to as a "high-risk intermediary"). Transferring data to a high-risk intermediary is not dissimilar to leaving an unlocked car in a high-crime area, which is likely to be stolen by criminals to commit crime.[48]

The most obvious high-risk intermediary is one who actively supplies personal data to those who misuse it. The intermediary could be an unscrupulous data trader that sells personal data to fraudsters on the dark web,[49] or an online forum that promotes revenge porn.[50] An intermediary may also facilitate data misuse without intending to do so. For example, an app that helps locate women around its users could in turn be used by criminals to stalk and harass women.[51] Similarly, apps that track police vehicles have reportedly been used to inflict harm on police officers.[52] Finally, an intermediary might disclose personal data to wrongdoers against his will. An intermediary might have access to a database containing valuable personal data but fail to adopt adequate data security measures to safeguard that data, which could result in repeated data breaches.[53] Alternatively, a data trading company might sell personal data to

47. *See* Issie Lapowsky, *Cambridge Analytica Could Have Also Accessed Private Facebook Messages*, WIRED (Apr. 10, 2018, 12:18 PM), https://www.wired.com/story/cambridge-analytica-private-facebook-messages.

48. *See, e.g.*, Palma v. U.S. Indus. Fasteners, Inc., 681 P.2d 893, 901–02 (Cal. 1984).

49. *See* Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web.

50. *See* Sophie Gallapher, *Revenge Porn Campaigner Warns "Well Intended" Petitions Are Giving Abuse Sites More Traffic*, INDEPENDENT (Dec. 2, 2019, 1:57 PM), https://www.independent.co.uk/life-style/women/revenge-porn-website-shut-down-petitions-not-your-porn-a9229221.html.

51. Erik Kain, *The Problem with the* '*Girls Around Me*' *App Isn't That Women Are Lazy About Privacy*, FORBES (Apr. 6, 2012, 2:15 PM), https://www.forbes.com/sites/erikkain/2012/04/06/the-problem-with-the-girls-around-me-app-isnt-that-women-are-lazy-about-privacy.

52. Jack Nicas, *Apple Removes App That Helps Hong Kong Protesters Track the Police*, N.Y. TIMES (Oct. 9, 2019), https://www.nytimes.com/2019/10/09/technology/apple-hong-kong-app.html (explaining that Apple removed the app after receiving "'credible information' from the authorities and people in Hong Kong 'that the app was being used maliciously to target individual officers'").

53. Indeed, reports of data breaches have become increasingly widespread in recent years. Juliana De Groot, *The History of Data Breaches*, DIGIT. GUARDIAN (Dec. 1, 2020), https://digitalguardian.com/blog/history-data-breaches.

wrongdoers or other high-risk intermediaries because it fails to conduct proper due diligence on its customers.[54]

A possible argument against treating individuals as gatekeepers is that individual data subjects may not be able to determine whether they are transferring personal data to a primary wrongdoer or a high-risk intermediary. Individuals often do not know when their data is being collected and by whom.[55] Even if an individual knows that his data is being collected, the individual may not know why it is being collected or how it is subsequently used.[56] Additionally, it is often difficult for individuals to assess the quality of their own data security standards, let alone that of the person to whom they transfer data to.

However, treating individuals as gatekeepers does not require each individual to identify wrongdoers and high-risk intermediaries at all times. Rather, it suggests that individuals should share part of the costs of detecting and thwarting the activities of those persons. Additionally, we can assist individual data subjects in determining whether a potential recipient is high-risk by introducing the following presumption (hereinafter referred to as the "presumption of high-risk intermediary"): an entity is presumed to be a high-risk intermediary unless it declares either that (1) it does not disclose personal data in the ordinary course of its business; or that (2) if it does, it has sufficient grounds for believing that the persons receiving data from it would not misuse that data.

3. Gatekeeper's Ability to Prevent Misconduct

Sometimes preventing disclosure is sufficient to prevent misuse of personal data. Other times, it is not. For instance, an individual might involuntarily disclose personal data to third parties (e.g., cyber criminals). This suggests that sometimes preventing data misuse requires an individual to take positive steps to secure the data in his possession.

Moreover, where a significant number of individuals disclose the personal data in their possession, it may be sufficient to form a sufficiently large dataset from which additional insights can be generated and misused. In that case, it may not make a difference whether any specific individual chooses or refuses to disclose his or her data. As such, a primary wrongdoer

54. *But see* Theodore Rostow, *What Happens When an Acquaintance Buys Your Data: A New Privacy Harm in the Age of Data Brokers Note*, 34 YALE J. ON REGUL. 667, 705 (2017) (concluding that "courts to date have been leery to find data brokers negligent in the data sale context").

55. *Your Data Is Shared and Sold . . . What's Being Done About It?*, KNOWLEDGE@WHARTON (Oct. 28, 2019), https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done.

56. Emilee Rader, *Most Americans Don't Realize What Companies Can Predict from Their Data*, CONVERSATION (Feb. 11, 2019, 6:43 AM), http://theconversation.com/most-americans-dont-realize-what-companies-can-predict-from-their-data-110760.

may evade gatekeeping by transacting with individuals who are less vigilant or more corruptible.[57] However, even though any individual alone may not be able to prevent data misuse, a significant number of individuals collectively could do so by refusing to disclose the personal data in their possession. Imposing a limited duty to prevent data misuse can help reduce the likelihood that a primary wrongdoer would be able to collect personal data from a sufficiently large number of individuals.

The presence of a black market (e.g., the dark web, where stolen data is often sold) for personal data suggests that a person intending to misuse data may not need to directly deal with individual data subjects, which further undermines the strategy of relying on individuals as gatekeepers.[58] While the need to clamp down on the black market for data is obvious, individuals' gatekeeping function is not redundant since they have some ability to prevent the data in their possession from entering the black market in the first place (e.g., by taking measures to secure such data and, where possible, by refraining from dealing with primary wrongdoers or high-risk intermediaries). A wrongdoer might also evade gatekeeping by transacting with commercial data holders. It is not surprising that under existing laws, many data holders are already charged with protecting the personal data in their possession.[59] As explained more fully below, the presence of other gatekeepers does not necessarily render individual gatekeepers redundant.[60]

4. Gatekeeper's Ability to Provide Compensation to Victims

Even where a victim has suffered physical or financial injury,[61] the victim may not be able to obtain compensation by bringing an action against

---

57. Kraakman, *supra* note 29, at 63, 74 ("Thus, multiple contracting may be a persuasive reason to abandon gatekeeping if the odds are against any individual gatekeeper detecting or vetoing misconduct.").

58. *Id.* at 66 (discussing the relevance of an illicit market).

59. *See, e.g.*, Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (regulating the disclosure of medical records by health plans, health care clearinghouses, and health care providers); Fair Credit Reporting Act, Pub. L. No. 91-508, 84 Stat. 1127 (1970) (regulating the disclosure of financial data by consumer reporting agencies); Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (regulating the disclosure of personally identifiable financial information obtained by financial institutions); Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g (regulating the disclosure of education records by educational institutions); *see also*, William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1141–75 (2019).

60. *See infra* Section II.C.3.

61. At the moment, victims often find it difficult to obtain legal redress against persons that misuse their personal data. One of the main difficulties is proving they have suffered legally cognizable injury: for example, some courts find that increased risk of future injury is too speculative and that unaggregated personal data has little value. As result, individuals may be held to lack standing to bring a claim or, if they do succeed in proving their case, receive nominal damages. *See* Spokeo, Inc. v. Robins, 578 U.S. 330, 342–43 (2016); Daniel J. Solove & Danielle Keats Citron, *Privacy Harms*, 102 B.U. L. REV. (forthcoming 2022). One response to this difficulty is to recognize more types of privacy injury, such as risk and anxiety. *See,*

individual data subjects with limited financial means. The situation is more complicated where the harm is caused by a large number of individuals. The amount of relief that a victim might be able to recover from each defendant is likely outweighed by the administrative cost of bringing a lawsuit. Imposing gatekeeper liability on individual data subjects, therefore, may not be an effective way to provide compensation for victims of data misuse.

