2022

Negligence at the Breach: Information Fiduciaries and the Duty to Care for Data

Daniel M. Filler

David M. Haendler

Jordan L. Fischer

CONNECTICUT
LAW REVIEW

VOLUME 54 MARCH 2022 NUMBER 1

Article

Negligence at the Breach: Information Fiduciaries and the Duty to Care for Data

DANIEL M. FILLER, DAVID M. HAENDLER & JORDAN L. FISCHER

Personal data is a cost of admission for much of modern life. Employers, tech companies, advertisers, information brokers, and others collect huge quantities of data about us all. Yet outside of a few highly-regulated industries, American companies face few legal restrictions on how they manage and use that data. Until now, individuals have had very limited remedies when their data is stolen from data collectors. But change is afoot. In a significant recent decision, the Pennsylvania Supreme Court took a consequential step holding that entities collecting personal data owe a duty of reasonable care to protect data subjects against harm.

This tort decision left a critical question unresolved. What is "harm" in the context of privacy? What is it exactly that data collectors must protect data subjects against? This Article takes one state's doctrinal move as a jumping-off point to consider a question of immense national importance—how to apply common law negligence principles in cases involving the disclosure and misuse of personal data, and specifically, what a "duty to care" means in the unsettled realm of privacy law. Building off Jack Balkin's work, this Article proposes that fiduciary law offers an appealing framework for conceptualizing privacy harms and the corresponding responsibilities of the entities who are collecting our data. In doing so, it begins the conversation of how tort law can take a central place in protecting individuals when data holders betray their trust.

ARTICLE CONTENTS

Negligence at the Breach: Information Fiduciaries and the Duty to Care for Data

DANIEL M. FILLER, [*] DAVID M. HAENDLER [**] & JORDAN L. FISCHER [***]

INTRODUCTION

Personal data is the price of admission to much of the Internet. Many leading service providers accept personal data as a substitute for cash payment. Facebook, Twitter, and Google rarely charge their "subscribers" a monthly tariff, but the choice to use these services comes at the cost of data. When individuals are uncomfortable sharing personal data with content providers or media companies—for example, if they are unwilling to risk a data spill—they can choose to cut the cord. However, in many cases, individuals must surrender personal data in exchange for the basics of survival. For example, what if you want a job?

Consider the University of Pittsburgh Medical Center (UPMC). UPMC is the largest private employer in Pennsylvania with approximately $23 billion in revenue.[1] It is a sprawling health care provider and insurer touching almost every corner of the state, with a growing international division.[2] Like pretty much every other employer in America, it collects data on its employees. It is required to do so to comply with tax, benefits, and employment laws, as well as for a variety of other practical reasons. You cannot get a job at UPMC, or frankly anywhere, without surrendering personal data. Unless you are independently wealthy, you cannot cut the cord on employment.

Thus, every employee puts herself at risk simply by choosing to work. UPMC employees learned that lesson in 2014. That spring, UPMC announced that cyber-criminals had infiltrated its computer systems, compromising the data of up to 62,000 individuals and exposing hundreds

---

[*] Dean and Professor of Law, Drexel University Thomas R. Kline School of Law.

[**] Research and Instructional Services Librarian and Adjunct Professor of Law, Drexel University Thomas R. Kline School of Law.

[***] Director of Center for Law and Transformational Technology and Assistant Teaching Professor of Law, Drexel University Thomas R. Kline School of Law.

[1] *UPMC Facts and Stats*, UNIV. OF PITTSBURGH MED. CTR., https://upmc.com/about/facts/ (last visited Sept. 1, 2021).

[2] *UPMC Fast Facts*, UNIV. OF PITTSBURGH MED. CTR., https://www.upmc.com/-/media/upmc/about/facts/documents/fast-facts.pdf?la=en&hash=020D1C5749D88500376CA9A0302F06B8F058AEFC (last visited Oct. 29, 2021).

of employees to possible tax fraud.[3] Such data breaches have become commonplace, as over 9,000 data breaches have been reported since 2005.[4] Victims of data breaches—and plaintiffs' litigators—have noticed, and they have turned to the courts for help, catalyzing the growth of a burgeoning new field of tort litigation.[5] More than fifty percent of the respondents in a 2019 survey of Fortune 1000 legal decisionmakers believed that data privacy and security issues represent "the next wave of class action[]" litigation, up from less than thirty percent in 2017.[6]

It was not inevitable that victims would turn to tort law as a solution to the data spill mess. Legislatures could have acted aggressively to address these issues, foreclosing the need for—or actively precluding the use of—tort litigation. They have not. While legislatures have made some limited efforts to address these issues, existing legislative initiatives have left major gaps in addressing the mass collection of data. At the same time, the judicial system has struggled to make sense of the role of tort law. Two questions have vexed many courts. First, in the absence of legislative action, is there a common law duty of care for data? For example, did UPMC have a duty to protect the trove of private employee data that it collected? Second, even if there is a duty, how can a court make sense of the concept of harm when this the duty is breached? What exactly did those UPMC employees lose?

Litigation has a way of forcing these questions, and it appears change is afoot. In the aftermath of the UPMC data breach, employees sued for relief under a common law negligence theory. Victims of the UPMC data breach argued that the Pennsylvania Supreme Court should expand the notion of duty between the employer and the employee.[7] In a landmark decision, the Pennsylvania Supreme Court obliged, holding that when an employer collects and stores employee data on its computers, it takes on "a duty to

---

[3] Second Amended Class Action Complaint ¶¶ 1–5, Dittman v. UPMC, No. GD-14-003285 (Pa. Ct. Com. Pl. June 25, 2014); *see also* Erica Teichert, *UPMC's Estimate of Data Breach Victims Skyrockets to 27k*, LAW360: EMP. AUTH. (Apr. 18, 2014, 7:12 PM), https://www.law360.com/employment-authority/articles/529625/upmc-s-estimate-of-data-breach-victims-skyrockets-to-27k (discussing the extent of the data breach).

[4] *Data Breaches*, PRIV. RTS. CLEARINGHOUSE, https://www.privacyrights.org/data-breaches (click "Download the Database") (last visited Aug. 18, 2021).

[5] *See* Sasha Romanosky, David Hoffman & Alessandro Acquisti, *Empirical Analysis of Data Breach Litigation*, 11 J. EMPIRICAL LEGAL STUD. 74, 74 (2014) (analyzing "court dockets for more than 230 federal data breach lawsuits from 2000 to 2010"). The most common causes of action in federal data breach lawsuits between 2000 and 2010 were unfair business practices, Fair Credit Reporting Act violations, breaches of contract, negligence, and Privacy Act violation claims. *Id.* at 101.

[6] CARLTON FIELDS, 2019 CARLTON FIELDS CLASS ACTION SURVEY: BEST PRACTICES IN REDUCING COST AND MANAGING RISK IN CLASS ACTION LITIGATION 13 (2019), https://classactionsurvey.com/pdf/2019-class-action-survey.pdf.

[7] *See* Dittman v. UPMC, 196 A.3d 1036, 1046 (Pa. 2018) ("[W]e agree with Employees that this case is one involving application of an existing duty to a novel factual scenario . . . .").

exercise reasonable care to protect [employees] against an unreasonable risk of harm arising out of that act."[8]

This decision, in *Dittman v. UPMC*, breaks new ground in its concrete application of duty to those collecting data. Indeed, defense attorneys have described the decision as a "landmark in state litigation" that could open "floodgates."[9] But, while it may spur a new wave of tort litigation, the story does not end there. This decision, and the broader doctrinal shifts that will likely follow, forces courts to begin addressing the second question. What exactly constitutes the "harm" that data collectors are obliged to protect data subjects against? Furthermore, what are the boundaries of those obligations to protect data? The concept of a duty to protect another is incoherent without a concept of what we are obliged to protect that person *from*. As the comments to the Restatement (Second) of Torts note, "[Duty in tort] is merely a means whereby the interest protected by the duty can be made secure."[10]

What precise interest was compromised during the UPMC data breach? Privacy interests are notoriously difficult to define or articulate.[11] Judges and scholars have produced many competing models of what privacy is, why people do or do not value it, and how privacy interests might be harmed.[12] Lacking a firm conception of what privacy is, how people benefit from privacy, and how people are harmed by privacy violations, courts have struggled in applying tort law to the unpredictable, fast-moving, and all-pervasive world of electronic data collection, with many cases foundering on the issue of whether a legally cognizable injury has occurred.[13] The U.S.

---

[8] *Id.* at 1047.

[9] *See infra* notes 65–69 and accompanying text. *See also infra* note 16.

[10] RESTATEMENT (SECOND) OF TORTS § 4 cmt. c (AM. L. INST. 1965).

[11] *See, e.g.*, Ignacio N. Cofone & Adriana Z. Robertson, *Privacy Harms*, 69 HASTINGS L.J. 1039, 1041 (2018) ("[D]espite the importance of information privacy in modern society, privacy harms are hard to pin down. This, in turn, creates challenges for information privacy law, since a clear conception of these harms is essential for determining both standing and remedies."); M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1132 (2011) ("What is a privacy harm? What makes it distinct from a burn or some other harm? We are often at a loss to say."); Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1088 (2002) ("Time and again philosophers, legal theorists, and jurists have lamented the great difficulty in reaching a satisfying conception of privacy."); Judith Jarvis Thomson, *The Right to Privacy*, 4 PHIL. & PUB. AFFS. 295, 295 (1975) ("Perhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is.").

[12] *See, e.g.*, Cofone & Robertson, *supra* note 11, at 1044–47 (discussing competing models of privacy); Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 920–21 (2005) ("[T]he American courts lack a coherent, consistent methodology for determining whether an individual has a reasonable expectation of privacy in a particular fact that has been shared with one or more persons. Indeed, jurisdictions cannot agree on a framework for resolving these kinds of cases."); Solove, *supra* note 11, at 1092 (arguing that the recurrent ideas in privacy discourse can be categorized "under six general headings"). Relatedly, the concept of what constitutes "public" information is also confused and contradictory. *See* Woodrow Hartzog, *The Public Information Fallacy*, 99 B.U. L. REV. 459, 459 (2019) (discussing incoherence in the definition of "public" information).

[13] *See, e.g.*, Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 739 (2018) ("The concept of harm stemming from a data breach has

Supreme Court's metaphor that only "concrete" injuries can support Article III standing[14] maps awkwardly, at best, to the evolving digital-era injuries caused by the transmission of electronic information.[15]

The question of how to define privacy harm has perplexed American jurists for more than one hundred years. That question has become increasingly urgent in the face of the exponential growth of tort litigation over data spills. Now, with *Dittman* establishing that employers (and likely other data collectors) have a common law duty to protect others from these ill-defined harms, the dam has broken. There will be growing pressure for other states to follow the lead of the *Dittman* Court, expanding the reach of the common law duty of care. But courts, lawyers, and the public need guidance on how to fill this significant conceptual gap, particularly as litigants seek to apply the case to new fact patterns emerging in the ever-changing information economy.[16] This is therefore a critical moment to

---

confounded the lower courts. There has been no consistent or coherent judicial approach to data-breach harms."); Margot E. Kaminski, *Standing After Snowden: Lessons on Privacy Harm from National Security Surveillance Litigation*, 66 DEPAUL L. REV. 413, 414 (2017) ("Standing to sue is one of the larger problems for both data breach and data privacy litigation. . . . Lower courts struggle with standing in data breach and data privacy cases, and have produced varied results."); Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2277 (2015) ("Contract law and tort law have not often been successfully applied to many of the issues involving the collection, storage, use, and disclosure of personal data—when courts have applied contract and tort theories to these issues, they have struggled significantly in the application. More broadly, the law has struggled to recognize privacy violations and data security breaches as harms.").

[14] Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992); *see also* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1545 (2016) (discussing harms that qualify for Article III injury-in-fact requirement).

[15] *See* Lauren Henry Scholz, *Privacy Remedies,* 94 IND. L.J. 653, 654 n.1 (2019) ("The Court's metaphor of concreteness to describe a matter sufficiently weighty to afford the attention of federal courts is hardly helpful for digital harms."); Kaminski, *supra* note 13, at 418–20 (discussing how the Supreme Court's decision in *Spokeo* has "given lower courts more fodder for dismissing privacy claims" and given rise to a "general sense of judicial skepticism over privacy injury"); Ryan Calo, *Privacy Harm Exceptionalism*, 12 COLO. TECH. L.J. 361, 361 (2014) ("[H]arm presents an especially acute challenge in the context of privacy. Courts generally demand that privacy plaintiffs show not just harm, but concrete, fundamental, or 'special' harm before they can recover.")

[16] *See, e.g.*, Matt Fair, *Pa. Ruling May Open Floodgates on Cybersecurity Suits*, LAW360 (Nov. 27, 2018, 8:44 PM), https://www.law360.com/articles/1105174 ("In the wake of the [*Dittman*] ruling, Duane Morris LLP partner Sandra Jeskie told Law360 that plaintiffs' attorneys were likely not only to start bringing a flurry of new cases on behalf of workers impacted by cyberattacks on their employers, but to also try and apply the ruling to cases involving consumers and others caught up in data breaches."); Carol Steinour Young, *Happy Thanksgiving Pennsylvania Businesses and Employers – This Year, the Pennsylvania Supreme Court Is Serving Up Increased Exposure to Liability*, JD SUPRA (Nov. 27, 2018), https://www.jdsupra.com/legalnews/happy-thanksgiving-pennsylvania-87391/ ("[I]t is likely that the Court's reasoning will be extended to other contexts where one party collects and stores another's information, such as the business-consumer context or the university-student context."); Edward McAndrew, Kristen Poetzel & Philip Yannella, *PA Supreme Court: Businesses Have Duty to Safeguard Sensitive Employee Information*, JD SUPRA (Nov. 28, 2018), https://www.jdsupra.com/legalnews/pa-supreme-court-businesses-have-duty-14177/ ("Because the court's recognition of a legal duty to protect data is tied to the very act of collecting and storing such data, this new legal principle is unlikely to be limited to the employment context."); Gary Schober, *Pennsylvania High Court Holds Employers Have an Affirmative Duty to Protect Employees' Personal Data*, JD SUPRA (Nov. 29, 2018),

consider a question of national significance—how to apply common law negligence principles in cases involving the disclosure and misuse of personal data. Courts around the country are likely to face the puzzle that *Dittman* did not solve.