However, the gatekeeper liability's compensation function can be achieved through public enforcement. If found to have breached his duty as a gatekeeper, an individual may be required to pay a statutory fine, and the proceeds can be used to fund a scheme to compensate victims of data misuse. Similar schemes have been established to provide compensation for victims of financial misconduct. For example, the Securities and Exchange Commission (SEC) is authorized to levy civil fines, order disgorgement in enforcement proceedings, and distribute the funds to victims of financial misconduct.[62] It is estimated that, between 2002 and 2013, the SEC deposited $14.46 billion into 243 distribution funds, often called "fair funds," to compensate harmed investors.[63] The decision to distribute funds is made by either the SEC or the court in which the SEC brings a judicial proceeding against a defendant.[64] While the amount recoverable from each individual gatekeeper might be relatively small, this need not be the only source of revenue for the proposed scheme to compensate victims of data misuse: the author has argued elsewhere in favor of a data tax on certain data controllers for the purpose of compensating victims of data misuse.[65]

B. *Costs of Individual Gatekeeper Liability*

The analysis in the previous section suggests that a *prima facie* case can be made for relying on individuals as gatekeepers to prevent data misuse where (1) direct deterrence against primary wrongdoers is likely to be ineffective; and (2) individual data subjects are able to both detect and prevent data misuse.

This section discusses two additional prerequisites for imposing gatekeeper obligations on individual data subjects. First, the costs of gatekeeping should be lower than the benefits of imposing gatekeeper liability. Second, the costs of gatekeeping should be lower than the costs of direct enforcement against primary wrongdoers.

---

e.g., *id.*; Solove & Citron, *supra* note 1, at 756–74. Another response is to seek gain-based remedies against data users. *See* Bernard Chao, *Privacy Losses as Wrongful Gains*, 106 IOWA L. REV. 555 (2020).

62. Urska Velikonja, *Public Compensation for Private Harm: Evidence from the SEC's Fair Fund Distributions*, 67 STAN. L. REV. 331, 333, 340–41 (2015).

63. *Id.* at 333.

64. *Id.* at 342.

65. Ying Hu, *The Case for an Information Tax: Cumulative Harm in the Collective Misuse of Information*, 29 CORNELL J.L. & PUB. POL'Y 295, 340-43 (2019).

1. Costs of Gatekeeping

Kraakman identifies three types of costs associated with gatekeeping: private costs on gatekeepers, tertiary costs on third parties, and administrative costs in policing gatekeepers.[66] A gatekeeper's private costs include not only the costs of complying with a rule, but also the costs of detecting when a rule is applicable, and the costs of misapplication.

An individual's cost of compliance can be further divided into two types. The first type concerns the costs of taking positive steps to comply with a rule. An individual may be required to take reasonable measures to protect the personal data in his possession. This may involve, for example, incurring the cost of setting and memorizing strong passwords, using two-factor authentication, and installing security software. The second type concerns "frustration costs" that an individual experiences when the individual is prevented from sharing personal data with certain persons or from receiving the benefit, monetary or otherwise, of disclosing such data (e.g., the benefit of using "free" apps). One way to reduce an individual gatekeeper's compliance costs is to limit the scope and content of positive duties imposed on the gatekeeper. Positive duties (e.g., a duty to report potential data misuse) are often more costly to fulfil than negative duties (e.g., a duty not to intentionally cause harm to others) since the former requires a gatekeeper to invest time, resources, and effort to achieve compliance. The cost of complying with a positive duty, however, may be reduced by providing the gatekeeper with technical and financial support. An individual's burden to take appropriate security measures to protect his personal data may be alleviated by making reliable security software freely available to the public, which helps reduce the cost of identifying and purchasing such software. In addition to positive duties, certain negative duties might also be too onerous to be imposed on the general public. For instance, it may not be feasible to require an individual to refrain from disclosing the personal data in his possession if such disclosure is required to purchase goods or services that cannot be easily or cheaply replaced.[67]

With respect to the cost of misapplication, one concern is that individuals may not be in a position to determine whether the personal data that they intend to disclose will be misused (the "information gap" problem). The data recipients might be acting under false pretenses or conceal the purpose for which they seek the data. Imposing liability on individuals who are not in a position to detect data misuse may result in both under-deterrence and over-deterrence. For over-deterrence, individuals might refrain from disclosing personal data to a broader group of recipients who do not misuse data; for under-deterrence, they might still be induced

66. Kraakman, *supra* note 29, at 75.

67. It is more appropriate to impose liability on the companies providing such goods or services.

into disclosing data to fraudsters who intend to misuse it. To help bridge the information gap between individual data subjects and data recipients, an entity data recipient should be required to disclose (1) whether it transfers personal data to third parties in its ordinary course of business; (2) whether it has adequate grounds to believe that the data it has disclosed will not be misused; and (3) whether it has suffered data breaches in the past and whether its data practice is the subject of an on-going disciplinary proceeding ("data practice disclosures").

There is a risk that those who receive another's personal data will make false disclosures.[68] Nevertheless, requiring an entity to disclose whether it has sufficient grounds to believe that the data it shares will not be misused carries several benefits. First, it is arguably easier to bring an action against an entity that makes a false declaration than one that does not make any declaration. Making a false declaration is likely to amount to "unfair or deceptive acts or practices."[69] This would entitle the Federal Trade Commission to bring an action against the relevant entity pursuant to Section 5 of the Federal Trade Commission Act (FTC Act).[70] A false declaration might also enable data subjects to bring a claim for breach of contract, promissory estoppel, or misrepresentation against the relevant entity. Second, this requirement shifts the focus from obtaining individual consent to share data to establishing a practice of responsible data sharing. As many commentators have noted, relying on individuals to withhold consent from data recipients is not always an effective strategy to minimize data misuse.[71] Third, this requirement can be supplemented with additional measures to incentivize whistleblowing by individuals who have first-hand knowledge of false declarations by data recipients.[72] Apart from the

68. An example of false promises relating to a company's data practice can be found in *In re* Nickelodeon Consumer Privacy Litigation, 827 F.3d 262 (3d Cir. 2016). Defendant Viacom's registration form included a message: "HEY GROWN-UPS: We don't collect ANY personal information about your kids. Which means we couldn't share it even if we wanted to." *Id.* at 269. Despite that promise, both Viacom and Google allegedly used cookies to track children's web browsing and video-watching habits on Viacom's websites. *Id.*

69. *See, e.g.*, FTC Policy Statement on Deception, Letter from James C. Miller III, Chairman, Fed. Trade Comm'n, to the Honorable John D. Dingell, Chairman, Comm. on Energy & Com., U.S. House of Representatives (Oct 14, 1983) https://www.ftc.gov/system /files/documents/public_statements/410531/831014deceptionstmt.pdf ("Practices that have been found misleading or deceptive in specific cases include false oral or written representations . . . .").

70. 15 U.S.C. § 45(a). Section 5(a) of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce." *Id.* § 45(a)(1). For a discussion of FTC's enforcement actions under Section 5 of the FTC Act in the context of privacy law, see Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).

71. *See, e.g.*, Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880 (2013).

72. Various programs already exist to provide reward for whistleblowers that report violations of the federal securities laws, tax fraud, and so on. *See* Jason Zuckerman &

information gap problem, there may also be misapplication costs caused by human error or by an individual's tendency to avoid risk. While unavoidable, these costs can be partially alleviated by reducing ambiguities in the applicable rule and by providing external guidance on compliance.[73]

An individual gatekeeper's costs of determining the applicability of a rule can also be reduced through various means. First, the cost of detecting whether a data recipient is high-risk can be reduced by requiring entity data recipients to make data practice disclosures and by relying on the presumption of high-risk intermediary. This presumption also has the incidental benefit of incentivizing data recipients to make those disclosures. Moreover, the cost of detecting high risk data recipients can be decreased by reducing the amount of time and effort each individual must invest in to read and understand the relevant declarations. This may be achieved, for example, by standardizing the language that each recipient uses to declare its practice for sharing personal data and by requiring the recipient to display these declarations in a prominent place (e.g., it may be contained in a website's footer in a large font and bright color immediately before the website starts to collect personal data).[74] Additionally, including a scienter requirement rather than basing liability on mere negligence is also likely to reduce individuals' cost in monitoring their behavior.[75]

Tertiary costs refer to the costs imposed on parties other than gatekeepers and primary wrongdoers.[76] These costs may be the result of a change in the gatekeepers' behavior in response to the prospect of incurring liability. For example, an individual might become less willing to disclose personal data in general, which could have a chilling effect on free speech or thwart efforts to use private information for socially beneficial causes.[77] It might also increase the cost of business for companies that collect and use personal data to develop products and services.[78] However, the fact that

---

Matthew Stock, *Whistleblower Rewards for Reporting Wrongdoing*, ZUCKERMAN L., https://www.zuckermanlaw.com/sp_faq/what-is-a-whistleblower-reward (last updated Nov. 23, 2021).

73. Such guidance might be supplied by the Federal Trade Commission, which has extensive experience enforcing privacy and data security law.

74. Indeed, many of the strategies which have been proposed to streamline privacy notices can be used. *See, e.g.*, Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1031–44 (2013).

75. Kraakman, *supra* note 29, at 75–76.

76. *Id.* at 75.

77. *See, e.g.*, Yafit Lev-Aretz, *Data Philanthropy*, 70 HASTINGS L.J. 1491, 1515 (2019). Lev-Aretz defines "data philanthropy" as the giving of private sector data for a socially beneficial purpose. *Id.* at 1503.

78. In a different context, it has been argued that allowing private companies to share data with the government could lead to a decrease in both the quantity and the quality of the data collected, thereby having a negative impact on data-driven innovation. Niva Elkin-Koren & Michal S. Gal, *The Chilling Effect of Governance-by-Data on Data Markets*, 86 U. CHI. L. REV. 403, 423–29 (2019).

individuals are more reluctant to disclose personal data also has several benefits: first, it reduces an individual's risk of being exposed to data misuse—even a responsible data recipient increases the risk of harm to the individual whose data was transferred (e.g., the recipient might fall victim to a malicious data breach, resulting in unintentional disclosure of the personal data in the recipient's possession). Second, as explained more fully in Part III, as the number of persons holding an individual's data decreases, the individual's incentive to invest in security measures to protect his own data increases. Moreover, to the extent that imposing individual gatekeeper responsibility helps reduce incidents of data misuse, it can also provide greater incentives for people to disclose their data in the first place. In addition, tertiary costs may be reduced through regulations that provide reliable channels for individuals to share their personal data. In addition to imposing disclosure obligations on entity data recipients, the government may, through an opt-in licensing regime, help individuals identify entities as safe data recipients. These would be entities that satisfy certain baseline data security requirements, including, for example, taking specific steps to secure the data in their possession, transferring personal data only to similarly licensed entities, and not using personal data for any illegal purpose. Transferring personal data to such entities would be presumptively compliant with an individual's duty as a gatekeeper.

Finally, the administrative costs of policing gatekeepers may be shared between individual victims of data misuse and the public. Those victims may pursue a private action against an individual gatekeeper if they are aware of the latter's role in causing their loss and if an action against the primary wrongdoer is impractical. By contrast, public enforcement is likely more effective where a victim is unaware of a gatekeeper's misconduct or where the cost of pursuing a private action is prohibitively high. While the level of public enforcement is limited by the labor and financial resources of the responsible agency, enforcement actions against individual gatekeepers may be combined with direct enforcement against primary wrongdoers, thereby enjoying some economies of scale.[79] Additionally, any enforcement action against individual gatekeeper is likely to have not only a specific, but also general, deterrent effect, which helps lower enforcement costs in the long run.

Given the significant costs of gatekeeping, the case in favor of gatekeeper liability is strongest where the data misuse in question is serious, such as cases where the misuse may lead to serious physical injury (e.g., terrorism), significant financial or emotional harm (e.g., revenge porn), or violations of human rights (e.g., discriminatory use of personal data). The

79. *See* Kraakman, *supra* note 29, at 56–57, 75 n.67.

difficulty lies in designing a carefully calibrated gatekeeper liability regime where its cost can be justified by its benefit.[80]

2. Is the Cost of Gatekeeping Lower Than Direct Enforcement?

Assume that a certain use of personal data is so undesirable that it should be prohibited. Imposing gatekeeper obligations on individual data subjects is justified only if the cost of doing so is at least sometimes lower than the cost of direct enforcement against primary wrongdoers.

The previous section sets out various ways to minimize costs of gatekeeping. By contrast, the cost of direct enforcement against primary wrongdoers can sometimes be insurmountably high due to factors that are difficult to change. As noted above, it is likely costly to locate a tech-savvy primary wrongdoer who hides behind the anonymity of the internet.[81] Moreover, where a wrongdoer resides out of the victim's jurisdiction, prosecutors and victims must overcome additional hurdles in order to bring a criminal or civil action against him/her.[82] They also risk obtaining an empty judgment where the wrongdoer has too few assets within the jurisdiction to be enforced against.[83] When weighed against such significant costs of direct enforcement, it is conceivable that the same deterrence effect can sometimes be achieved more cost-effectively through the imposition of limited gatekeeper responsibility on individual data subjects. In Section II.D, this article proposes a new legal duty to prevent data misuse. It seeks to strike a balance between preventing data misuse and minimizing gatekeeping costs.

C. *Alternatives to Imposing Gatekeeper Liability on Individuals*

Imposition of gatekeeper liability on individuals must not be redundant. Gatekeeper liability might be redundant where there are adequate private gatekeeping incentives, effective private contracting for gatekeeping services, or other more cost-effective gatekeepers.[84] Each of these three factors will be examined in turn.

1. Inadequate Private Gatekeeping Incentives

One might argue that individuals already have sufficient incentives not to disclose personal data to potential wrongdoers or high-risk

80. Various scholars have highlighted the difficulty of choosing an appropriate gatekeeper regime. *See, e.g.*, Ronald J. Mann & Seth R. Belzley, *The Promise of Internet Intermediary Liability*, 47 WM. & MARY L. REV. 239 (2005).

81. *See supra* Section II.A.1.

82. *See supra* Section II.A.1.

83. *See supra* note 43 and accompanying text.

84. Kraakman noted that wholly private incentives might suffice to encourage private enforcement. See Kraakman, *supra* note 29, at 56.

intermediaries. First, individuals likely possess personal data relating to both themselves and to their acquaintances. To avoid harming themselves, individuals are likely unwilling to disclose data about themselves to persons who are likely to misuse it. Moreover, social norms, including a sense of personal integrity, would probably discourage individuals from disclosing personal data about their acquaintances to persons suspected of data misuse. These non-legal incentives are further bolstered by existing legal duties not to disclose (e.g., torts like public disclosure of private facts and breach of confidence).