We propose that a solution may lie in the conception of the "information fiduciary" developed by legal theorist Jack M. Balkin. In his article *Information Fiduciaries and the First Amendment*, Balkin sets out a framework for privacy duties based on the relationships between data collectors and data subjects, analogizing to common law information security duties owed by fiduciaries such as doctors, lawyers, and accountants.[17] In this formulation, a privacy violation, like a breach of fiduciary duty, is a violation of trust—trust that the information provided to another would not be misused.[18]

Fiduciary law has traditionally worked to enable trust in relationships characterized by imbalances of power, knowledge, and control, protecting principals from exploitation and providing them with legal mechanisms to enforce the confidence that they place in their fiduciaries.[19] With some adaptations, we believe that it can fulfill a similar role in the modern information economy. Although we depart from Balkin's analysis in certain respects, the fiduciary law's emphasis on relationships provides a useful model for understanding privacy harms in the context of common law negligence claims regarding personal data.

In Section I of this Article, we describe the general landscape of data security and privacy law in the United States and the legal system's failure to develop a coherent theory of privacy harms. Section II discusses the *Dittman* litigation, including the case's place within the broader jurisprudence of data breach litigation. Section III outlines Balkin's information fiduciary model, providing a framework to address the fundamental gap that the *Dittman* duty of care model left open. Section IV responds to some potential objections to our theory. We follow these discussions with a conclusion.

---

https://www.jdsupra.com/legalnews/pennsylvania-high-court-holds-employers-79345/ ("There should be no doubt that *all* holders of personal information will ultimately be required to implement reasonable security measures to protect personal information."); White & Williams LLP, *Five Quick Thoughts on Dittman*, JD SUPRA (Dec. 4, 2018), https://www.jdsupra.com/legalnews/five-quick-thoughts-on-dittman-85038 ("*Dittman* likely extends beyond the employment context.").

[17] Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1205–09 (2016) [hereinafter Balkin, *First Amendment*].

[18] *See id.* at 1208 ("Relationships of trust and confidence are often centrally concerned with the collection, analysis, use, and disclosure of information. . . . So, in general, the duties of a fiduciary include duties not to use information obtained in the course of the relationship in ways that harm or undermine the principal . . . .") (footnote omitted).

[19] *See id.* at 1216–17 (discussing why fiduciary law assumes that fiduciaries and principals do not stand on equal footing).

I. U.S. DATA PRIVACY AND SECURITY LAW

An overview of the current approach to privacy within the United States requires an exploration of both statutory protections and common law jurisprudence. Because of the patchworked, disjointed approach to privacy protections within statutory law, courts have turned to state tort law to fill the doctrinal gaps in privacy protections. Exploring each, in turn, will demonstrate that *Dittman* provided a novel solution to a growing challenge in technology and the law.

A. *Statutory Data Protections*

Both the federal government and the states have enacted some statutory provisions regarding data privacy, but these laws are fragmented and offer little meaningful protection to data subjects. In particular, they provide very limited recourse for individuals who suffer from data breaches.

1. *Statutory Federal Protections*

Currently, there is no all-inclusive U.S. federal data privacy law. However, there are some federal statutory protections, as well as some limited administrative guidance, for data within certain industries and for certain entities collecting data.[20] Those federal privacy protections generally fall into two categories: (1) industry-specific regulations, and (2) agency authority to direct certain privacy requirements.[21]

First, certain federal industry-specific regulations impact private sector collection of personal information. Generally, the industries that are required to take proactive measures in protecting information include healthcare, finance, childcare, and education.[22] While these statutory privacy protections do provide some mechanism to hold data collectors accountable for the data within their control, the government often has sole authority to enforce accountability for those privacy protections, and recourse for individuals is

---

[20] The U.S. government itself operates under the Privacy Act of 1974 when it collects and processes data from U.S. citizens. 5 U.S.C. § 552a. Enforced by the Office of Management and Budget, the Privacy Act requires that the U.S. government and its agencies provide transparency in data collection and incorporate privacy principles of purpose limitation and data minimization. *Id.* However, the Privacy Act only applies to data collection by the federal government, not by private entities. *Id.*

[21] While the Fourth Amendment does provide certain privacy protections at the federal level—specifically, privacy protections from the federal government—it is beyond the scope of this Article, which focuses on privacy requirements of private-sector entities.

[22] *See* Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (providing privacy standards aimed at financial institutions); Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (providing privacy standards aimed at health records); Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub. L. No. 111-5, 123 Stat. 226 (2009) (requiring notification of data breaches by entities covered under HIPAA); Family Educational Rights and Privacy Act of 1974, Pub. L. No. 93-380, 88 Stat. 571 (providing privacy standards aimed at educational records); Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681-730 (providing privacy standards aimed at children's online activity).

often limited.

For example, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Breach Notification Rule requires covered entities (i.e., hospitals, medical institutions, etc.) to provide *notice* of any breach of the security or privacy of Protected Health Information, but it does not provide a cause of action for individuals to seek redress where covered entities have disclosed their personal data and thereby exposed them to harm or the risk of harm.[23] Instead, the Office for Civil Rights (OCR) is charged with enforcing HIPAA and taking any action under the law.[24]

Second, certain federal agencies possess authority to direct privacy protections within the private sector. These agencies include the OCR, the Federal Communications Commission (FCC), and the U.S. Securities and Exchange Commission (SEC), among others.[25] One of the most prominent agencies in the enforcement of privacy protections within private industry is the Federal Trade Commission (FTC).

The FTC has derived federal privacy and security protections in commercial sectors from section 5(a)(1) of the Federal Trade Commission Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce."[26] The FTC has therefore claimed authority to ensure that companies live up to their promises related to data security and privacy. However, the FTC's approach to ensuring the enforcement of data security and privacy practices is subject to criticism. First, through the use of enforcement actions against individual companies, the FTC is creating "a 'patchwork' of data security standards" and "businesses do not have fair notice of how the FTC will apply the standards to their own practices."[27] Second, the FTC's authority is limited to companies' practices that are deemed unfair or deceptive.[28] As such, the FTC is often left to making discrete decisions about security and privacy practices, not necessarily

---

[23] 45 C.F.R. §§ 164.400–.414 (2021).

[24] *Id.*

[25] *See generally Compliant Portal Assistant*, U.S. DEP'T HEALTH & HUM. SERVS.: OFF. FOR C.R., https://ocrportal.hhs.gov/ocr/smartscreen/main.jsf (last visited Oct. 24, 2021) (providing portal for reporting violations of privacy or security of health information under HIPAA); *Privacy Act Information*, FED. COMMC'NS COMM'N, https://www.fcc.gov/managing-director/privacy-transparency/privacy-act-information (last visited Oct. 24, 2021) (providing information on how the FCC collects, uses, shares, and protects personal information); *Privacy Impact Assessments*, U.S. SEC. & EXCH. COMM'N, https://www.sec.gov/oit/privacy-impact-assessments (last visited Oct. 24, 2021) (providing information on SEC privacy impact assessments).

[26] 15 U.S.C. § 45(a)(1). The FTC's authority in this area was recognized and upheld by the Third Circuit in *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015). *See also* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 650–56 (2014) (discussing the FTC's use of settlement agreement to establish best practices for privacy policies).

[27] Robert S. Turchick, *Is the FTC Playing Fair? The Third Circuit's Decision in* FTC v. Wyndham Worldwide Corp. *Furthers Agency's Data Security Efforts but Creates Tension for Smaller Businesses*, 61 VILL. L. REV. 71, 73 (2016).

[28] *Id.* at 72 n.10.

mandating global security and privacy standards across a wide variety of business functions.

Thus, while federal law provides data protection mandates for federal government agency and private data collectors in some sectors, its coverage is limited, and it provides little meaningful recourse for individuals who have been harmed through data breaches.

2. *State Data Protection Laws*

With a lack of clear guidance at the federal level, states have stepped in to create their own legislative privacy protections. State legislators dealing with privacy issues have taken a number of approaches that can be categorized as follows: (1) general privacy legislation; (2) data-specific legislation; and (3) cyber breach legislation.

First, there is a growing focus on creating more "general" privacy legislation that governs the collection and processing of any type of personal information, regardless of the industry. The strongest example of this approach in the United States to date is the California Consumer Privacy Act of 2018 (CCPA).[29] The CCPA applies to the collection and processing of personal information of California consumers, defined as natural persons who are California residents.[30] Unlike the standard United States siloed approach to privacy, the CCPA is industry agnostic. There is, however, a threshold of revenue or amount of data that needs to be collected to trigger a business's requirement to comply with the CCPA.[31] The CCPA has changed the dialogue in the United States, with many states looking to California as an example of how to protect privacy.[32] Often, these general privacy-oriented regulations include protections for individuals, as well as mechanisms to bring a private right of action in the event of a violation.[33]

Second, in addition to these general privacy-oriented regulations, states continue to select specific types of data to protect. Currently, biometric data is the most heavily regulated data category.[34] For example, Illinois created one of the strongest biometric data protection laws—the Biometric Information Privacy Act (BIPA).[35] BIPA has provided some of the most

---

[29] CAL. CIV. CODE § 1798.100 (2021).

[30] *Id.* § 1798.140(g).

[31] *Id.* § 1798.130(c).

[32] *See, e.g.*, Assemb. 4640, 218th Leg., Reg. Sess. (N.J. 2018) (proposing requirements for certain business to notify data subjects of collection of personally identifiable information and establishing security standards); H.R. 1049, 2019 Gen. Assemb., Reg. Sess. (Pa. 2019) (proposing requirements for all businesses to provide notice to consumers on what personal information is being collected and if it will be sold, and granting consumers opt-out rights).

[33] *See, e.g.*, CAL. CIV. CODE § 1798.150 (2021) (providing a private right of action for consumers in the event of a security breach impacting their personal information).

[34] *See, e.g.*, TEX. BUS. & COM. CODE §503.001 (2021) (regulating the use of biometric identifiers); WASH. REV. CODE § 19.375 (2021) (regulating the same).

[35] 740 ILL. COMP. STAT. 14/1, /5, /10, /15, /20 /25, /99 (2021).

proactive protections in the collection and use of biometric data, with numerous court cases developing these protections.[36] Under BIPA, "biometric information" is defined as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual."[37] Any private entity, regardless of size, that collects biometric information is required to take proactive measures to protect that information, including maintaining a written policy available to the public, notifying individuals prior to any collection of biometric information, and respecting restrictions on the transfer or sale of any biometric information.[38] While BIPA only impacts one category of information, it aligns with influential frameworks like the Fair Information Practice Principles[39] in providing key requirements such as notice, transparency, purpose limitation, and data minimization.

States historically have provided protections retroactively after the unauthorized access or inadvertent misuse of personally identifiable information. Currently, all fifty states maintain data breach notification laws, each with some unique nuances and requirements.[40] Generally, these data breach notification laws are triggered when certain combinations of unencrypted data are unlawfully accessed or exfiltrated. The combination creating personally identifiable information typically includes an individual's full name plus financial information, driver's license, or other similar document.[41]

---

[36] *See, e.g.*, Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1199–200 (Ill. 2019) (allowing an action to continue under the Illinois Biometric Information Privacy Act without showing an actual injury; violation of the act alone is sufficient).

[37] 740 ILL. COMP. STAT. 14/10 (2021).

[38] *Id.* at 14/15.

[39] U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS xxiii–xxxv (1973), https://www.justice.gov/opcl/docs/rec-com-rights.pdf.

[40] *Security Breach Notification Laws*, NAT'L CONF. OF STATE LEGISLATURES (Apr. 15, 2021), https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[41] *See, e.g.*, Breach of Personal Information Notification Act, 73 PA. CONS. STAT. § 2302 (2021) (specifying that for purposes of data breach notification act, "personal information" constitutes a first or last name linked with an unencrypted Social Security number, driver's license number, or financial account number and password). Following the Equifax breach in 2017, states have begun to broaden their definitions of "personally identifiable information," recognizing that identifying information, beyond even financial information, can harm the individual. For example, in Delaware, the personally identifiable information triggering a data breach notification requirement was expanded to include (1) a username or email address in combination with a password or security question and answer that would permit access to an online account, and (2) unique biometric data generated from measurements or analyses of human body characteristics for authentication purposes. DEL. CODE tit. 6, § 12B-101(7) (2021).

The majority of these data breach notification regulations do not include an express private right of action for individuals.[42] Instead, these laws usually only require data collectors to alert data subjects when a third party has stolen their information, limiting any remedy solely to notice, with little or no monetary compensation.

B. *Common Law Privacy Protections*

Within this gap of legislative protections for privacy, and particularly with the limited recourse for individual victims, litigants and courts have looked to tort law to fill the gap. The common law offers two leading approaches to protecting privacy—first, the privacy torts, and, second, the law of negligence. However, tort law has not been an effective approach due to the conceptual limitations of the privacy torts and the difficulty of defining privacy harm in the negligence context.

In the United States, the privacy torts are often conceptualized as protecting a "right to be let alone," an idea that can be traced back to Samuel D. Warren and Louis D. Brandeis's groundbreaking 1890 article, *The Right to Privacy*.[43] Over subsequent decades, state common law evolved in the direction advocated by Warren and Brandeis, culminating in the work of the legal scholar William Prosser, who analyzed the development of privacy tort law and identified four discrete privacy torts: (1) intrusion upon seclusion; (2) public disclosure of private facts; (3) false light; and (4) appropriation.[44]

Yet, even before 1890, a number of Anglo-American legal doctrines developed to protect the distinct-but-related concept of confidentiality in contexts including evidentiary privileges, fiduciary law, government records, postal law, and telegraphy.[45] Privacy—as defined by Warren, Brandeis, and Prosser—is an individualistic concept based on the right to shield certain types of information from others; confidentiality is a relational concept based on the right to selectively disclose sensitive information without fear that it will be disseminated beyond the boundaries contemplated by the discloser-confidant relationship.[46] The implications of the two

---

[42] PRIV. RTS. CLEARINGHOUSE, DATA BREACH NOTIFICATION IN THE UNITED STATES AND TERRITORIES 128 (2018), https://privacyrights.org/sites/default/files/pdfs/Data%20Breach%20Notification%20in%20the%20United%20States%20and%20Territories.pdf.

[43] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890); *see also* ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE 94–96 (2018) [hereinafter WALDMAN, INFORMATION PRIVACY] (describing the development and adoption of the Warren-Brandeis-Prosser approach to privacy).

[44] WALDMAN, INFORMATION PRIVACY, *supra* note 43, at 94–96; *see also* Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 148–56 (2007) (discussing the historical development of the privacy torts).

[45] *See* Richards & Solove, *supra* note 44, at 134–44 (discussing the law of confidential relationships).