A closer examination of the above-mentioned incentives suggests that they may not be sufficient to induce adequate gatekeeping. Individuals might disclose their personal data upon belief that such data will harm only other people. For example, individuals might disclose their race, sexual orientation, or genetic data, believing that they are unlikely to be discriminated against based on such data.[85] Alternatively, as Fairfield and Engel have pointed out, individuals might be induced to disclose personal data where they reap all the benefit of such disclosure but bear only a fraction of the cost.[86] This may be the case where data misuse causes social harm and all citizens share the cost (e.g., where it undermines national security).[87]

Additionally, existing legal sanctions may not be adequate to deter an individual from making disclosures that harm others. As Danielle Keats Citron has argued, the four types of privacy torts formulated by William Prosser in his seminal article, *Privacy*,[88] are ill-equipped to prevent privacy harms caused by modern technology.[89] For example, the four privacy torts fail to adequately address data leakage as well as doxing.[90] Moreover, private enforcement is unlikely to be effective where the victims are unaware that their personal data has been, directly or indirectly, disclosed (e.g., where there is no public disclosure of information) or are unable to identify the source of the disclosure. Sometimes victims may not even know the person disclosing their personal data (e.g., a woman skinny dipping in her backyard might be accidentally filmed by a drone), and thus may be unable to persuade or pressure that person not to disclose that data.

---

85. According to one study, individuals who voluntarily post their genetic information online suggest that they believed they were less likely to suffer privacy-related harm because they did not belong to vulnerable social groups. Tobias Haeusermann et al., *Genes Wide Open: Data Sharing and the Social Gradient of Genomic Privacy*, 9 AJOB EMPIRICAL BIOETHICS 207, 211 (2018).

86. Fairfield & Engel, *supra* note 10, at 423.

87. For a summary of the social harms that flow from "emission" of data, see Ben-Shahar, *supra* note 1, at 112–16.

88. William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960).

89. Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1809–10 (2010).

90. *See id.* at 1809.

Finally, various studies indicate that people are willing to disclose the personal data in their possession for a relatively small benefit.[91] A recent survey of 15,600 people across six countries found that people are willing to part with their personal data for fairly trivial amounts of money: an average of $1.82 per month to share their location, $7.56 to share their fingerprint, and a "whopping" $8.44 to share their bank balance.[92] People also seem to value their own personal data more highly than that of their friends,[93] so they may be more willing to disclose data that appears to relate only to other people.

2. Ineffective Private Contracting for Gatekeeping Activities

In theory, potential victims of personal data misuse could contract with individual gatekeepers for their service. However, several obstacles are likely present. First, for any individual, a large number of persons likely already or will possess their personal data.[94] Therefore, the cost of negotiating a gatekeeping service with each person is likely to be prohibitively high. Second, there is a fair amount of uncertainty over the value of such a gatekeeping service. While there is hardly any legitimate market for individuals to trade their personal data, anecdotal evidence suggests that the market value of a given piece of personal data is quite minimal.[95] This is compounded by the fact that the quality of each gatekeeper's service cannot be easily assessed.

Third, it can be difficult for an individual to police the performance of his gatekeepers, especially since personal data, unlike a trade secret or confidential information, is often held by multiple people. It is therefore

---

91. *See, e.g.*, Alessandro Acquisti, Leslie K. John & George Loewenstein, *What Is Privacy Worth?*, 42 J. LEGAL STUD. 249 (2013); Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1, 9–10 (2021).

92. Chris Stokel-Walker, *People Will Sell Access to Their Fingerprints for Just $7.56 a Month*, NEW SCIENTIST (Feb. 7, 2020), https://www.newscientist.com/article/2232793-people-will-sell-access-to-their-fingerprints-for-just-7-56-a-month.

93. Yu Pu & Jens Grossklags, *Towards a Model on the Factors Influencing Social App Users' Valuation of Interdependent Privacy*, PROC. ON PRIV. ENHANCING TECHS., Apr. 2016, at 61, 67–68 (in their study, social app users appeared to place greater value on their own privacy than the privacy of their social network friends combined). The authors suggest that this can be partially explained by the fact that "most friendship ties are weak on SNSs." *Id.* at 68.

94. For example, the information that John has dined at a particular restaurant could be possessed by the restaurant, an independent restaurant booking system (such as OpenTable), Google (if he shared the booking information with Gmail or Google Calendar), Uber (or other ride-sharing app), any person at the restaurant at the same time as John, and any other person with whom these parties choose to share the information.

95. According to Financial Times' personal data calculator, "[g]eneral information about a person, such as their age, gender and location is worth a mere $0.0005 per person." Emily Steel et al., *How Much Is Your Personal Data Worth?*, FIN. TIMES (June 12, 2013), https://ig.ft.com/how-much-is-your-personal-data-worth.

hard to identify the faulty gatekeeper. Moreover, private contracting is impracticable where individuals do not know or have no interaction with the persons holding their personal data. Finally, private contracting is unlikely to adequately take into account the harm caused by data misuse to the general public since each individual only bears a small fraction of the cost of that harm.[96]

3. Interaction with Other Gatekeepers

Individual data subjects are not the only, or the most obvious, gatekeepers to prevent misuse of personal data. A number of commentators have advocated for imposing gatekeeper liability on online service providers (OSPs) (e.g., social media platforms and other website operators),[97] and software vendors.[98]

OSPs and software vendors have several advantages as gatekeepers. For instance, OSPs are sometimes more effective gatekeepers since wrongdoers rely on their service to access victims. Their experience in dealing with different types of users may enable them to identify patterns of misconduct more easily.[99] Moreover, they are more likely to have the financial and technical means to implement measures to detect and prevent wrongdoing.

The presence of other gatekeepers, however, does not necessarily render individual gatekeepers redundant. To begin with, imposing gatekeeper liability on intermediaries such as OSPs has its drawbacks. One major concern is that OSPs might overreact and exclude services from certain users.[100] For example, an OSP might be over-zealous in removing questionable posts for fear of attracting liability, resulting in undue

96. *See* Ben-Shahar, *supra* note 1, at 119–21.

97. *See, e.g.*, Lichtman & Posner, *supra* note 32, at 222–23 (arguing in favor of imposing liability on internet service providers (ISP) on the basis that "ISPs are in a good position to reduce the number and severity of bad acts online"); Raphael Cohen-Almagor, *The Role of Internet Intermediaries in Tackling Terrorism Online*, 86 FORDHAM L. REV. 425, 426, 445–51 (2017); Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans Sec. 230 Immunity*, 86 FORDHAM L. REV. 401, 414–19 (2017) (suggesting that website operators that are designed to facilitate illegal activities should bear some form of civil liability); *Information Fiduciaries*, *supra* note 3, at 1205–34; *Second Gilded Age*, *supra* note 3, at 1004–11.

98. Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, BERKELEY TECH. L.J. 1553, 1557–58 (2005). Rustad & Koenig argue that software vendors may expose their customers to third party crime just as landowners may do to people who enter their premises. *Id.* at 1582. Landowners have been held to owe a duty to protect tenants from foreseeable criminal attacks in common areas. *Id.* at 1570 n.84. By analogy, it may be appropriate to impose a duty on software vendors to minimize risks to their customers. *Id.* at 1569-70.

99. For example, it may be able to conduct "threat profiling" based on its users' behavior. *See* Daphne Keller, *Facebook Filters, Fundamental Rights, and the CJEU's* Glawischnig-Piesczek *Ruling*, 69 GRUR INT'L 616, 619 (2020).

100. Lichtman & Posner, *supra* note 32, at 241.

interference with freedom of speech.[101] To alleviate concerns over imposing excessive burden on the OSPs, a number of statutory provisions, notably Section 230 of the Communications Decency Act,[102] provide OSPs with broad immunity over user-generated content.[103] Courts have traditionally taken an expansive view of Section 230 immunity,[104] shielding a platform from liability for user generated content unless the platform assisted in the development of what made the content unlawful.[105] Although some commentators argue that these provisions over-protect OSPs,[106] others maintain that such immunity is essential to promote innovation on the internet and to motivate voluntary content moderation.[107] These provisions, as applied by the courts, significantly limit the scope of OSP gatekeeper liability.

Moreover, individual data subjects are sometimes in a better position than OSPs to identify potential wrongdoers and to take cost-effective measures to halt or prevent the misuse of personal data. Firstly, an individual may interact with a primary wrongdoer directly, whose conduct might provide ample grounds for a reasonable person to question the purpose for which s/he seeks personal data. By contrast, an OSP may have tens of thousands of users and therefore must devote substantial resources to identify and take action against wrongful activities initiated by its users. This could impose an undue hardship on certain OSPs, particularly start-ups.[108] While some OSPs use content filter technology to remove harmful

---

101. *See, e.g.*, Zeran v. Am. Online, Inc., 129 F.3d 327, 333 (4th Cir. 1997); Assaf Hamdani, *Who's Liable for Cyberwrongs*, 87 CORNELL L. REV. 901, 916–21 (2002); Felix T. Wu, *Collateral Censorship and the Limits of Intermediary Immunity*, 87 NOTRE DAME L. REV. 293, 298–309 (2011); Daphne Keller, *Who Do You Sue? State and Platform Hybrid Power over Online Speech* (Hoover Inst., Aegis Series Paper No. 1902, 2019), https://pacscenter.stanford.edu/publication/who-do-you-sue-state-and-platform-hybrid-power-over-online-speech.

102. 47 U.S.C. § 230.

103. *See also, e.g.*, Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified in scattered sections of 17 U.S.C.).

104. *See, e.g.*, Eric Goldman, *Why Section 230 Is Better Than the First Amendment*, 95 NOTRE DAME L. REV. REFLECTION 33 (2019); *see also* Citron, *supra* note 89, at 1839–41; Citron & Wittes, *supra* note 97, at 406–14.

105. *See, e.g.*, Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157, 1174–75 (9th Cir. 2008).

106. *See, e.g.*, Lichtman & Posner, *supra* note 32 *passim*.

107. *See, e.g.*, Eric Goldman, *An Overview of the United States' Section 230 Internet Immunity*, *in* OXFORD HANDBOOK OF ONLINE INTERMEDIARY LIABILITY 155, 165 (Giancarlo Frosio ed., 2020); Daphne Keller, *Internet Platforms: Observations on Speech, Danger, and Money* 9 (Aegis Series Paper No. 1807, 2018), http://papers.ssrn.com/abstract=3262936.

108. YouTube reportedly employs 10,000 people in monitoring and removing content globally. *Social Media: How Do Other Governments Regulate It?*, BBC NEWS (Feb. 12, 2020), https://www.bbc.com/news/technology-47135058. Often, platforms cannot rely purely on content filter technology, which are likely to unnecessarily silence lawful speech. *See, e.g.*, Keller, *supra* note 99, at 617–18. Attempts to use AI to help identify illegal materials are not as successful as one would hope. *Id.* at 619.

materials, such technology is often ill-equipped to deal with novel situations[109] and are also prone to make technical mistakes.[110] Secondly, sometimes the communication an individual has with a primary wrongdoer is unique—this is particularly likely where the wrongdoer selectively targets individuals based on their characteristics or past experience. Even if a platform tries to identify potential misconduct by creating fictitious accounts, that account may not receive similar messages.[111] Thirdly, it may not be legal or practical for a platform to monitor certain parts of its users' interactions. For example, a messaging app might adopt encryption methods that prevent the platform itself from seeing its users' messages.[112] Finally, some platforms might simply be unwilling to take measures against wrongdoers because doing so is contrary to their business model. As Andrew Tuch has noted in the context of corporate and securities transactions, we rarely rely on a single gatekeeper to deter wrongdoing in practice.[113] Gatekeeping responsibility is often more appropriately shared among multiple gatekeepers, each with "distinct spheres of influence and expertise."[114] Given that individual data subjects and OSPs are each better positioned to deter data misuse in different contexts, a strategy involving multiple gatekeepers is likely most effective.

D. *A New Legal Duty to Prevent Data Misuse*

As a gatekeeper, an individual data subject should be under a legal duty not to disclose his personal data in certain circumstances, which are set out below. This proposed duty would not only deter misuse of personal data, but also, more importantly, clarify the nature of an individual gatekeeper's appropriate conduct with respect to the personal data in his possession. This will help develop norms around the handling of personal data in this digital era.

The proposed duty can be stated as follows:

---

109. *See* Keller, *supra* note 107, at 6–8.

110. EVAN ENGSTROM & NICK FEAMSTER, THE LIMITS OF FILTERING: A LOOK AT THE FUNCTIONALITY & SHORTCOMINGS OF CONTENT DETECTION TOOLS (2017), https://www.engine.is/the-limits-of-filtering.

111. For example, a fictitious account for a mid-aged man who likes country music may not receive messages from fraudsters that target Beyoncé fans.

112. *Answering Your Questions About WhatsApp's January 2021 Privacy Policy Update*, WHATSAPP, https://faq.whatsapp.com/general/security-and-privacy/answering-your-questions-about-whatsapps-privacy-policy/?lang=en (last visited Nov. 25, 2021).

113. Tuch, *supra* note 30, at 625; s*ee also* Andrew F. Tuch, *Multiple Gatekeepers*, 96 VA. L. REV. 1583, 1585 (2010) (pointing out that the literature on gatekeeper liability has overlooked the multiple gatekeeper phenomenon).

114. Tuch, *supra* note 30, at 625.

> Where an individual is aware of facts indicating that the person seeking personal data from him is highly likely to (a) misuse it (i.e., a primary wrongdoer);[115] or (b) facilitate its misuse (i.e., a high-risk intermediary), then the individual is obligated to take reasonable measures to prevent that misuse. [116]

High-risk intermediaries include entities that (a) disclose personal data in the ordinary course of business and (b) do so without adequate grounds to believe the data will not be misused. To establish a reasonable belief that the data in its possession will not be misused, an entity must show that its data recipients have undertaken not to use personal data for illegal purposes and that the entity has reasonable means to verify the validity of that undertaking.[117] For example, the entity may order production of periodic reports as to how recipients of personal data use it. An entity can also show grounds to believe that the data will not be misused where the data recipient has a compliance team to monitor its data practices. In other words, an entity should establish that it is reasonable for the entity to rely on the recipient as a responsible data user.[118]

The proposed duty strikes a balance between preventing data misuse and minimizing individual gatekeeping costs in several ways. Firstly, it imposes a scienter requirement: individuals are only liable if they are aware of facts indicating that they are likely dealing with a primary wrongdoer or a high-risk intermediary. Secondly, as noted in Section II.B.1, an entity should be required to make a series of data practice disclosures, such as whether it transfers personal data to third parties in its ordinary course of business and whether it has adequate grounds to believe that the data it has disclosed will not be misused. Individuals should be entitled to rely on such disclosures to fulfil their legal obligations. As such, these disclosures help reduce the amount of investigative costs that individuals must incur to

115. If an individual chooses to disclose personal data and a tort materializes, s/he might also be liable for aiding and abetting that tort.

116. An individual data subject is only required to take reasonable measures: s/he is not an insurer of data misuse. A similar point was made in *Kline v. 1500 Massachusetts Avenue Apartment Corp.*, 439 F.2d 477, 487 (D.C. Cir. 1970) in respect to a landlord's duty to protect his tenants. ("We do not hold that the landlord is by any means an insurer of the safety of his tenants. His duty is to take those measures of protection which are within his power and capacity to take, and which can reasonably be expected to mitigate the risk of intruders assaulting and robbing tenants.").

117. Indeed, commentators have argued that platforms such as Google and Facebook should be considered "information fiduciaries", which owe a duty not to disclose personal data to anyone who does not assume similar fiduciary obligations. *See, e.g.*, JACK BALKIN, FIXING SOCIAL MEDIA'S GRAND BARGAIN 11–15 (Hoover Inst., Aegis Paper Series No. 1814, 2018) https://www.hoover.org/research/fixing-social-medias-grand-bargain; *Information Fiduciaries*, *supra* note 3.