[46] *See id.* at 173–75 ("In contrast to Warren and Brandeis's individualistic conception of privacy, the English law of confidentiality focuses on relationships rather than individuals. Far from a right to be

doctrines are strikingly different—voluntary disclosure of information to any third person may waive a privacy interest, but not necessarily a confidentiality interest.[47]

Because the privacy torts are focused on protecting information that has never been voluntarily disclosed, whereas, in Richard A. Posner's words, "one cannot negotiate modernity without continuously revealing personal information to a variety of demanders,"[48] scholars have criticized the privacy torts as poorly suited to modern concerns and the growing data economy.[49] Existing privacy torts heavily rely on a user's expectation of privacy, that is, the concept that a user should intend for a facet of their life to remain private. The challenge under this framework is the increasingly blurred lines between private and public, especially as surveillance technology creeps further into our daily lives. This reliance on an individual user's expectation of privacy gives rise to a "privacy paradox," through which Lindsey Barrett succinctly concludes that "an individual's behavior that is less privacy-protective than their expressed preferences reveals a true preference against privacy in favor of other values, such as convenience, efficiency, or economic gain."[50] Courts are unable to truly discern a baseline level of privacy to protect when they rely on the perceived expectations of individuals who are required to use data-collecting technologies in order to engage with modern society.

With the privacy torts conceptually incapable of dealing with modern privacy concerns, negligence is currently the predominant theory under which data breach class action plaintiffs seek recovery.[51] In 2017, sixty-five percent of all federal data breach class actions alleged negligence as their primary theory of liability, and ninety-five percent of such complaints included it as a cause of action.[52] Yet, if courts cannot conceptualize privacy harms, then the law of negligence will also fail to protect data subjects from the misuse or exposure of their information. Courts are currently split on

---

let alone, confidentiality focuses on the norms of trust within relationships. Indeed, most of our personal information is known by other people, such as doctors, spouses, children, and friends, as well as institutions, such as ISPs, banks, merchants, insurance companies, phone companies, and other businesses.").

[47] *See id.* at 174–75 ("In applying the American privacy torts, many courts find that information is not private because it is shared with others or exposed in some way to the public. . . . Confidentiality stands directly at odds with the notion that when people share information with others they necessarily assume the risk of betrayal. The very purpose of confidentiality law is to recognize and enforce expectations of trust.") (footnote omitted).

[48] Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U. CHI. L. REV. 245, 249 (2008).

[49] *See, e.g.*, *supra* note 12 and accompanying text.

[50] Lindsey Barrett, *Model(ing) Privacy: Empirical Approaches to Privacy Law & Governance*, 35 SANTA CLARA HIGH TECH. L.J. 1, 13 (2018).

[51] DAVID ZETOONY, JENA VALDETERO, TAMARA KOURY & STEPHANIE DRUMM, 2017 DATA BREACH LITIGATION REPORT 6 (2017), https://www.bclplaw.com/images/content/9/6/v2/96690/Bryan-Cave-Data-Breach-Litigation-Report-2017-edition.pdf.

[52] *Id.*

whether digital breaches can create a sufficiently concrete harm to find that a plaintiff has standing to bring a case.

The cyber breach context is illustrative in demonstrating the challenge in articulating the concept of harm. Often, following a cyber breach, unless there is immediate use of personal information to cause harm to the individual, the idea of future harm is amorphous. Courts are split on whether future harm is sufficient to demonstrate a viable cause of action. The First, Second, Third, and Fourth Circuits have held that plaintiffs must allege more than the fact that their information was stolen to show an Article III injury.[53] In contrast, the Sixth, Seventh, and Ninth Circuits have held that allegations of future harm are sufficient when plaintiffs allege that their data has been stolen and is in the hands of ill-intentioned criminals.[54] However, without an express statutory right to bring a lawsuit, individuals are finding it hard, if not impossible, in the current legal frameworks, to demonstrate harm sufficient to hold private actors accountable for misuse or negligent handling of personal information under tort theories of liability.

The articulation of harm directly impacts the finding of a duty by collectors of data. Courts have weighed in on this concept, but a comprehensive approach still remains elusive. For example, in *Sackin v. TransPerfect Global, Inc.*, the U.S. District Court for the Southern District of New York addressed a breach of an employer's information systems resulting in the exposure of employee information.[55] The court found that the employees had stated a viable negligence claim against their employer because "employers have a duty to take reasonable precautions to protect the [personally identifiable information] that they require from employees."[56]

Further, in *In re Sony Gaming Networks & Customer Data Security Breach Litigation*, the U.S. District Court for the Southern District of California addressed the existence of a duty in the consumer context.[57]

---

[53] *See* Whalen v. Michaels Stores, Inc., 689 F. App'x 89, 91 (2d Cir. 2017) (holding that theft of credit card information, risk of future identity fraud, and time and money expended in resolving attempted fraudulent charges did not constitute injury sufficient for standing purposes); *see also*, *e.g.*, Beck v. McDonald, 848 F.3d 262, 274 (4th Cir. 2017) (holding that increased future risk of identify fraud did not constitute injury sufficient for standing purposes); Katz v. Pershing, LLC, 672 F.3d 64, 80 (1st Cir. 2012) (holding the same); Reilly v. Ceridian Corp., 664 F.3d 38, 40, 44 (3d Cir. 2011) (holding the same).

[54] *See, e.g.*, Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 388 (6th Cir. 2016) ("Plaintiff's allegations of a substantial risk of harm, coupled with reasonably incurred mitigation costs, are sufficient to establish a cognizable Article III injury at the pleading stage of the litigation."); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) (holding that standing existed because "[a]t this stage in the litigation, it is plausible to infer that the plaintiffs have shown a substantial risk of harm from the Neiman Marcus data breach"); Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (finding standing where "Plaintiffs-Appellants have alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data").

[55] 278 F. Supp. 3d 739, 748 (S.D.N.Y. 2017).

[56] *Id.*

[57] 996 F. Supp. 2d 942, 966 (S.D. Cal. 2014).

There, the court found a legal duty existed within the contract between the two parties that was "well supported by both common sense and California and Massachusetts law."[58] However, the court rejected a finding of a common law duty, explaining that "Plaintiffs have failed to allege a 'special relationship' with Sony beyond those envisioned in everyday consumer transactions, and therefore, negligence is the wrong legal theory on which to pursue recovery for Plaintiffs' economic losses."[59]

In *Cooney v. Chicago Public Schools*, the Illinois Appellate Court declined to recognize a common law duty under Illinois law because the Illinois data breach notification statute did not provide for statutory liability.[60] The plaintiffs attempted to draw a duty sufficient to support their negligence claim from existing statutory law.[61] However, because those statutes only provided for notice as a remedy for a breach of personal information, the court rejected any claim that a duty to safeguard personal information existed,[62] highlighting the challenge of using tort theories to fill gaps in statutory protections.

As an additional example, in *Attias v. CareFirst, Inc.*, the U.S. District Court for the District of Columbia held that no common law duty to safeguard private information existed in the plaintiffs' relationship with a health insurer.[63] The court held that all of the duties alleged by the plaintiffs were asserted under a contract between the parties, and no independent tort duty outside of that contract existed between the parties, barring the plaintiffs' tort claims.[64]

These cases articulate the challenge and divergence in current case law in providing a workable framework to address liability in the collection and processing of personal data.

II. NEGLIGENCE LAW INTO THE BREACH

With both state and federal statutory law offering fragmented, limited protections for data subjects, and the privacy torts being largely non-responsive to modern privacy concerns, there is a gap in the legal landscape leaving much of our data unprotected. This is where the *Dittman* decision and its recognition of a duty to protect third-party data could come into play. As the first state supreme court decision to squarely recognize a

---

[58] *Id.*
[59] *Id.* at 969.
[60] 943 N.E.2d 23, 28–29 (Ill. App. Ct. 2010).
[61] *Id.*
[62] *Id.*
[63] 365 F. Supp. 3d 1, 20 (D.D.C. 2019).
[64] *Id.* at 18.

tort duty to protect personal data,[65] commentators have described *Dittman* as a "landmark in state litigation over data breaches";[66] as a decision that "drastically changed the data breach litigation landscape";[67] as "[o]pen[ing] [the] floodgates" to employee and consumer privacy lawsuits;[68] and as a precedent which "all employers should be cognizant of when developing their data security strategy."[69] This Section explores *Dittman* and its reasoning in depth, particularly exploring its undeveloped theory of harm, which may provide both redress for victims of data breaches and an avenue for litigation based on data practices well beyond the cybersecurity failures that are now so familiar to litigants and courts.[70]

A. *Data Collection: Subject to a Common Law Duty of Care*

Dittman was a purported class action lawsuit brought on behalf of UPMC employees regarding a data breach alleged to have compromised the personal and financial information of more than 62,000 people, including their names, addresses, Social Security numbers, and dates of birth.[71] Plaintiffs brought claims for negligence and breach of contract.[72] They alleged that UPMC failed to take reasonable and appropriate measures to safeguard the personal data that it required them to provide as a condition of employment, thereby causing the employees to incur damages relating to fraudulently filed tax returns and placing them at an increased risk of identity theft.[73]

The trial court granted UPMC's motion to dismiss in May 2015.[74] The

---

[65] The Georgia Supreme Court has also held that data collectors have a duty of care with regard to personal data. *See* Collins v. Athens Orthopedic Clinic, P.A., 837 S.E.2d 310, 316 (Ga. 2019) (holding that allegations that personal data was stolen on a mass scale by a criminal, who offered it for sale to other criminals and created risk of identity theft, were sufficient to allege a cognizable injury). *See also In re* Hannaford Bros. Co. Customer Data Sec. Breach Litig., 4 A.3d 492, 498 (Me. 2010) (holding that, in the absence of physical harm, economic loss, or identity theft, data theft did not constitute a cognizable harm).

[66] Alexander R. Bilus & Patrick Hromisin, *Pennsylvania Supreme Court Recognizes Employers' Duty to Safeguard Employees' Personal Data*, SAUL EWING ARNSTEIN & LEHR LLP (Dec. 5, 2018), https://www.saul.com/publications/alerts/pennsylvania-supreme-court-recognizes-employers%E2%80%99-duty-safeguard-employees%E2%80%99-personal-data.

[67] Philip N. Yannella, *PA Supreme Court: Businesses Have Duty to Safeguard Sensitive Employee Information*, BALLARD SPAHR (Nov. 27, 2018), https://www.ballardspahr.com/insights/alerts-and-articles/2018/11/pa-supreme-court-businesses-have-duty-to-safeguard-sensitive-employee-info.

[68] Fair, *supra* note 16.

[69] *Pennsylvania High Court Holds Employers Have an Affirmative Duty to Protect Employees' Personal Data*, HODGSON RUSS LLP (Nov. 28, 2018), https://www.hodgsonruss.com/newsroom-publications-10710.html.

[70] *See generally* Romanosky et al., *supra* note 5 (analyzing "court dockets for more than 230 federal data breach lawsuits from 2000 to 2010").

[71] Dittman v. UPMC, No. GD-14-003285, 2015 WL 13779479, at *1 (Pa. Ct. Com. Pl. May 28, 2015), *aff'd*, 154 A.3d 318 (Pa. Super. Ct. 2017), *vacated*, 196 A.3d 1036 (Pa. 2018).

[72] *Id.* at *1, *5.

[73] *Id.*

[74] *Id.* at *6.

trial court held that plaintiffs' negligence claim was barred by the economic loss doctrine, which it interpreted as providing that "no cause of action exists for negligence that results solely in economic losses" without physical harm or destruction of property.[75] The court also declined to recognize a negligence cause of action.[76] In a split opinion, a three-judge panel of the Superior Court of Pennsylvania likewise held that UPMC did not owe a duty of reasonable care in its collection and storage of employee data and that, even if a duty did exist, the economic loss doctrine would bar plaintiffs' claims.[77] On appeal, the Pennsylvania Supreme Court reversed.[78] Unlike the lower courts, which approached the case through the doctrinal rubric used when Pennsylvania courts consider the creation of a new cause of action,[79] the Supreme Court considered the case as fitting into a traditional negligence framework—the application of an already-existing duty of care to a novel set of facts, rather than the creation of an entirely new duty.[80] Applying the negligence principle that a person assumes a duty of care where their affirmative actions have created a risk of harm, the Court held that the act of collecting and storing employee data on a computer system gives rise to a duty on the part of the data collector, requiring the exercise of reasonable care to protect the data subjects against an unreasonable risk of harm arising out of its actions.[81]

Regarding the economic loss doctrine, the Court held that, where a duty arises independently of any contractual duties between the parties, the economic loss doctrine will not bar a tort action.[82] As such, the Court further held that the plaintiffs' claims were not barred because UPMC's duty to safeguard its employees' data existed independently of any contractual relationship between them.[83]

Dittman is by no means the only court decision examining the issue of whether a duty of care to protect personal data exists. Some courts have found, like *Dittman*, that a duty to provide reasonable data security exists under tort law, rooted in principles such as the foreseeability of harm and the need to exercise reasonable care when engaging in affirmative conduct.[84]

---

[75] *Id.* at *2.

[76] *Id.* at *4–5.

[77] Dittman v. UPMC, 154 A.3d 318, 322–26 (Pa. Super. Ct. 2017).

[78] Dittman v. UPMC, 196 A.3d 1036, 1056 (Pa. 2018).

[79] *Dittman*, 2015 WL 13779479, at *3–4; *Dittman*, 154 A.3d at 322–23.

[80] *Dittman*, 196 A.3d at 1046.

[81] *Id.* at 1046–48.

[82] *Id.* at 1054 ("[I]f the duty arises under a contract between the parties, a tort action will not lie from a breach of that duty. However, if the duty arises independently of any contractual duties between the parties, then a breach of that duty may support a tort action.").

[83] *Id.* at 1056.

[84] *See, e.g.*, Sackin v. TransPerfect Glob., Inc., 278 F. Supp. 3d 739, 748 (S.D.N.Y. 2017) (stating that "employers have a duty to take reasonable precautions to protect the [personally identifiable information] that they require from employees"); *In re* Sony Gaming Networks & Customer Data Sec.

On the other hand, some courts have held that there is no duty in tort to care for personal data.[85] Those courts have often stressed the importance of the relationship between the data custodian and the data subject in determining whether a duty of care exists.[86] However, to our knowledge, *Dittman* is the first decision by a state supreme court expressly holding that data collectors have a duty of care to protect data subjects from harm. Therefore, the decision presents a useful opportunity for all jurisdictions considering this issue to evaluate the pros, cons, and complexities of a duty to care for data.

B. *The New Challenge: What Is the Harm Data Collectors Must Take Care to Protect?*

Although *Dittman* held that data collectors must take reasonable steps to protect data subjects against harm, the court did not explore the question of what constitutes "harm" in the data privacy context. Perhaps because some of the *Dittman* plaintiffs alleged that they had suffered tax fraud as a result of the data breach,[87] unlike other data breach plaintiffs alleging only

---

Breach Litig., 996 F. Supp. 2d 942, 966 (S.D. Cal. 2014) ("Although neither party provided the Court with case law to support or reject the existence of a legal duty to safeguard a consumer's confidential information entrusted to a commercial entity, the Court finds the legal duty well supported by both common sense and California and Massachusetts law."); Witriol v. LexisNexis Grp., No. C05-02392 MJJ, 2006 WL 4725713, at *8 (N.D. Cal. Feb. 10, 2006) (holding that the plaintiff sufficiently alleged that the custodian of the plaintiff's personal information owed a duty of care to prevent access by unauthorized third parties); *In re* Home Depot, Inc., Customer Data Sec. Breach Litig., No. 1:14-md-2583-TWT, 2016 WL 2897520, at *3–4 (N.D. Ga. May 18, 2016) (holding that a duty to safeguard information existed based on the foreseeability of harm); Daly v. Metro. Life Ins. Co., 782 N.Y.S.2d 530, 535 (N.Y. Sup. Ct. 2004) ("[T]his court is convinced that Met Life had a duty to protect the confidential personal information provided by the plaintiffs. When Ms. Daly wished to purchase a life insurance policy from Met Life, she was required to, and agreed to, supply Met Life with highly sensitive personal information . . . . Implicit in this agreement was a covenant to safeguard this information.").

[85] *See, e.g.*, Attias v. CareFirst, Inc., 365 F. Supp. 3d 1, 20–21 (D.D.C. 2019) (holding that the plaintiffs' relationship with the health insurer did not give rise to either a common law duty to safeguard private information or a fiduciary duty, such that negligence and breach of the duty of confidentiality were not avenues on which the plaintiffs could recover for a data breach); Cooney v. Chi. Pub. Schs., 943 N.E.2d 23, 28–29 (Ill. App. Ct. 2010) (declining to recognize a common law duty under Illinois law where the state data breach notification statute did not provide for liability).

[86] *See, e.g.*, Attias, 365 F. Supp. 3d at 23 (examining the relationship between insurers and insureds to determine if a duty of data care exists); Top Trade v. Grocery Outlet, No. 2:17-cv-08467-SVW-MRW, 2018 WL 6038297, at *3–4 (C.D. Cal. May 9, 2018) (finding a duty of care based on the foreseeability of harm and the plaintiff-defendant relationship); Veridian Credit Union v. Eddie Bauer, LLC, 295 F. Supp. 3d 1140, 1158 (W.D. Wash. 2017) (holding that "[b]ecause Eddie Bauer can only be held liable for its alleged omissions or nonfeasance in the context of a 'special relationship,' . . . the court concludes that Eddie Bauer does not owe a duty to Veridian based on common law principles of negligence").

[87] Dittman v. UPMC, 196 A.3d 1036, 1038–39 (Pa. 2018) ("Employees further alleged that the stolen data, which consisted of information UPMC required Employees to provide as a condition of their employment, was used to file fraudulent tax returns on behalf of the victimized Employees, resulting in actual damages."). *See also* Second Amended Class Action Complaint ¶¶ 1–5, Dittman v. UPMC, No. GD-14-003285 (Pa. Ct. Com. Pl. June 25, 2014) (alleging that as a result of UPMC's failure to protect data, "the personal and financial information of Plaintiffs and the members of the proposed Classes was used, inter alia, to file fraudulent tax returns").

heightened risk,[88] the court did not see a need to delve into the difficult, philosophically challenging inquiry of what distinguishes a data-driven harm from business as usual in the twenty-first century, thus leaving the matter open for further litigation. This judicial modesty is wholly consistent with the philosophy that courts should limit their holdings to the facts of the cases before them, such that the common law will evolve to fit new social circumstances through its gradual application to newly emerging facts.[89] Yet it also means that any court attempting to apply *Dittman*'s negligence framework in the field of data privacy will face as-yet-unresolved questions and challenges about what "harm" really means.

For example, in the realm of social media, it seems plain that collecting and storing the personal data of millions (or billions) of users on a networked computer system would be considered "affirmative conduct," thus giving rise to risks under *Dittman*, and that social media companies owe their users a duty to exercise reasonable care to protect them against unreasonable risks of harm arising out of that conduct.[90] But what does it mean for Facebook to protect its users from an unreasonable risk of harm arising from its collection of data? At a baseline level, the existence of a duty of care mandates that Facebook must take reasonable measures to prevent cyber-criminals from stealing data.[91] This is straightforward enough, aside from the ever-shifting question of what constitutes reasonable cybersecurity.[92] More interesting

---

[88] *See, e.g.*, Beck v. McDonald, 848 F.3d 262, 273–74 (4th Cir. 2017) (discussing a federal circuit split over whether a plaintiff may establish an Article III injury-in-fact based on an increased risk of identity theft, and holding that plaintiffs' allegations "of an enhanced risk of future identity theft" were too speculative to support standing).

[89] *See* Maloney v. Valley Med. Facilities, Inc., 984 A.2d 478, 490 (Pa. 2009) ("For very good reasons, our decisional law generally develops incrementally, within the confines of the circumstances of cases as they come before the Court. For one thing, it is very difficult for courts to determine the range of factual circumstances to which a particular rule should apply in light of the often myriad possibilities."); Scampone v. Highland Park Care Ctr., LLC, 57 A.3d 582, 599 (Pa. 2012) ("Like any other cause of action at common law, negligence evolves through either directly applicable decisional law or by analogy, meaning that a defendant is not categorically exempt from liability simply because appellate decisional law has not specifically addressed a theory of liability in a particular context."); *see also* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 408–09 (2013) (describing the law of standing as being built on separation-of-power principles that prevent the judicial branch from usurping the powers of the political branches).

[90] *See Dittman*, 196 A.3d at 1047 ("Thus, we agree with Employees that, in collecting and storing Employees' data on its computer systems, UPMC owed Employees a duty to exercise reasonable care to protect them against an unreasonable risk of harm arising out of that act.").

[91] *See id.* at 1048 (holding that UPMC possessed a duty to protect its employees' personal and financial information from breach by criminal third parties).

[92] *See generally* William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1139 (2019) (discussing fourteen frameworks for data security); Scott J. Shackelford, Andrew A. Proia, Brenton Martell & Amanda N. Craig, *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 305, 311–26 (2015) (reviewing existing U.S. law shaping a cybersecurity duty of care); Solove & Hartzog, *supra* note 26, at 650–56 (discussing the FTC's data security jurisprudence).

problems emerge when we consider negligence fact patterns emerging principally from Facebook's own actions, rather than from the criminal acts of third parties, involving financial, emotional, and dignitary injuries distinct from the risk of identity theft. Were Facebook's users harmed when the company's failure to control third-party app developers allowed Cambridge Analytica to gather information about them—including details on their user identities, friend networks, likes, and possibly even private messages—for use in an election-influence campaign?[93] Were users harmed when Facebook stored millions of Instagram passwords in a readable format, giving staff unfettered access to accounts?[94] Is a user harmed if Facebook alerts her family to her pregnancy by targeting her with baby-themed advertising,[95] or if it ruins the surprise of a marriage proposal by publicly revealing that a user recently purchased a diamond ring?[96] Is a user harmed if he is fired from his job after malfunctioning privacy settings show his employer offensive postings that he only meant to share with a small group of friends?[97] These are difficult legal questions, and we cannot answer them without a coherent theory of privacy harm.

Data brokers also affirmatively gather vast quantities of information about individuals, thereby potentially taking on a duty of care under the

---

[93] *See* Matthew Rosenberg, Nicholas Confessore & Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html (discussing the Cambridge Analytica data-harvesting scandal); 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/ (reporting that Facebook security gaps allowed an app to read private messages between 1,500 Facebook users and their contacts).

[94] *See* Zak Doffman, *U.S. Authorities Target Zuckerberg as Facebook 'Buries' Huge Instagram Password Breach*, FORBES (Apr. 19, 2019, 2:53 AM), https://www.forbes.com/sites/zakdoffman/2019/04/19/u-s-authorities-target-zuckerberg-as-instagram-security-breach-hits-millions/#2a2370ac5062 (discussing an instance in which millions of Instagram passwords were internally stored in a readable format); *Keeping Passwords Secure*, FACEBOOK: NEWSROOM, https://newsroom.fb.com/news/2019/03/keeping-passwords-secure./ (Apr. 18, 2019, 10:00 AM) (discussing the same).

[95] *See* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG. (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp (reporting on companies' usage of data analytics to profile consumers); Cotton Delo, *Does Facebook Know You're Pregnant?; What It Knows Depends on Whom You Ask: Social Network Says One Thing, Its Advertisers Another*, ADVERT. AGE (Sept. 10, 2012), https://adage.com/article/digital/facebook-pregnant/237073 (reporting the same); *see also* Theodore Rostow, *What Happens When an Acquaintance Buys Your Data?: A New Privacy Harm in the Age of Data Brokers*, 34 YALE J. REGUL. 667, 686 (2017) ("Marketers will pay $0.11 to know that a woman is pregnant and in her second trimester.").

[96] *See 5 Data Breaches: From Embarrassing to Deadly*, CNN MONEY, https://money.cnn.com/galleries/2010/technology/1012/gallery.5_data_breaches/3.html (Dec. 14, 2010, 1:03 PM) (discussing data breach incidents, including an incident in which a Facebook user found that the details of his engagement ring purchase were publicly posted).

[97] *See* Sheera Frenkel, *Facebook Bug Changed Privacy Settings of Up to 14 Million Users*, N.Y. TIMES (June 7, 2018), https://www.nytimes.com/2018/06/07/technology/facebook-privacy-bug.html (discussing incident in which as many as fourteen million Facebook users who thought they were creating private posts were, in fact, making public posts that anyone could view).

doctrine developed in *Dittman*.[98] Data brokers collect billions of data elements covering nearly every U.S. consumer, obtaining information from businesses, government records, and other publicly available sources,[99] largely without consumers' knowledge.[100] They also derive inferences from the collected data (for example, inferring that an individual who recently applied for a mortgage may be interested in furniture sales and home repair products), then resell this data for marketing products, risk mitigation products, and people search products, including analytic products designed to predict consumer preferences.[101] Data brokers may or may not offer consumers the ability to access the information about them or to correct errors in their databases.[102] The FTC has found that, although consumers benefit from many data brokerage activities, data brokerage also poses risks, such as the risk of being forbidden services on account of opaque algorithms or consumer segmenting.[103] If a person is denied an affordable loan because a data broker's algorithms have characterized him as a credit risk due to false information or racial bias, should that be considered a harm implicating a duty of care?[104] What about if a people search company helps a domestic abuser find and kill his ex-wife? [105]

Many industries affirmatively collect information that could conceivably implicate a duty of care. Brick-and-mortar retail firms use big data analytics in each step of their businesses;[106] Walmart alone processes 2.5 petabytes of data every hour from over 200 internal and external

---

[98] *See generally* FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (2014) (discussing results of an FTC in-depth study of nine data brokers).

[99] Some of the sources from which data brokers collect information include: (1) U.S. Census records; (2) the Social Security Administration's Death Master File; (3) U.S. Postal Service records; (4) criminal records; (5) court and bankruptcy filings; (6) professional licensure databases; (7) real property and assessor records; (8) voter registration information; (9) motor vehicle and driving records; (10) birth, marriage, divorce, and death records; (11) blogs and social media; (12) retail websites; (13) financial services companies; (14) marketing surveys; (15) telephone companies; and (16) other data brokers. *Id.* at 11–14.

[100] *Id.* at iv.

[101] *Id.* at ii–iii.

[102] *Id.* at iii.

[103] *Id.* at v.

[104] *See id.* at 48 (noting risks that consumers may be denied services as a result of data brokerage).

[105] *See id.* at 48–49 (noting risks that data brokerage may enable harassment, stalking, and other harms).

[106] Bernard Marr, *Big Data: A Game Changer in the Retail Sector*, FORBES (Nov. 10, 2015, 1:34 AM), https://www.forbes.com/sites/bernardmarr/2015/11/10/big-data-a-game-changer-in-the-retail-sector/#758d957b9f37; *see also* Rory Van Loo, *Helping Buyers Beware: The Need for Supervision of Big Retail*, 163 U. PA. L. REV. 1311, 1331 (2015) ("In recent years, firms have invested hundreds of millions of dollars to build information technologies that enable them to collect and mine data from billions of transactions—online and offline, loyalty card and otherwise. . . . They film consumers' in-store movements and install cameras that track the movement of consumers' eyes as they walk down the aisles. Marketers combine these various data sources with the literature on decisionmaking to generate hypotheses about pricing practices that are then tested in stores.") (footnotes omitted).

streams.[107] In the legal field, the two leading legal research platforms are components of sprawling data brokerage conglomerates that, amongst other things, sell surveillance data to Immigrations and Customs Enforcement, raising ethical concerns about whether attorneys are entrusting sensitive information to entities hostile to their clients' interests.[108] Even companies that sell beds,[109] children's toys,[110] and household appliances[111] now surveil their users, such that, "[t]he regulatory challenge of the early twenty-first century is the toaster that betrays you."[112]

The surveillance economy[113] offers an almost limitless number of fact patterns in which data subjects might be injured, degraded, or aggrieved without data breaches or identity theft.[114] In addition to the psychological anxieties and self-censorship that may arise from constant monitoring,[115] modern data collection practices and technologies may expose data subjects

---

[107] Bernard Marr, *Really Big Data at Walmart: Real-Time Insights From Their 40+ Petabyte Data Cloud*, FORBES (Jan. 23, 2017, 2:06 AM), https://www.forbes.com/sites/bernardmarr/2017/01/23/really-big-data-at-walmart-real-time-insights-from-their-40-petabyte-data-cloud/#7525357b6c10.

[108] *See generally* Sarah Lamdan, *When Westlaw Fuels ICE Surveillance: Legal Ethics in the Era of Big Data Policing*, 43 N.Y.U. REV. L. & SOC. CHANGE 255 (2019) (discussing partnerships between U.S. Immigrations and Customs Enforcement and legal research companies).

[109] *See* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 235–36 (2019) (discussing the privacy implications of the Sleep Number smart bed).

[110] Donell Holloway & Lelia Green, *The Internet of Toys*, COMMC'N RSCH. & PRAC. 506, 506–07 (2016) ("The emerging risks of Internet-connected toys to children and families include corporate and government surveillance of children's activities and encroachments upon their data privacy and security . . . . Other risks include hacked surveillance of Internet-connected toys, geo-locational tracking of children and remote control of toys' various recording and 'speaking' technologies by others."); Kate Fazzini, *Toys and Apps Often Track Your Kids and Collect Information About Them—Here's How to Keep Them Safe*, CNBC, https://www.cnbc.com/2018/11/23/connected-toys-privacy-risks.html (Nov. 26, 2018, 11:29 AM).