118. An entity would not be able to establish such belief if, for example, it is aware that its data recipient has repeatedly failed to adopt appropriate measures to secure the personal data in the recipient's possession.

determine whether they are dealing with a primary wrongdoer or high-risk intermediary. If, for example, an entity has revealed that its data practices are subject to an ongoing disciplinary proceeding, then any individual transferring personal data to that entity will run the risk that he or she might be held liable for doing so.

Thirdly, "high-risk intermediary" is narrowly defined to exclude natural persons, in order to avoid undue interference with individuals' daily lives. [119] Individuals have to decide whether it is appropriate to disclose certain personal data to other individuals on a daily basis. The risk of incurring legal liability for such decisions might cause individuals to be unduly cautious when interacting with others. It is arguably more appropriate to leave these decisions to be guided by social norms.

Finally, individuals should not be required to refrain from disclosing personal data to an entity if such disclosure is necessary to obtain goods or services that are essential to their lives and cannot be replaced at a reasonable cost. For example, an argument can be made that, given that Facebook has 2.91 billion monthly active users,[120] its social networking service is an essential part of modern social life.[121] The "network effect" makes the service even more difficult to replace, as an individual's decision to switch to a different social networking platform is not the same as staying with an existing social network unless one's friends and family also switch social networks. As such, an individual should not be expected to dissociate himself from Facebook completely but may be expected to refrain from disclosing personal data to certain persons or apps that use Facebook as a platform to collect or use personal data.

III. A SOCIAL DUTY TO SECURE PERSONAL DATA

At present the legal duty to prevent data misuse does not entail a duty to take positive steps to secure the personal data in one's possession. Nevertheless, this part explains why we should recognize a social duty to secure personal data.

---

119. A full discussion of whether the proposed duties are consistent with the First Amendment is outside the scope of this article. One might argue that the proposed duty should be treated as content neutral time, place, and manner regulation. One might even argue that it does not raise First Amendment questions because it targets conduct, not speech.

120. *Facebook Fast Facts*, CNN (Oct. 31, 2021, 5:39 PM) https://www.cnn.com/2014/02/11/world/facebook-fast-facts/index.html.

121. *See, e.g.*, Packingham v. North Carolina, 137 S. Ct. 1730, 1737–38 (2017) (recognizing that social media platforms are "integral to the fabric of modern society and culture"—they are the "principal sources for knowing current events, checking ads for employment, speaking and listening in the modern public square, and otherwise exploring the vast realms of human thought and knowledge").

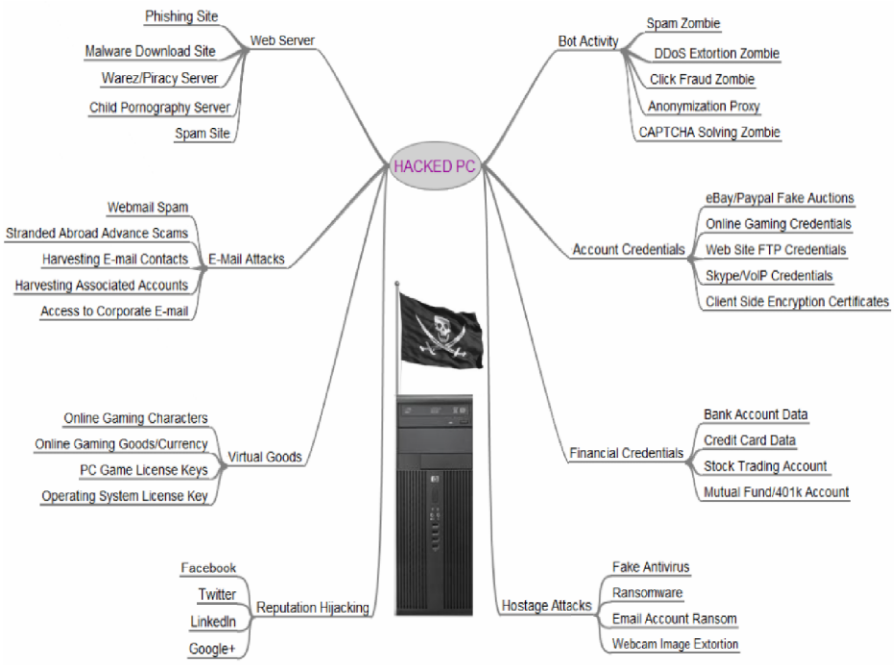
Individuals who possess personal data sometimes unwittingly facilitate unlawful collection and use of such data by others. If we do not safeguard our email accounts, for instance, they may be used by hackers to send phishing or spam messages to our contacts, who might in turn be tricked into disclosing their personal data or fall victim to other scams.[122] Similarly, our accounts with cloud service providers, such as Dropbox and Google Drive, might be used to host and share malware or illegal content (e.g., child pornography).[123] Our computers, if hacked, may become part of a network that attacks other individuals or websites without our knowledge.[124] Indeed, security experts have outlined many ways that a hacked computer could be used to harm the computer owner and other people (see the chart below[125]).

122. Bruce Barnett, *Are You a Target for Hackers?*, INFO SEC. ADVISOR (Apr. 13, 2017), https://infosecurityadvisor.wordpress.com/2017/04/13/are-you-a-target-for-hackers ("Your email account can be used to send spam and phishing messages. This can be used to trick your friends into sending money or your co-workers into clicking on a malicious link.").

123. *Id.* ("Your accounts on remote services like Dropbox, Google Drive, or OneDrive can be used to host and share malware or illegal files.").

124. *Id.* ("Your computer is valuable to hackers—and the faster your computer and your network connection, the more your computer is worth. If it gets infected with malware, it could become part of a robot network (botnet): one of millions of computers that allow a hacker to run automated programs on it without you ever knowing.").

125. Brian Krebs, *The Scrap Value of a Hacked PC, Revisited*, KREBS ON SEC. (Oct. 15, 2012), https://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited.



As explained more fully below, individuals who invest in security measures to protect their personal data generate positive externalities by incentivizing others to invest in security as well. Under the appropriate circumstances, this could lead to a self-reinforcing virtuous cycle which helps improve the level of data security in a given community.

A. *Interdependent Security*

As noted in Part I, an individual's personal data is likely held by one or more parties (his acquaintances, service providers, and so on). From the individual's perspective, then, the risk of data breach comes from two sources: (1) an attack initiated against the individual himself and (2) an attack against another person holding his data. As such, the security of an individual's personal data depends on not only his own actions, but also on the actions of others (i.e., security is interdependent). If the individual does not invest in security to protect that personal data, a data breach could cause him to suffer losses. For simplicity, let us assume that if an individual invests in security, he would not suffer any data breach against himself. However, he may nevertheless suffer loss as a result of a data breach committed against another who holds his personal data. Let us further assume that an individual suffers the same loss whether or not the breach happens to the individual, or to another person holding the individual's personal data.

An individual's incentive to invest in security is clearly influenced by his cost of investing in security ($C_{security}$). The individual has little incentive to invest in security if $C_{security}$ is greater than the loss that would result of a data breach committed against him. That loss is calculated as the magnitude of the loss of a data breach ($L_{data\ breach}$) multiplied by the probability of the individual suffering a data breach ($P_{individual}$). In other words, a rational individual will not invest in security if $C_{security} > P_{individual} * L_{data\ breach}$.