[111] *See* David C. Vladeck, *Consumer Protection in an Era of Big Data Analytics*, 42 OHIO N.U. L. REV. 493, 500–01 (2016) (discussing privacy implications of products and technologies like the Amazon Echo, Apple's Siri, and others).

[112] Jack M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. DAVIS L. REV. 1149, 1169 (2018) [hereinafter Balkin, *Algorithmic Society*].

[113] *See generally* ZUBOFF, *supra* note 109 (discussing the role of surveillance and data monetization in the modern economy).

[114] *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 477–78 (2006) [hereinafter Solove, *Taxonomy*] (attempting to create a taxonomy of privacy harms); Rostow, *supra* note 95, at 671–72 (discussing privacy harms that flow from the collection, aggregation, use, and dissemination of digital information).

[115] S*ee* Solove, *Taxonomy*, *supra* note 114, at 493 ("Not only can direct awareness of surveillance make a person feel extremely uncomfortable, but it can also cause that person to alter her behavior. Surveillance can lead to self-censorship and inhibition. Because of its inhibitory effects, surveillance is a tool of social control, enhancing the power of social norms, which work more effectively when people are being observed by others in the community.").

to discrimination,[116] consumer manipulation,[117] voter manipulation,[118] manipulation by persons within one's social networks,[119] blackmail,[120] wage theft,[121] stalking,[122] and harassment.[123] What does a duty to protect others from harm mean in such an environment?

One possible answer to this problem would be to rely on the analytic framework of the Prosserian common law privacy torts—intrusion upon seclusion, appropriation of name or likeness, publicity given to private life, and publicity placing a person in false light[124]—to determine whether an individual has been harmed by the collection of data. This is similar to the

---

[116] *See* Vladeck, *supra* note 111, at 513 ("The process of engaging in algorithmic decision-making is one that is opaque and complex, and can effectively mask discrimination. . . . But regulators will have a hard time uncovering discrimination when the decision is made by machine-learning algorithms that process mounds of data.") (footnotes omitted); Amy J. Schmitz, *Secret Consumer Scores and Segmentations: Separating "Haves" from "Have-Nots"*, 2014 MICH. ST. L. REV. 1411, 1415–16 (discussing how consumer segmentation using brokered data may augment power imbalances by making better deals available to consumers with greater social capital and further explaining that "scores and segmentations that factor in race, gender, and other suspect considerations may foster discrimination"); Nate Cullerton, *Behavioral Credit Scoring*, 101 GEO. L.J. 807, 820 (2013) ("Digital profiles have profound real-world effects, determining access to and pricing for credit, insurance, and consumer products in ways that entrench existing disadvantages of class and race.").

[117] *See* Ryan Calo & Alex Rosenblat, *The Taking Economy: Uber, Information, and Power*, 117 COLUM. L. REV. 1623, 1650–51 (2017) (discussing digital market manipulation as a method for firms to identify and exploit consumer cognitive biases); Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 999 (2014) ("A specific set of emerging technologies and techniques will empower corporations to discover and exploit the limits of each individual consumer's ability to pursue his or her own self-interest. Firms will increasingly be able to trigger irrationality or vulnerability in consumers . . . .").

[118] *See* Jonathan Zittrain, *Engineering an Election*, 127 HARV. L. REV. F. 335, 336–37 (2014) (discussing the potential of digital information platforms to swing election results via selective dissemination of news).

[119] *See* Rostow, *supra* note 95, at 673 ("When data brokers sell consumer data to individuals, they allow buyers to learn about the behavior and motivations of those whose data they purchase. These insights allow the buyers to influence the decisions of those around them, leading to potential harms unrecognized by privacy scholarship to date.").

[120] *See* Jonah Engel Bromwich, *Ashley Madison Users Face Threats of Blackmail and Identity Theft*, N.Y. TIMES (Aug. 27, 2015), https://www.nytimes.com/2015/08/28/technology/ashley-madison-users-face-threats-of-blackmail-and-identity-theft.html?searchResultPosition=1 (reporting on blackmail threats against users of dating website intended to facilitate affairs); Ariana Eunjung Cha, *Charlie Sheen's HIV Status and the Dawn of Medical-Data Blackmail*, WASH. POST (Nov. 17, 2015) (reporting on attempt to blackmail actor Charlie Sheen for $10 million by people who threatened to reveal his HIV test results).

[121] *See* Joelle Gamble, *The Inequalities of Workplace Surveillance*, NATION (June 3, 2019), https://www.thenation.com/article/worker-surveillance-big-data/ (discussing the use of data technology to surveil workers and alter workplace dynamics).

[122] *See* Jennifer Valentino-DeVries, *Hundreds of Apps Can Empower Stalkers to Track Their Victims*, N.Y. TIMES (May 19, 2018), https://www.nytimes.com/2018/05/19/technology/phone-apps-stalking.html (reporting on consumer apps that can be used to surveil domestic partners); Symposium, *The Spyware Used in Intimate Partner Violence*, INST. OF ELEC. & ELECS. ENG'RS COMPUT. SOC'Y 441, 441 (2018) (reporting the same).

[123] Valentino-DeVries, *supra* note 122.

[124] *See* RESTATEMENT (SECOND) OF TORTS §§ 652A–E (AM. L. INST. 1997) (providing the Restatement definitions of the common law privacy torts).

approach that Facebook has advocated for in the Cambridge Analytica multidistrict litigation, where it argued that courts should look to the common law privacy torts to determine whether intangible privacy harms qualify as concrete for purposes of Article III standing.[125]

However, as many legal scholars have argued, the common law privacy torts are ill-equipped to recognize harms flowing from the misuse of electronic data.[126] Because the governing theory of common law privacy torts is that privacy is a right to keep people out—based on individual rights, rather than on social relationships[127]—they are not well-suited to address problems flowing from the misuse of information which we have already voluntarily shared or been made to share.[128] Furthermore, the concepts of private space and seclusion are central to the privacy torts and incoherent in the realm of cyberspace.[129] As Lauren Henry Scholz has written:

---

[125] *See* Memorandum of Law in Support of Motion of Defendant Facebook, Inc. to Dismiss Plaintiffs' First Amended Consolidated Complaint at 10–15, *In re* Facebook, Inc. Consumer Priv. User Profile Litig., No. 3:18-MD-02843-VC (N.D. Cal. Mar. 15, 2019) (arguing that the court should refer to the common law privacy torts in Article III standing analysis). *But cf.* Matthew S. DeLuca, Note, *The Hunt for Privacy Harms After* Spokeo, 86 FORDHAM L. REV. 2439, 2466–67 (2018) (arguing that the law of Article III standing does not restrict courts to the framework of the privacy torts).

[126] *See, e.g.*, Scholz, *supra* note 15, at 668 (criticizing the "cramped nature of the privacy torts"); Alicia Solow-Niederman, *Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches*, 127 YALE L.J.F. 614, 621–22 (2018) (noting that the privacy torts' "focus on the actual public exposure and dissemination of private information is a poor analytic fit for data breaches"); WALDMAN, INFORMATION PRIVACY, *supra* note 43, at 94–96 (discussing the historic development of the privacy torts and their limitations based on the "governing theory that the right to privacy was a tool to keep others out"); Samantha Barbas, *Saving Privacy From History*, 61 DEPAUL L. REV. 973, 973–74 (2012) ("As many have convincingly argued, tort privacy is especially inadequate to address the needs of the twenty-first century, when new technologies magnify privacy injuries."); Richards & Solove, *supra* note 44, at 155 ("[T]he privacy torts have struggled when addressing emerging privacy problems in the Information Age, such as the collection, use, and disclosure of personal data by businesses."); Patricia Sánchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARV. J.L. & TECH. 1, 4 (2007) ("The Restatement (Second) of Torts, which reflects the general state of privacy tort law in the United States, has been a poor guide and is now outdated.") (footnotes omitted); Sarah Ludington, *Reining in the Data Traders: A Tort for the Misuse of Personal Information*, 66 MD. L. REV. 140, 159 (2006) ("To suggest that the existing scheme of privacy torts would be an effective tool for addressing the complex problems of personal information abuse is akin to suggesting that one could use a toy drill to fix a nuclear reactor.").

[127] *See* Richards & Solove, *supra* note 44, at 173–74 (discussing how conceptions of privacy in American law "are defined in very individualistic terms," and contrasting with confidentiality, which "focuses on the norms of trust within relationships")

[128] *Id.* at 175–76 (discussing doctrinal reasons why the American privacy torts "have often struggled when applied to the disclosure of personal data by businesses"); *see also* Strahilevitz, *supra* note 12, at 920–21 ("Despite the centrality of this issue, the American courts lack a coherent, consistent methodology for determining whether an individual has a reasonable expectation of privacy in a particular fact that has been shared with one or more persons. Indeed, jurisdictions cannot agree on a framework for resolving these kinds of cases.").

[129] *See* Abril, *supra* note 126, at 18–20 (discussing how the traditional privacy torts rely on privacy as a function of location, with actions within a bedroom being entitled to greater privacy protection than actions in the town square, but that this spatial analysis breaks down in cyberspace).

> The Prosserian approach to the worry that privacy plaintiffs would bring too many general claims into court was to consciously cabin the right into highly specific fact patterns. . . . When problems are framed highly specifically, they struggle to apply effectively to newly possible infringements created by technosocial developments.[130]

In any case, from the number and scope of breaches[131] and the continued persistence of poor security practices,[132] it seems fair to say that existing legal doctrines have not effectively deterred the negligent handling of personal information.[133]

Another answer to this problem might be to cabin *Dittman*'s definition of "harm" such that only injuries to person or property are actionable, and some courts considering allegations of privacy harm have done just so.[134] However, this trend is at tension with other threads of the common law of torts, which have long acknowledged that violations of privacy interests, relational interests, interests in self-determination, and other intangible interests may, in some instances, form the basis for a tort action, even if such violations do not result in physical or pecuniary injuries.[135] For example, under the common law tort of invasion of privacy, damages are awarded to compensate the plaintiff for harm to dignity, and a victim may be entitled to general damages, special damages, punitive damages, and injunctive

---

[130] Scholz, *supra* note 15, at 668 (footnotes omitted); *see also* Richards & Solove, *supra* note 44, at 148–56 (discussing Prosser's influence in limiting the scope of privacy law).

[131] *See Data Breaches*, PRIV. RTS. CLEARINGHOUSE, https://www.privacyrights.org/data-breaches (last visited Aug. 13, 2021) (providing a database of publicly-reported data breaches).

[132] *See, e.g.*, David W. Opderbeck, *Cybersecurity, Data Breaches, and the Economic Loss Doctrine in the Payment Card Industry*, 75 MD. L. REV. 935, 981 (2016) ("Much of the economic literature suggests that the persistent incidence of large scale data breaches demonstrates that network externalities or other market failures have led to an underinvestment in security."); Jacob W. Schneider, Note, *Preventing Data Breaches: Alternative Approaches to Deter Negligent Handling of Consumer Data*, 15 B.U. J. SCI. & TECH. L. 279, 299 (2009) ("A prominent security company has claimed that [seventy-seven percent] of its clients are insecure when consultation begins and as many as [seventy-five percent] of all online retailers are vulnerable.") (footnotes omitted).

[133] Opderbeck*, supra* note 132, at 983; Schneider*, supra* note 132, at 282.

[134] *See, e.g.*, Fed. Aviation Admin. v. Cooper, 566 U.S. 284, 304 (2012) (holding, as a matter of statutory interpretation, that the Privacy Act of 1974 does not authorize damages for emotional distress); Duqum v. Scottrade, Inc., No. 4:15-CV-1537-SPM, 2016 WL 3683001, at *8 (E.D. Mo. July 12, 2016) ("Courts have held that loss of privacy and breach of confidentiality are too abstract to establish Article III standing."); Khan v. Child.'s Nat'l Health Sys., 188 F. Supp. 3d 524, 533 (D. Md. 2016) (citing *In re* Zappos.com, Inc., Customer Data Sec. Breach Litig., 108 F. Supp. 3d 949, 962 n.5 (D. Nev. 2015) (holding that the loss of privacy arising from a data breach was not a "concrete and particularized injury" and therefore did not give rise to damages).

[135] *See* Nancy Levit, *Ethereal Torts*, 61 GEO. WASH. L. REV. 136, 140–58 (1992) (discussing the evolution of tort law to compensate for harms other than direct and tangible injuries to persons or property, including harms to privacy, emotions, relational interests, and self-determination interests, as well as lost chances and increased risks); Solove & Citron, *supra* note 13, at 756–74 (discussing judicial recognition of claims for damages based on risk and anxiety).

relief.[136] Similarly, in a suit regarding the publication of private information, damages include harm to the plaintiff's privacy interests, mental distress of a kind normally resulting from an invasion, and special damages caused by the invasion.[137] Even if the common law privacy torts do not represent a viable framework for resolving modern data injuries,[138] the fact that the law has historically recognized claims for redress based on factors other than out-of-pocket consequential damages[139] suggests that restricting the modern definition of data-driven "harm" to solely pocketbook injuries would represent an ahistorical breach with the past, as well as a judicial abdication of the traditional responsibility to protect individuals from the affirmative acts of others.[140]

III. INFORMATION FIDUCIARY THEORY AS A RUBRIC FOR UNDERSTANDING THE DUTY OF CARE

This Article proposes that the information fiduciary concept developed by Jack M. Balkin[141] and expounded on by other scholars[142] can fill

---

[136] *See* 5 Damages in Tort Actions § 44.02 (2019) (Matthew Bender) (discussing elements of invasion of privacy claims).

[137] *Id.* § 44.03.

[138] *See supra* note 126 and accompanying text (discussing shortcomings of common law privacy torts).

[139] *See* Solove & Citron, *supra* note 13, at 771 ("In case after case involving the privacy torts and breach-of-confidentiality tort, courts have recognized harm based on pure emotional distress or psychological impairment. Fear, anxiety, embarrassment, and loss of trust are all recognized as harms. Humiliation, nervousness, worry, and loss of sleep are understood as compensable harms.") (footnotes omitted).

[140] For a discussion of damages, *see infra* Section III.C.

[141] *See, e.g.*, Balkin, *First Amendment*, *supra* note 17, at 1185–87 (discussing the information fiduciary concept); Jack M. Balkin, *Free Speech Is a Triangle*, 118 COLUM. L. REV. 2011, 2048 (2012) [hereinafter Balkin, *Triangle*] (arguing that companies "that create and maintain . . . relations of digital dependence and vulnerability should be considered *information fiduciaries* toward their end users.") (emphasis in original); Balkin, *Algorithmic Society*, *supra* note 112, at 1160–62 (discussing the information fiduciary concept). Professor Kenneth Laudon appears to have coined the phrase in the early 1990s. *See* Kenneth C. Laudon, *Markets and Privacy*, in ICIS 1993 Proceedings 65, 70–71 (1993).

[142] *See, e.g.*, Ariel Dobkin, *Information Fiduciaries in Practice: Data Privacy and User Expectations*, 33 BERKELEY TECH. L.J. 1, 10–12 (2018) (proposing four main principles of (1) anti-manipulation, (2) antidiscrimination, (3) limited sharing with third parties, and (4) compliance with privacy policies as touchstones for determining user expectations for information fiduciaries); Ari Ezra Waldman, *Designing Without Privacy*, 55 HOUS. L. REV. 659, 665 n.20 (2018) [hereinafter Waldman, *Designing*] ("Many scholars, including Jack Balkin, Jonathan Zittrain, Dan Solove, Danielle Citron, and others, have recommended a shift toward a fiduciary or trustee model to ensure corporations take consumer privacy seriously."); Solow-Niederman, *supra* note 126, at 625 (arguing that holders of consumer data in commercial transactions should be considered "data confidants" with a duty to securely maintain the information); Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 457–58 (2016) [hereinafter Richards & Hartzog, *Taking Trust Seriously*] (arguing that the information fiduciary concept can help rejuvenate privacy law and policy by introducing notions of trust); Jane R. Bambauer, *The Relationships Between Speech and Conduct*, 49 U.C. DAVIS L. REV. 1941, 1943–44 (2016) (discussing implications of information fiduciary theory for free speech jurisprudence); Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies*

Dittman's gap by creating a theory of privacy harm based on a framework of "privacy as trust," rather than "privacy as secrecy," in which courts determine whether data practices should be considered "harms" principally by looking to the relationships between data collectors and data subjects and the expectations of the parties.

A. *Information Fiduciary Theory*

Information fiduciary theory is a conception of privacy rights centered on the idea that certain kinds of information represent matters of private concern that the government may regulate consistent with the First Amendment based, not upon their content, but upon the social relationships that produce them.[143] The law has long recognized that professionals, such as doctors, lawyers, and accountants, have a duty to exercise appropriate care with information related to their clients, as such professionals occupy a special relationship of trust and confidence with their clients.[144] Balkin argues that the digital age "has given rise to new fiduciary relationships created by the explosion of the collection and use of personal data" and that the law should recognize such relationships "for the same reason that the law recognized older forms of fiduciary duties in the past."[145] Due to the difficulties that principals face in monitoring fiduciaries and the potential for fiduciaries to dominate or exploit their principals, the common law has traditionally imposed a duty of confidentiality, requiring fiduciaries to keep their principals' information secure,[146] and a duty of loyalty, requiring fiduciaries to act in good faith and put their principals' interests ahead of their own.[147] Balkin argues that companies collecting digital information

---

Trustworthy, ATLANTIC (Oct. 3, 2016), http://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/ (proposing a "grand bargain" in which tech companies that agree to user-protective standards and practices would be exempted from compliance with a range of state and local laws); Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611, 649–50 (2015) (arguing that the information fiduciary concept can be used to reform Fourth Amendment jurisprudence that no longer reflects modern privacy concerns); Zittrain, *supra* note 118, at 339–40 (discussing information fiduciary theory as a potential solution to "digital gerrymandering" in which firms use control over consumer information to influence elections); Danielle Citron, *Big Data Brokers as Fiduciaries*, CONCURRING OPS. (June 19, 2012), https://perma.cc/8DV4-TUXQ (discussing the potential of information fiduciary theory to regulate data brokers).

[143] *See* Balkin, *First Amendment*, *supra* note 17, at 1209–20 (discussing how fiduciary law framework has allowed courts to limit speech by professionals such as lawyers or doctors without violating the First Amendment).

[144] *See id.* at 1205–07 (discussing fiduciary duties traditionally owed by professionals); *see also* ABA Comm. on Ethics & Pro. Resp., Formal Op. 477 (2017) (providing guidance on securing the communication of protected client information); ABA Comm. on Ethics & Pro. Resp., Formal Op. 483 (2018) (providing guidance on lawyers' obligations after an electronic data breach or cyberattack).

[145] Balkin, *First Amendment*, *supra* note 17, at 1221.

[146] *See* TAMAR FRANKEL, FIDUCIARY LAW 20–22 (2011) (discussing the duty of security).

[147] *See id.* at 106–07 (discussing the duty of loyalty); *see also* Deborah A. DeMott, *Beyond Metaphor: An Analysis of Fiduciary Obligation*, 1988 DUKE L.J. 879, 882 (discussing the same).

should owe similar duties to their end users: a duty of care and confidentiality, meaning that companies must keep end users' data confidential and secure, and a duty of loyalty, meaning that companies must not betray end users' trust or otherwise manipulate them.[148] Together with Jonathan Zittrain, Balkin has proposed a Digital Millennium Privacy Act, offering digital media companies a "grand bargain" wherein the federal government would provide a safe harbor preempting state privacy regulations for companies that agree to a set of information practices along these lines.[149]

Fiduciary law provides a model for the legal governance of power relationships that can be adapted to diverse circumstances.[150] Anglo-American courts have applied the fiduciary framework in areas of law including agency, bankruptcy, charities and nonprofits, corporations, employment, family relationships, guardianship, health, investment banking, legal representation, partnerships, pensions, and trusts.[151] According to Evan J. Criddle, "[c]ourts have eschewed formalistic criteria for identifying fiduciary relations and instead reason by analogy to paradigmatic relations such as trust, partnership, and agency."[152] Furthermore, although fiduciary duties are often referred to in moralizing tones as duties of "the finest loyalty. . . . stricter than the morals of the market place,"[153] the law recognizes limited or quasi-fiduciary duties in instances where one party has greater access to information and/or the opportunity to dominate another, but the relationship between the parties is not such where a full fiduciary obligation, including the duty to put the principal's interests above those of the fiduciary, would be warranted.[154] Some examples of

---

[148] Balkin, *Triangle*, *supra* note 141, at 2051–53.

[149] *See* Balkin & Zittrain, *supra* note 142 ("The DMPA would provide a predictable level of federal immunity for those companies willing to subscribe to the duties of an information fiduciary and accept a corresponding process to redress privacy and security violations. . . . [T]hose who accept the deal would gain the consistency and calculability of a single set of nationwide rules.").

[150] *See* Evan J. Criddle, *Fiduciary Foundations of Administrative Law*, 54 UCLA. L. REV. 117, 125 (2006) [hereinafter Criddle, *Fiduciary Foundations*] (discussing the historical genesis and development of the fiduciary concept); DeMott, *supra* note 147, at 880–81 ("The term 'fiduciary' itself was adopted to apply to situations falling short of 'trusts,' but in which one person was nonetheless obliged to act *like* a trustee. . . . The evolution of fiduciary obligation thus owed much to the situation-specificity and flexibility that were Equity's hallmarks.") (footnotes omitted).

[151] *See* Evan J. Criddle, *Liberty in Loyalty: A Republican Theory of Fiduciary Law*, 95 TEX. L. REV. 993, 994 n.1 (2017) [hereinafter Criddle, *Liberty*] (providing examples of different areas of the law in which fiduciary duties arise).

[152] Criddle, *Fiduciary Foundations*, *supra* note 150, at 125; *see also* FRANKEL, *supra* note 146, at 2 ("One reason for the paucity of a general definition of fiduciary relationships may be the many situations and contexts in which these relationships appear. That could make the courts' generalization difficult or even impossible.").

[153] Meinhard v. Salmon, 164 N.E. 545, 546 (N.Y. 1928).

[154] *See* Robert A. Prentice, *Permanently Reviving the Temporary Insider*, 36 J. CORP. L. 343, 374–76 (2011) (listing quasi-fiduciary duties often recognized by common law or statute).

quasi-fiduciary duties include a majority shareholder's quasi-fiduciary duty to minority shareholders,[155] a carrier's quasi-fiduciary duty to shippers,[156] and a trusted employee's quasi-fiduciary duty not to reveal trade secrets.[157]

One of the main goals of information fiduciary theory is to shift the focus of privacy debates from arguments about regulating *information* to protect privacy interests to arguments about regulating *relationships* to protect privacy interests.[158] Another virtue of information fiduciary theory is that it draws upon a mature area of law that has traditionally been used to safeguard vulnerable parties in relationships that are characterized by imbalances of knowledge and power.[159] Scholars have widely applauded Balkin's work as an innovative and appealing approach to modern privacy problems,[160] attracting interest from lawmakers of both parties at the federal level,[161] with a group of Democratic senators having introduced legislation to impose duties of care, loyalty, and confidentiality on online service providers.[162]

One of the drawbacks of information fiduciary theory is that it is difficult to adopt a legal framework largely, but not entirely, designed to govern professional services into the strikingly different realm of electronic data collection, even though they both implicate core concerns of power,

---

[155] *See* Ferber v. Am. Lamp Corp., 469 A.2d 1046, 1050 (Pa. 1983) (recognizing a quasi-fiduciary duty owed by majority shareholders).

[156] *See In re* Penn Cent. Transp. Co., 351 F. Supp. 1348, 1350 (E.D. Pa. 1972) (recognizing a quasi-fiduciary duty owed by carriers).

[157] *See* Safeway Transp., Inc. v. W. Chambers Transp., Inc., 100 F. Supp. 2d 442, 445 (S.D. Tex. 2000) (recognizing a quasi-fiduciary duty owed with respect to trade secrets); *see also* Prentice, *supra* note 154, at 374–76 (listing quasi-fiduciary duties often recognized by common law or statute).

[158] *See* Balkin, *First Amendment*, *supra* note 17, at 1187 ("My goal, in other words, is to shift the focus of First Amendment arguments about privacy from the kinds of *information* to the kinds of *relationships*—relationships of trust and confidence—that governments may regulate in the interests of privacy."); *see also, e.g.*, WALDMAN, INFORMATION PRIVACY, *supra* note 43, at 40 (arguing that the central goal of privacy is to "maintain different sorts of social relationships with different people," not to keep information hidden from all others).

[159] *See* Calo & Rosenblat, *supra* note 117, at 1689 (arguing that one of the advantages of information fiduciary theory is that "it imports a relatively mature area of law" in an area that "is premised upon information and power asymmetries").

[160] *See, e.g.*, Dobkin, *supra* note 142, at 7 ("Conceiving of service providers as 'information fiduciaries' may be the way to balance freedom of speech with data privacy, while still allowing service providers to grow and innovate."); Rostow, *supra* note 95, at 705 (praising Balkin's proposal as protecting consumers from digital abuse while still "accommodating a digital environment that places highly sensitive information in the hands of a diverse array of commercial entities"); Calo & Rosenblat, *supra* note 117, at 1688–89 (discussing the advantages of the information fiduciary approach); Richards & Hartzog, *Taking Trust Seriously*, *supra* note 142, at 458 ("We agree with Balkin and Solove that the concept of fiduciaries helpfully reorients privacy and crystallizes the concept of trust in information relationships."). *But see generally* Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497 (2019) (criticizing information fiduciary theory on various grounds).

[161] *See* Khan & Pozen, *supra* note 160, at 500 (discussing legislative proposals inspired by information fiduciary theory).

[162] Data Care Act of 2018, S. 3744, 115th Cong. (2018).

vulnerability, and trust.[163] Balkin himself acknowledges that consumer expectations of many modern data collectors are very different from consumer expectations of professionals and other traditional fiduciaries, such that standards that are appropriate to protect doctor-patient relationships are not necessarily appropriate to protect employer-employee, store-customer, or Facebook-user relationships.[164]

For example, some of the leading data collectors, including Facebook and Google, have adopted the business model of offering digital services in exchange for personal data, rather than for cash payments— thereby evoking the frequently-repeated mantra, "If you are not paying for the product, you are the product."[165] Consequently, adopting a lawyerly standard of fiduciary loyalty that flatly prohibits fiduciaries from profiting on the personal information of their clients would wreak havoc on the economic foundations of the Internet.[166] Lina Khan and David Pozen suggest that imposing a duty of loyalty for data collection will lead to an insurmountable conflict in which data collectors will be torn between loyalty to shareholders and loyalty to data subjects.[167] Other scholars have criticized the information fiduciary framework as being too limited in scope to offer meaningful protection since so many major data collectors cannot be considered to be in relationships of trust with data subjects,[168] and courts have resisted the application of fiduciary responsibilities to data custodians.[169]

---

[163] *See* Balkin, *Triangle*, *supra* note 141, at 2049 (discussing differences between the business models of tech companies and traditional fiduciaries like doctors and lawyers).

[164] *See id.* ("[W]e should expect that [tech companies] will not have all of the same obligations as doctors and lawyers."); Balkin, *First Amendment*, *supra* note 17, at 1225–26 ("Fiduciary duties or duties of confidentiality for doctors and lawyers are often quite broad and strong; they may be greater than we would reasonably expect of online service providers and related digital enterprises.")

[165] *See generally* Will Oremus, *Are You Really the Product?*, SLATE (Apr. 27, 2018, 5:55 AM), https://slate.com/technology/2018/04/are-you-really-facebooks-product-the-history-of-a-dangerous-idea.html (discussing the genesis and history of the "you are the product" aphorism).

[166] Balkin, *First Amendment*, *supra* note 17, at 1227.

[167] *See* Khan & Pozen, *supra* note 160, at 508–10 (arguing that it may be impractical for corporate boards and executives to manage cross-cutting fiduciary obligations to data subjects and shareholders).

[168] *See, e.g.*, Rostow, *supra* note 95, at 699 (criticizing the information fiduciary framework as not being designed to protect data subjects from indirect abuses from persons other than the companies that initially collect their data); Bambauer, *supra* note 142, at 1950–51 (arguing that Balkin's formulation of an information fiduciary is too narrow to contain Amazon, Netflix, and most other web services).

[169] *See, e.g.*, Cmty. Bank of Trenton v. Schnuck Mkts., Inc., 887 F.3d 803, 818 (7th Cir. 2018) (finding no fiduciary relationship between a grocery store and banks issuing payment cards); Attias v. CareFirst, Inc., 365 F. Supp. 3d 1, 20–21 (D.D.C. 2019) (finding no fiduciary relationship between data subjects and a health insurer); Fero v. Excellus Health Plan, Inc., 236 F. Supp. 3d 735, 774 (W.D.N.Y. 2017) (finding no fiduciary relationship between data subjects and a health insurer); *In re* Premera Blue Cross Customer Data Sec. Breach Litig., 198 F. Supp. 3d 1183, 1202–03 (D. Or. 2016) (finding no fiduciary relationship between data subjects and a health insurer); Anderson v. Hannaford Bros., 659 F.3d 151, 157–58 (1st Cir. 2011) (finding no fiduciary relationship between grocery customers and a store regarding payment card data).