Even if $C_{security} < L_{data\ breach} * P_{individual}$, however, a rational individual might nevertheless choose not to invest in security if the expected utility of investing in security is lower than the expected utility of not doing so. Assume that the benefit of retaining control over a piece of personal data is B_{data}. Assume further that, in addition to the individual, that piece of data is held by *x* number of persons. However, none of them choose to invest in security to protect the data in their possession. As a result, each of *x* number of persons imposes a risk of data breach on the individual. The sum of the probabilities that the individual would suffer a data breach as a result of others' failure to invest in security is P_x. From the individual's perspective, then, the expected utility of investing in security to protect that piece of data can be expressed as follows[126]:

$$B_{data} - C_{security} - (P_x * L_{data\ breach}).$$

The expected of utility of not investing in security, on the other hand, can be expressed as follows:

$$B_{data} - P_{individual} * L_{data\ breach} - (1 - P_{individual}) * P_x * L_{data\ breach}.$$

Therefore, the individual has an incentive to invest in security if and only if

$$C_{security} < P_{individual} * L_{data\ breach} * (1 - P_x).$$

As the number of persons holding the individual's personal data (*x*) increases, the probability that the individual will suffer a security breach as a result of others' failure to invest in security also increases. In the extreme case where *x* is infinite, that probability (i.e., P_x) would approach one.[127] In that case, the individual would have no incentive to invest in security as long as the cost of doing so is positive (i.e., greater than zero).

126. This is a simplified version of the equations presented in Howard Kunreuther & Geoffrey Heal, *Interdependent Security*, 26 J. RISK & UNCERTAINTY 231, 236–37, 237, 243 (2003).

127. From an individual data subject's perspective, this is similar to the "computer security" scenario discussed by Kunreuther and Heal. *See id*. at 242–43.

B. *Explaining the Privacy Paradox*

Interdependent security sheds new light on the phenomenon known as the "privacy paradox," that is, individuals claim to value privacy highly, but fail to take easy steps to protect it.[128] For example, one study found that people "do not always act in line with their stated privacy preferences, giving away information about themselves without any compelling reason to do so."[129] Another study found "little or no relation" between people's reported privacy attitudes and their propensity to provide certain personal data such as date of birth.[130] Even among the respondents who "expressed the highest concern for the scenario in which someone 5 years from now could know their current sexual orientation, partner's names, and political orientation," 48% identified their sexual orientation on social media, 47% revealed their political orientation, and 21% revealed their partners' name.[131]

Many scholars have sought to explain the privacy paradox. Some argue that individuals expressed attitude towards privacy may be at odds with what they truly feel, and thus, the actions they take to assure their privacy. Individuals might, due to peer pressure or other reason, express opinions that reflect perceived norms about privacy rather than their true opinion.[132] Alternatively, individuals might fail to take into account the opportunity cost of making decisions that protect privacy, and thus overstate their demand for privacy.[133]

Others maintain that even if a person's expressed preference for privacy is authentic, their behavior may not adequately reflect that preference for two main reasons. First, privacy-related decisions are often made under unfavorable conditions: individual behavior might be affected by various biases and heuristics. A person might risk disclosing personal data as a result of an "optimism bias";[134] they might be more willing to disclose personal data in exchange for a small short-term benefit due to "hyperbolic

128. Solove, *supra* note 91, at 1.

129. Bettina Berendt, Oliver Günther & Sarah Spiekermann, *Privacy in E-Commerce: Stated Preferences vs. Actual Behavior*, 48 COMMC'NS ACM 101, 104 (2005).

130. Alessandro Acquisti & Ralph Gross, *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook*, *in* PRIVACY ENHANCING TECHNOLOGIES 36, 50 (George Danezis & Philippe Golle eds., 2006).

131. *Id.* at 51.

132. Tobias Dienlin & Sabine Trepte, *Is the Privacy Paradox a Relic of the Past? An In-Depth Analysis of Privacy Attitudes and Privacy Behaviors*, 45 EUR. J. SOC. PSYCH. 285, 287 (2015).

133. Caleb S. Fuller, *Is the Market for Digital Privacy a Failure?*, 180 PUB. CHOICE 353, 371 (2019).

134. "Optimism bias" refers to "[t]he tendency for people to be optimistic about future events." *Optimism Bias*, OXFORD REFERENCE, https://www.oxfordreference.com/view/10.1093/oi/authority.20110803100252318 (last visited Nov. 25, 2021).

discounting";[135] their decision to share personal data might also be affected by seemingly innocuous things such as the timing when privacy notices are presented.[136] Moreover, people sometimes disclose more personal data than they intend where they have mistaken or incomplete information. For instance, according to one study, 62% of the people surveyed believed that if a website had a privacy policy, it could not share personal data about them with other companies without their consent.[137] Additionally, people's attitudes towards privacy may not be "relevant and consolidated enough" to influence actual behavior where attitudes are based on second hand rather than firsthand experiences.[138] The implicit assumption of this type of explanation is that remedying one or more of those unfavorable conditions could cause people to make more privacy protective decisions. As a result, proposed solutions seek to counteract people's biases and reduce information asymmetry by providing people with clearer and more salient information about privacy practices.[139] The discussion in this article is consistent with these observations and provides an additional explanation for the privacy paradox phenomenon—interdependent security. It also suggests, as explained below, that certain attempts to counteract those biases might be counterproductive.

The second explanation for the discrepancy between people's expressed preference about privacy and their behavior is that they may be behaving perfectly rationally when they make decisions that appear to be privacy invasive. For example, according to Ben-Shahar, a significant part of the harm caused by the collection and use of personal data is suffered by the general public.[140] People's expressed attitude towards privacy reflects their concerns about the social harms caused by data; however, they are less worried that data breaches will harm them personally and therefore continue to share their data.[141] Consequently, Ben-Shahar's proposal focuses on measures that force individuals and entities to internalize those social harms.[142] The analysis in this section remains agnostic as to whether people's attitude towards privacy mainly reflects their views on the social

135. Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality*, *in* PRIVACY AND TECHNOLOGIES OF IDENTITY: A CROSS-DISCIPLINARY CONVERSATION 15, 27 (Katherine J. Strandburg & Daniela Stan Raicu eds., 2006).

136. Solove, *supra* note 91, at 13. The timing when consent to share personal data is given is also relevant. As Christine Jolls has pointed out, an in-advance consent is often less reliable than a contemporaneous one because it lacks the "rationality-encouraging feature of certainty." Christine Jolls, *Privacy and Consent over Time: The Role of Agreement in Fourth Amendment Analysis*, 54 WM. & MARY L. REV. 1693, 1705 (2013).

137. JOSEPH TUROW ET AL., AMERICANS REJECT TAILORED ADVERTISING AND THREE ACTIVITIES THAT ENABLE IT 21 tbl.9 (2009), https://papers.ssrn.com/abstract=1478214.

138. Dienlin and Trepte, *supra* note 132, at 287.

139. *See, e.g.*, Calo, *supra* note 74, at 1042–44.

140. Ben-Shahar, *supra* note 1, at 112.

141. *Id.*

142. *Id.* at 131–48.

harms associated with data. It is therefore able to explain the privacy paradox where this is not the case, for example, where the collection and use of personal data does not cause significant public harm or where the relevant individual is unaware of or indifferent to public harm.

In contrast to Ben-Shahar, Daniel Solove claims that the privacy paradox is a myth—it does not exist.[143] According to Solove, studies about people's attitudes toward privacy often invite them to express concerns and preferences in general terms; by contrast, studies about people's privacy-related behavior observe their decisions in specific contexts.[144] As a result, the attitudes and behavior revealed by these two types of studies naturally diverge, which explains the privacy paradox phenomenon.[145] My discussion on interdependent security differs from Solove's in two respects. First, it does not rely on a distinction between general attitudes and specific decisions to explain the privacy paradox. Therefore, it can explain why an individual who values retaining control over a piece of data in a specific context may nevertheless fail to incur any cost protecting that data.[146] Secondly, it provides a more nuanced analysis of an individual's decision to invest in security. In particular, this article points out that whether an individual has sufficient incentive to protect his data in a particular instance depends not only on the cost of the relevant security measures, but also on his expectation of the security decisions made by others who also possess that data.