However, as Woodrow Hartzog and Neil Richards have written,

> [T]he law need not face the binary choice of treating information relationships as either "fiduciary" or "unprotected." Surely some middle ground exists between these two extremes. Accordingly, we recommend that duties inspired by fiduciary law can apply in a flexible and variable way across the full spectrum of information relationships.[170]

We agree. Like Hartzog and Richards, we propose that courts can employ fiduciary concepts to define the common law duties owed by data collectors without imposing "the highest duty implied by law"[171] upon them or requiring them to act "with the utmost good faith in furthering and advancing" [172] data subjects' interests.

B. *Using Information Fiduciary Theory to Fill the Conceptual Gap*

We return to the crucial question about the nature of "harm." When the Pennsylvania Supreme Court held that UPMC owed its employees "a duty to exercise reasonable care to protect them against an unreasonable risk of harm,"[173] what did the word "harm" encompass?

We propose that the affirmative act of collecting personally identifiable data forms a relationship between the data collector and the data subject whereby the data subject is made vulnerable to the data collector, which has the ability to exploit asymmetries of power and knowledge inherent to the relationship or which may allow those asymmetries to be exploited by others by failing to secure the data.[174] *Thus, the affirmative act of collecting personally identifiable data gives rise to a quasi-fiduciary relationship, such that data subjects suffer harm if the collected data are exploited in ways that are inconsistent with the reasonable expectations of the parties and the intended scope of the relationship*.[175] Revisiting the language of *Dittman*, we might say that, "in collecting and storing Employees' data on its computer systems, UPMC owed Employees a duty to exercise reasonable care to protect them against an unreasonable risk of harm arising out of that act."[176] The

---

[170] *See* Richards & Hartzog, *Taking Trust Seriously*, *supra* note 142, at 458 (discussing the use of information fiduciary concepts to emphasize the importance of trust in privacy law).

[171] Yenchi v. Ameriprise Fin., Inc., 161 A.3d 811, 819 (Pa. 2017).

[172] *Id.* at 820.

[173] Dittman v. UPMC, 196 A.3d 1036, 1047 (Pa. 2018).

[174] *See* Balkin, *Algorithmic Society*, *supra* note 112, at 1157–58 ("[T]he actual practices of collecting, analyzing, and using Big Data for governance and control involve relationships of power between people. . . . [T]echnology is actually a way of exemplifying and constituting relationships of power between one set of human beings and another set of human beings.").

[175] Note that the data collector has the option of severing this relationship at any time by deleting its information about the data subject (although, of course, deletion would not cure any harms that the data subject had already suffered from breaches or other causes).

[176] *Dittman*, 196 A.3d at 1047.

relationship between the parties is the locus of any prospective harm—that is, if a person is "harmed" for *Dittman* purposes, it is because their expectations of the relationship were violated. In Ariel Dobkin's formulation, "[W]hat separates an acceptable practice from an unacceptable one is users' expectations: if a service provider is using data in a way that reasonable users would not expect, the service provider may have violated its duty."[177]

But how can courts determine the boundaries of these information relationships to determine whether they have been violated? This is where fiduciary law comes into play as a body of law that is concerned with relationships involving inevitable asymmetries of knowledge and power,[178] the transfer and safeguarding of sensitive information,[179] and the need to protect vulnerable parties from domination.[180] In particular, the fiduciary duties of confidentiality and loyalty provide helpful guidance for conceptualizing the rights and responsibilities of persons within an information relationship.

The duty of confidentiality means that data collectors must keep the data that they obtain confidential and secure against unauthorized access and that they must take reasonable precautions to ensure that anyone whom they grant authorized access abides by the same restrictions that they do.[181] This is not a duty of absolute secrecy but, rather, a duty to maintain sensitive information within reasonable contextual boundaries. After all, even a professional subject to strong fiduciary duties of confidentiality, such as an attorney, may disclose information protected by the attorney-client privilege

---

[177] Dobkin, *supra* note 142, at 17; *see also* Balkin, *Triangle*, *supra* note 141, at 2049 ("What constitutes a breach of trust depends on the nature of their business, and this, in turn, depends on what consumers would reasonably consider unexpected or abusive for digital companies to do.").

[178] *See* Dobkin, *supra* note 142, at 10 ("[Fiduciary] relationships have a common dynamic: there is an information asymmetry, so both parties know that the person with less information will trust or rely on the person with more information. To manage this dependency, the law imposes a special duty on the person with more information to ensure that she does not take advantage of the asymmetry."); Balkin, *First Amendment*, *supra* note 17, at 1227 ("[O]nline service providers present the familiar problems that generally give rise to fiduciary obligations. First, there are significant asymmetries of knowledge and information between online service providers and end-users. Second, it is very difficult for end-users to verify online companies' representations about data collection, security, use, and dissemination. Third, it is very difficult for end-users to understand what online companies do with their data and how data analysis and use affects their interests. Fourth, even if end-users understood these information practices, it would be almost impossible for end-users to monitor them.").

[179] *See* FRANKEL, *supra* note 146, at 20–22 (discussing fiduciary relationships created by the entrustment of sensitive information); Richards & Solove, *supra* note 44, at 173–75 (discussing the law of fiduciaries and confidential relations).

[180] *See* Criddle, *Liberty*, *supra* note 151, at 997 (arguing that the primary purpose of private fiduciary law is to prevent fiduciaries from dominating their beneficiaries).

[181] *See* Balkin, *Triangle*, *supra* note 141, at 2051–52 (arguing that under a duty of confidentiality, social media companies would be required to ensure that anyone who shares or uses their data is equally trustworthy and legally bound by the same requirements that they are).

where ethical requirements demand it to prevent harm to third parties;[182] where a dispute has arisen between the attorney and client;[183] or with third parties, like paralegals and expert witnesses, who are supervised by the attorney.[184] Likewise, UPMC had a duty to keep its employees' tax information confidential as against the public,[185] but not against payroll processors or tax authorities. Note that both of these scenarios contemplate situations in which the data collector may disclose information to others without the data subject's consent, even though doing so would harm the data subject's material interests. For example, a client could suffer severe penalties if their lawyer reveals that the client has perjured himself, and an employee of UPMC might prefer to be paid under the table, rather than to have her employer inform tax authorities about her salary. Nonetheless, we would not say that disclosure inflicts a legally cognizable harm in either case. This illustrates why consent and material interests are not firm foundations to base a "harm" analysis upon.

The duty of loyalty means that data collectors must use information in a manner that is consistent with data subjects' reasonable expectations and their own business models.[186] They may not "act like con artists" or "induce trust in their end users to obtain personal information from them and then turn around and betray that trust by harming and manipulating them for the company's own benefit."[187] Using UPMC as an example, having collected its employees' information for tax and employment purposes, it would breach the duty of loyalty for UPMC to sell that data to marketing firms, as that is unrelated to the purpose for which UPMC solicited the data. It would not, however, represent a breach of the duty of loyalty if Google were to sell information about customers' search histories to advertisers since doing so is consistent with Google's business model and user expectations. Firms with attenuated relationships to data subjects, such as third-party data brokers, may have no duty of loyalty at all; the data subjects never willingly provided their

---

[182] *See* MODEL RULES OF PRO. CONDUCT r. 1.6(b)(1)–(4) (AM. BAR ASS'N 2019) (setting out rules for the confidentiality of information within the client-lawyer relationship).

[183] *See id.* r. 1.6(b)(5) ("A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary . . . to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and a client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client . . . .").

[184] *See* RONALD D. ROTUNDA & JOHN S. DZIENKOWSKI, LEGAL ETHICS: THE LAWYER'S DESKBOOK ON PROFESSIONAL RESPONSIBILITY § 1.6-7(b) (2021–2022 ed.) (discussing the relationship between client confidentiality and paraprofessionals under the lawyer's control).

[185] *See* Dittman v. UPMC, 196 A.3d 1036, 1047 (Pa. 2018) (concluding that the defendant owed a duty to exercise reasonable care in collecting and storing their personal and financial information on its computer systems).

[186] *See* Balkin, *Triangle*, *supra* note 141, at 2053 ("The duties of information fiduciaries depend in part on what is reasonable to expect from them given their business models.").

[187] *Id.*

information to the firms, and they have no reasonable expectation that the data will be used in a way that is consistent with their interests.

In most cases, we expect that data subjects have a baseline expectation of data security—that anyone gathering sensitive information about them will take reasonable precautions to prevent the data from being stolen by criminals. Thus, in the run-of-the-mill data breach case such as *Dittman*, proving that reasonable data subject expectations were violated will not be difficult. However, plaintiffs proceeding on other theories of harm will need to provide proof of what a reasonable person would have expected in the context of their relationship to the data collector. Any assessment of data subject expectations should be based on an objective, "reasonable person" standard, *not* on the subjective expectations of the plaintiffs. There are two reasons for this. *First*, using such a standard will prevent data collectors from being held liable for violating expectations that are unreasonable, idiosyncratic, or unknowable. *Second*, and more importantly, a standard that looks to subjective expectations will not be amenable to class certification and therefore will not be a realistic means for protecting data subjects' rights.[188] Some forms of evidence that have been used to show the expectations of the hypothetical "ordinary consumer" in the product liability context include seller representations, circumstantial evidence, industry customs and standards, statutes and regulations, expert testimony, and survey data.[189]

It is also worth noting that this would represent a duty of care, not a strict liability standard. Consider a hypothetical employer who used reasonable cybersecurity to protect employee data but suffered a network breach at the hands of a particularly sophisticated intruder who used a zero-day exploit that no existing security measures could shield against.[190] Its employees would suffer harm from the breach since the hack violated their expectation of confidentiality. But the employer would not be liable to its employees under a tort theory since it satisfied its duty of care. Similarly, consider a rogue Human Resources employee who downloads names and photographs of co-workers from a company database, then posts them on an internet forum dedicated to mocking unattractive people. The affected employees would be harmed insofar as their expectation of loyalty was violated, but the

---

[188] *See infra* Section IV.C.

[189] *See* Jerry J. Phillips, *Consumer Expectations*, 53 S.C. L. REV. 1047, 1061–63 (2002) (discussing methods for proving the existence and content of consumer expectations); *see also* Tincher v. Omega Flex, Inc., 104 A.3d 328, 387 (Pa. 2014) ("The nature of the product, the identity of the user, the product's intended use and intended user, and any express or implied representations by a manufacturer or other seller are among considerations relevant to assessing the reasonable consumer's expectations.").

[190] A zero-day exploit is a cyberattack that occurs on the first day that a weakness is publicly discovered in software, before the program's creators have had the opportunity to develop a security patch. *See What Is a Zero-Day Attack? – Definition and Explanation*, KASPERSKY, https://usa.kaspersky.com/resource-center/definitions/zero-day-exploit (last visited Oct. 18, 2021).

employer itself would not be liable, provided that it had satisfied its duty of care by taking reasonable precautions to ensure that the data would only be used for intended, employment-related purposes.[191]

C. *Remedies*

If we conceive of privacy harm as a breach of trust, what does that imply for damages? How is a court or jury supposed to put a dollar value on, for example, an employee's trust that their employer will exercise due care with their Social Security number? Again, fiduciary law can come into play to help answer these questions. One of the reasons why fiduciary theory represents an attractive model for assessing privacy harm is because fiduciary law's framework of flexible, equitable remedies can recognize injuries and offer redress, even where the victim has not suffered an out-of-pocket loss.[192] Courts have imposed a number of different remedies for breaches of fiduciary duty, including compensatory damages, restitution, punitive damages, and injunctive relief,[193] each of which we briefly discuss below.

1. *Compensatory Damages*

As set forth in the Restatement (Second) of Torts, "[o]ne standing in a fiduciary relation with another is subject to liability to the other for harm resulting from a breach of duty imposed by the relation."[194] In data breach cases where plaintiffs seek recovery from the inadvertent disclosure of private information, awards representing the costs of identity theft, credit monitoring, and emotional distress would likely represent the standard measure of compensatory damages.[195] But courts have generally been skeptical of such claims in data breach litigation, holding that they are too

---

[191] Whether the rogue HR employee might be held liable is a separate question that revolves around whether the duty of care owed by UPMC would also run towards UPMC's employees—an interesting and important question beyond the scope of this Article.

[192] *See* DeMott, *supra* note 147, at 888 ("The general goal of contract damages, in short, is to compensate the plaintiff for loss of an expected advantage. The law of fiduciary obligation calculates damages from a very different perspective. That perspective dictates that the plaintiff is entitled to recover specific restitution of any benefit that the defendant obtained through his breach or, if specific restitution is not feasible, money damages that quantify the defendant's benefit. Even if the fiduciary's actions have not injured the beneficiary, and even if the beneficiary has in some sense gained as a result of the fiduciary's act, the fiduciary must account to the beneficiary for its profits.") (footnotes omitted).

[193] *See* RESTATEMENT (THIRD) OF AGENCY § 8.01 cmt. (d)(1) (AM. L. INST. 2006) (discussing remedies for breach of fiduciary duties).

[194] RESTATEMENT (SECOND) OF TORTS § 874 (AM. L. INST. 1979). *See also* RESTATEMENT (THIRD) OF TRUSTS § 100 cmt. (e) (AM. L. INST. 2012) ("A trustee who commits a breach of trust is liable for a loss resulting from the breach."); *In re* Lampe, 665 F.3d 506, 517 (3d Cir. 2011) ("Under Pennsylvania law, a director is liable to the corporation for breaching his duty of care for 'losses which were proximately caused by the negligent and wasteful conduct' at issue.").

[195] *See* Romanosky et al., *supra* note 5, at 83–84 (noting that the typical elements of damages claimed in data breach lawsuits include actual losses from identity theft, credit monitoring costs, emotional distress, and anticipated future losses).

speculative or remote to support standing.[196] However, at a minimum, the *Dittman* approach supports the notion that claims relating to identity theft remediation and an "increased and imminent risk" of identity theft[197] constitute cognizable economic damages.[198]

2. *Restitution*

Where a fiduciary has committed a breach of duty, the principal may elect the restitutionary remedy of forcing the fiduciary to disgorge any profits that it accrued through the breach—thus imposing a constructive trust to prevent unjust enrichment.[199] Such disgorgement-based remedies encourage loyalty and transparency by deterring fiduciaries from taking advantage of their position of trust, even when they can do so without inflicting an obvious loss upon the principal.[200] Restitutionary remedy theories are appealing in the privacy context because they directly address the economic incentives that motivate data collectors to misuse personal information.[201] Although restitution will be inapposite in most data breach cases since data collectors are not enriched by the actions of criminal hackers, it will represent the most intuitive remedy in scenarios where data collectors violate the trust of data subjects for commercial gain. It is, however, worth noting that, in most instances, restitutionary remedies will be fairly modest on an individual level. For example, Facebook's worldwide average revenue per user was $24.96 in 2018,[202] and marketers can buy access to information regarding the certain prescription drugs that an individual takes for as little as $0.26.[203]

---

[196] *See* Solove & Citron, *supra* note 13, at 749–52 (discussing judicial skepticism towards theories of data-breach harm).