The discussion in this section suggests that an individual's decision to invest in security can be "contagious," that is, it incentivizes others (in particular, people whose data is in the individual's possession) to invest in security as well. This contagion effect can be illustrated with a numerical example. Consider a simple case in which a piece of data about A is held only by A and B. Assume further that the likelihood of A suffering a data breach against himself is 0.3 while the likelihood that A would suffer a data breach as a result of a data breach against B is 0.2. The magnitude of the loss from a data breach is 100 and the cost of investing in security for A is 28. If B does not invest in security, then A's expected utility of investing in security would be $B_{data} - 48$. At the same time, A's expected utility of not investing in security would be $B_{data} - 44$. As a result, a rational person in A's position would choose not to invest in security. By contrast, if B invests in security, then A's expected utility of investing in security would only be $B_{data} - 28$, which is higher than the expected utility of not investing in security (i.e., $B_{data} - 30$). As a result, a rational person would choose to invest in security. The table below shows A's expected utility in both

143. Solove, *supra* note 91, at 4.
144. *Id.* at 4, 19, 23–29.
145. *Id.* at 4.
146. *See supra* Section III.A above, explaining why an individual sometimes has no incentive to invest in security as long as the cost of doing so is positive.

scenarios as well as how A's optimal course of action changes depending on whether B invests in security.

	B invests in security	B does not invest in security
A invests in security	$B_{data} - 28$*	$B_{data} - 48$
A does not invest in security	$B_{data} - 30$	$B_{data} - 44$*[147]

My discussion of interdependent security also has a more counter-intuitive implication: that is, a privacy conscious individual might sometimes have less incentive to invest in privacy protective measures. An individual who is concerned about privacy (let us call him Allan) is more likely to be aware of the ubiquitous collection of personal data and widespread data breaches. As a result, he is more likely to believe that his data is held by a large number of persons who do not take adequate measures to safeguard it. The greater that number, my analysis suggests, the less incentive Allan has to invest to secure his own data. If Allan believes that the probability of him suffering a data breach as a result of others' failure to invest in security is sufficiently high, then Allan may not have an adequate incentive to protect his own data even where the cost of doing so is very low. Let us illustrate this point with a slightly different example. Assume that Allan's personal data is held by himself and ten other people who do not invest in security to protect their data. Similar to the previous example, the likelihood of Allan suffering a data breach against him is 0.3 while the likelihood that Allan would suffer a data breach as a result of a data breach against any of those ten people is 0.2. The magnitude of the loss from a data breach is 100 and Allan's cost of investing in security is 28. The main difference between this example and the previous one is that each of those ten people now imposes a risk of data breach on Allan. The cumulative probability that Allan would suffer a data breach as a result of those ten people's failure to protect their data becomes $[1 - (1 - 0.2)^{10}] \approx 0.9$. Consequently, Allan has an incentive to invest in security if and only if the cost of doing so is lower than $P_{individual} * L_{data\ breach} * (1 - P_{ten\ people}) \approx 3$. By contrast, in the previous example, even though the cost of investing in security is much higher (i.e., 28), A will still have incentive to invest in security if B also invests in security.

C. *Policy Implications*

The two examples in the last section suggest several ways to increase an individual's incentive to take measures to protect privacy. To begin with, the examples show that, as the number of persons investing in data security increases, the cumulative probability that an individual would suffer a security breach as a result of others' failure to invest decreases. Eventually,

147. The asterisk marks A's optimal course of action.

it may reach a point at which it would be cost-effective for the individual to invest in security as well. An individual's decision to invest in security provides additional incentive for others to do the same, thereby leading to a virtuous cycle in which more and more individuals choose to take privacy protective measures.[148] In this respect, the government may serve the important role of a "norm entrepreneur" by providing the initial incentive, whether legal,[149] financial, or reputational, for a number of individuals to invest in security measures to protect their personal data.[150] That number might subsequently reach a tipping point after which investing in security becomes a dominant strategy for most members of our society. By contrast, scare stories about irresponsible data handling are likely counter-productive: people would be led to believe that others do not invest in data security and in turn have less incentive to invest in security themselves, which undermines the proposed social duty to protect one's personal data.

Moreover, the analysis in this section suggests that an individual would have less incentive to invest in data security as the number of persons holding that individual's personal data increases. As such, the proposed social duty to invest in security would likely need to be supplemented by additional measures to discourage unnecessary acquisition and transfer of personal data. While existing laws, such as the Health Insurance Portability and Accountability Act,[151] impose a duty on certain entities to limit the use and disclosure of personal data to the minimum necessary to accomplish their intended purpose,[152] such requirements do not apply to all commercial data holders. Moreover, relatively few restrictions have been placed on individuals to disclose the personal data that they have legally acquired. Fostering a culture in which more individuals and entities are committed to collecting and transferring less personal data would not only reduce potential data misuse, but also bolster the social duty to secure personal data.

Finally, sometimes third parties are in a good position to enhance the competency of individuals as gatekeepers. For example, the government might cooperate with suppliers of cybersecurity services to make inexpensive and user-friendly security measures more widely available to

148. A detailed discussion of when this tipping point can be reached, however, is outside the scope of this paper.

149. For example, by recognizing a duty to prevent data misuse, as suggested in this article. *See supra* Section II.D.

150. "Norm entrepreneurs" are people interested in changing social norms. *See* Cass R. Sunstein, *Social Norms and Social Roles*, 96 COLUM. L. REV. 903, 909 (1996).

151. *See supra* note 59.

152. Office for Civil Rights (OCR), *Minimum Necessary Requirement*, U.S. DEP'T HEALTH & HUM. SERVS. (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement/index.html. Section 1798.100 of the California Consumer Privacy Act also provides that a business shall not collect additional categories of personal data without providing the consumer with the requisite notice. CAL. CIV. CODE § 1798.100 (2020).

the public. Reducing the cost of taking privacy protective measures is highly likely to encourage more individual gatekeepers to take such measures. The government might also impose design obligations on entities which collect and use personal data (the "entities"). Promoting privacy by design has several benefits: requiring entities to make the most privacy friendly setting as the default setting helps reduce the likelihood that individuals unwittingly disclose their personal data. Moreover, entities (especially social media platforms) might sometimes prompt their users to check whether they intend to disclose personal data before they (a) disclose what appears to be sensitive data or (b) disclose data to questionable recipients (e.g., potentially fraudulent account users). The suggested privacy prompts will encourage individuals to consider the consequences of their disclosure, which can potentially lead to less harmful disclosure.[153] In this respect, privacy by design serves a dual purpose: not only can it make entities more effective guardians of the personal data in their possession, but it can also make individuals more competent gatekeepers against data misuse.[154]

CONCLUSION

This article contributes to academic efforts to reduce data misuse. Rather than viewing individual data subjects only as victims of data misuse, they should be enlisted as part of the solution and should share part of the burden of detecting and preventing data misuse. Sometimes, the most cost-effective way to prevent data misuse is for individual data subjects to remain vigilant and to refrain from disclosing personal data to high-risk recipients. Imposing a duty on individuals to prevent data misuse does not, however, abrogate the need to impose similar obligations on big technology companies. Rather, an effective strategy to prevent data misuse requires imposing duties on individual data subjects, as well as on persons that use and collect personal data. These duties supplement and reinforce each other. On the one hand, imposing disclosure and design obligations on entities can help make individual data subjects more effective gatekeepers. On the other hand, the proposed duty on individuals to prevent data misuse can also incentivize the entities they interact with to compete more vigorously on privacy to attract and retain customers.

153. In a different context, researchers found that prompting individuals to consider the accuracy of the information that they are sharing on social media can potentially make them share fewer fake news stories. *See* Gordon Pennycook et al., *Shifting Attention to Accuracy Can Reduce Misinformation Online*, 592 NATURE 590 (2021).

154. I would like to thank Professor Jack Balkin for raising and discussing this point.