[197] Dittman v. UPMC, 196 A.3d 1036, 1039 (Pa. 2018).

[198] *See id.* at 1048 (characterizing the plaintiffs as claiming "purely economic damages").

[199] *See* RESTATEMENT (THIRD) OF RESTITUTION AND UNJUST ENRICHMENT § 43 (AM. L. INST. 2011) ("A person who obtains a benefit (a) in breach of a fiduciary duty [or] (b) in breach of an equivalent duty imposed by a relation of trust and confidence . . . is liable in restitution to the person to whom the duty is owed."); RESTATEMENT (THIRD) OF TRUSTS § 100 cmt. c (AM. L. INST. 2012) ("A trustee who commits a breach of trust normally is not allowed to benefit individually from the breach, and the trustee is subject to liability to eliminate any such benefit."); *see also* Robert H. Sitkoff, *The Economic Structure of Fiduciary Law*, 91 B.U. L. REV. 1039, 1048 (2011) ("In the event of the fiduciary's breach of duty, the principal is entitled to an election among remedies that include compensatory damages to offset any losses or to makeup any gains forgone owing to the fiduciary's beach, or to disgorgement by the fiduciary of any profit accruing to the fiduciary owing to the breach."); *In re Lampe*, 665 F.3d at 519–20 (noting that Pennsylvania courts often use the concept of unjust enrichment as a measure of liability for breach of fiduciary duty).

[200] Sitkoff, *supra* note 199, at 1048–49; DeMott, *supra* note 147, at 888.

[201] *See* Scholz, *supra* note 15, at 677–78 ("[T]he principal motivation for the law's action here is the wrongful profit and the incentives that it creates for businesses, not what it means for the aggrieved party to possess what has been taken.").

[202] Facebook, Inc., Annual Report (Form 10-K) 39 (2019).

[203] Rostow, *supra* note 95, at 686–87.

3. *Punitive Damages*

Punitive damages may be available for especially malicious, reckless, or oppressive breaches of fiduciary duties.[204] Punitive damages could serve an important deterrent function, especially in instances where compensatory or restitutionary remedies are insufficient because companies have egregiously breached their users' trust without imposing out-of-pocket injuries on their users or earning significant profits for themselves.

4. *Injunctions*

Finally, injunctive relief has traditionally been available in cases for breach of fiduciary duty.[205] The Pennsylvania Supreme Court has held that a preliminary injunction was appropriate to prevent the potential compromise of confidential information by a law firm[206] and that, even in the absence of an express agreement, employers are entitled to equitable protection against the misuse of confidential information entrusted to employees.[207] Treating privacy as a matter of trust would potentially allow courts to enjoin ongoing or imminent privacy harms.

IV. POTENTIAL OBJECTIONS

It is said that the mark of a good compromise is that it makes everyone unhappy, and both privacy advocates and data industry representatives may find faults in our conception of privacy harm. We characterize some of the likely objections as falling into six categories—(1) scope, (2) self-exculpation, (3) practicality, (4) ambiguity, (5) dynamism, and (6) doctrine—and discuss each of these below.

---

[204] *See* FRANKEL, *supra* note 146, at 258–60 (discussing punitive damages as a remedy for breach of fiduciary duty); RESTATEMENT (THIRD) OF TRUSTS § 100 cmt. d (AM. L. INST. 2012) (noting that punitive damages for breach of trust are permitted under the laws of many jurisdictions in egregious cases). Pennsylvania has adopted § 908(2) of the Restatement (Second) of Torts regarding the imposition of punitive damages, which permits punitive damages for conduct that is "outrageous because of the defendant's evil motives or his reckless indifference to the rights of others." Rizzo v. Haines, 555 A.2d 58, 69 (Pa. 1989).

[205] *See* FRANKEL, *supra* note 146, at 249–51 (explaining injunctive relief as a fiduciary law remedy).

[206] *See* Maritrans GP Inc. v. Pepper, Hamilton & Scheetz, 602 A.2d 1277, 1286–87 (Pa. 1992) (affirming grant of injunction because "the danger of revelation of the confidences of a former client is so great that injunctive relief is warranted"); *see also* Mylan, Inc. v. Kirkland & Ellis LLP, No. 15-581, 2015 WL 12733414, at *24 (W.D. Pa. June 9, 2015) (finding that a preliminary injunction was a proper mechanism to abate a breach of fiduciary duty by a law firm).

[207] *See* Carl A. Colteryahn Dairy, Inc. v. Schneider Dairy, 203 A.2d 469, 471 (Pa. 1964) ("[W]e have long recognized that the use of confidential material obtained by an employee from a position of trust and confidence may not be used in later competition to the prejudice of his employer.").

A. *Scope*

Advocates for strong privacy rights might object that our relationship-based definition of privacy harm is too narrow since it focuses primarily upon data collectors with whom data subjects have voluntarily shared information, excluding many other important players in the information ecosystem.[208] We have two responses to this objection. *First*, the limited scope of our theory is a feature, not a bug. The mass collection and resale of personal data by third parties gives rise to privacy risks, but it also produces a number of social benefits, including fraud prevention and improved product offerings.[209] Legislatures and regulators are more appropriately situated to deal with these tradeoffs than courts wielding the blunt instrument of tort law. Furthermore, broad-based rules against the disclosure of information that are not grounded in party relationships will be more vulnerable to First Amendment challenges.[210] *Second*, even data collectors who do not have a direct relationship with data subjects would still face a (limited) duty of confidentiality. Because all data subjects would reasonably expect their private information to be kept secure from criminals, regardless of whether they consented to the initial collection of that information, our standard would require all data collectors to take reasonable cybersecurity precautions against the unauthorized theft of personally identifiable information—an improvement over the current fragmented state of data breach law.[211]

B. *Self-Exculpation*

Privacy advocates might also object that data collectors could potentially limit data subjects' reasonable privacy expectations through the use of disclaimers and broadly-worded privacy policies.[212] A relationship-based model of harm may fail to recognize any harms if the stronger party can unilaterally set the terms of the relationship so as to exculpate itself from any meaningful responsibility.[213] The idea of protecting privacy through a "notice and choice" framework is generally thought to be ineffective[214] because most

---

[208] *See* discussion *supra* Section III.B (discussing the data broker industry).

[209] *See* FED. TRADE COMM'N, *supra* note 98, at v (discussing consumer benefits from data broker products).

[210] *See* Balkin, *First Amendment*, *supra* note 17, at 1209–20 (discussing how restrictions on speech by fiduciaries are treated differently than restrictions on speech in general under the First Amendment).

[211] *See* discussion *supra* Section II.

[212] *See id.*

[213] *See* Omri Ben-Shahar & Lior Jacob Strahilevitz, *Contracting Over Privacy: Introduction*, 45 J. LEGAL STUD. S1, S8 (2016) (noting that, if privacy law protections are merely default rules, lawmakers should anticipate wholesale opt-outs by firms posting privacy notices that effectively override the default rules).

[214] *See, e.g.*, Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, 42 SEATTLE U. L. REV. 1057, 1072 (2019) ("Notice and choice has been roundly criticized

people do not read privacy policies,[215] privacy policies are generally difficult to understand,[216] and data subjects often have little power to decline,[217] particularly in contexts such as the employer-employee relationship. Consider, for example, an employer who creates a company privacy policy containing a clause to the effect that, "Employer undertakes no responsibility to protect Employees' data against the risks of theft, misappropriation, publication, or misuse, and Employer may use, share, publish, or sell Employees' data for any purposes whatsoever, including purposes not germane to the employer-employee relationship." Would such a clause be effective to define a duty of care out of existence by unilaterally setting the terms of the parties' relationship and the employees' expectations?

We think the answer to this question is probably no for two reasons. While most fiduciary law rules are treated as default rules that may be changed by agreement between the fiduciary and the beneficiary,[218] fiduciary law recognizes a "mandatory core" that cannot be overridden by agreement, including a requirement that the "principal cannot authorize the fiduciary to act in bad faith."[219] Even where a principal has authorized self-dealing, fiduciary law still requires the fiduciary to act in good faith and to inform the principal of material facts.[220] The existence of these mandatory standards "insulates fiduciary obligations that the law assumes would not be bargained away by a fully-informed, sophisticated principal."[221] When fiduciary duties are waived, transforming fiduciary relationships into

---

by policymakers, academics, social scientists, advocates, and others for quite some time, and with good reason.") (footnotes omitted); Ari Ezra Waldman, *Privacy, Notice, and Design*, 21 STAN. TECH. L. REV. 74, 76 (2018) [hereinafter Waldman, *Notice*] ("Privacy policies are confusing, inconspicuous, and inscrutable.") (footnotes omitted).

[215] *See* DELOITTE, 2017 GLOBAL MOBILE CONSUMER SURVEY: US EDITION 12 (2017), https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-2017-global-mobile-consumer-survey-executive-summary.pdf (finding that ninety-one percent of consumers accept online legal terms and conditions without reading them).

[216] *See* Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1479–81 (2019) [hereinafter Richards & Hartzog, *Pathologies*] (discussing phenomenon of "unwitting consent" in which consumers fail to understand the legal agreements they are agreeing to or the technology that mediates their relationship with the company).

[217] *See id.* at 1486–90 (discussing phenomenon of "coerced consent" in which consumers have no realistic option except to agree to company policies).

[218] FRANKEL, *supra* note 146, at 195; *see also* Criddle, *Fiduciary Foundtions*, *supra* note 150, at 130 (noting that, while some fiduciary duties may be modified by contract, courts often treat some as non-negotiable).

[219] Sitkoff, *supra* note 199, at 1046.

[220] *Id.*; *see also* Warehime v. Warehime, 761 A.2d 1138, 1142 (Pa. 2000) (Saylor, J., concurring) ("Whether, and to what extent, parties may contractually alter or eliminate [fiduciary] duties implicates an extensive, ongoing debate in the legal community among segments sometimes denominated in the commentary as contractarians and anti-contractarians. . . . Even under contractarian theory, however, in order for general principles regarding fiduciary duty to be overridden, there must be a sufficient meeting of the minds concerning the action of the fiduciary . . . .") (citations omitted).

[221] Sitkoff, *supra* note 199, at 1047.

contractual relationships, the waiver generally must meet conditions including full notice to the beneficiary, a finding that the beneficiary is capable of independent will and judgment, clear and specific consent by the beneficiary, and substantive fairness.[222] Courts faced with data collectors attempting to stretch their rights beyond that which a reasonable data subject would agree to could draw upon these lines of precedent in refusing to recognize such "agreements."[223]

Moreover, we believe that an analysis based on relationships and data subject expectations would view privacy policies as evidence of the parties' expectations, but only as inconclusive evidence, worthy of consideration insofar as they are likely to be read and understood. A 2009 study estimated that, "if all American Internet users were to annually read the online privacy policies word-for-word each time they visited a new site, the nation would spend about [fifty-four] billion hours reading privacy policies," an average of 244 hours per year or forty minutes per day.[224] Former FTC chairman Jon Leibowitz has remarked, "We all agree that consumers don't read privacy policies."[225] Not even Chief Justice John Roberts reads all of the "clickwrap" contracts that he encounters while browsing the Internet.[226] Reasonable people cannot and do not read all of the boilerplate legalese that they come across online, much less understand it; thus, such documents cannot represent the last word defining online relationships.[227] A privacy policy that is incomprehensible to the average person, painfully lengthy, or hidden deep within a corporate website, therefore, represents very weak evidence of what a reasonable user should expect. On the other hand, even boilerplate privacy policies could provide a useful floor for defining the duty of care since a company's violations of its own policies would constitute strong evidence that user expectations were violated, as well.[228] Companies that wish to limit

---

[222] FRANKEL, *supra* note 146, at 200–07.

[223] *But see Warehime*, 761 A.2d at 1141 (holding that the contractual language was effective to limit a fiduciary's duty of loyalty to a duty of good faith).

[224] Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S 543, 563 (2008).

[225] Jon Leibowitz, Chairman, Fed. Trade Comm'n, Introductory Remarks at the FTC Privacy Roundtable (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/introductory-remarks-ftc-privacy-roundtable/091207privacyremarks.pdf.

[226] *See* Debra Cassens Weiss, *Chief Justice Roberts Admits He Doesn't Read the Computer Fine Print*, ABA J. (Oct. 20, 2010, 1:17 PM), https://www.abajournal.com/news/article/chief_justice_roberts_admits_he_doesnt_read_the_computer_fine_print ("Answering a student question, Roberts admitted he usually doesn't read the computer jargon that is a condition of accessing websites . . . .").

[227] *See generally* Richards & Hartzog, *Pathologies*, *supra* note 216, at 1478–86 (discussing the phenomena of unwitting consent, coerced consent, and incapacitated consent as they relate to consumer adoption of privacy policies).

[228] The FTC has pursued companies for issuing misleading privacy policies under the theory that such policies constitute deceptive trade practices. *See, e.g.*, Fed. Trade Comm'n v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 626–31 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015) (denying a motion

their *Dittman* liabilities would have to adopt transparent design principles, making clear to users how their data are being used.[229]

C. *Practicality*

Privacy advocates might also argue that, as a practical matter, only theories that are amenable to class litigation are likely to provide meaningful protection for data subjects since, in most instances, the costs of litigation will make it impracticable for injured data subjects to pursue individual lawsuits. Because damages for privacy violations are likely to be low on the individual level,[230] in many cases collective litigation will be the only practicable way to vindicate data subjects' rights. Since modern data collectors gather information at an enormous scale, rights that can only be vindicated at the individual level will not offer any realistic hopes of deterrence or redress. However, as discussed above, we believe that claims decided under our theory would be capable of class adjudication since the subjective privacy expectations of individual class members would be irrelevant.[231] Notably, Pennsylvania courts have held that claims for breaches of fiduciary duty may be amenable to class treatment.[232]

D. *Ambiguity*

We have discussed some of the objections that privacy advocates may raise in response to our theory. Alternatively, data collectors and industry advocates might argue that a relationship-based standard of care is too flexible and indeterminate to provide companies or the public with ex ante notice of what the law requires, thus making it impossible for companies to appropriately calibrate their privacy and data use policies, providing a

---

to dismiss where the FTC brought action alleging that a hospitality company had falsely represented that it had implemented reasonable and appropriate data security measures).

[229] *See* Waldman, *Notice*, *supra* note 214, at 117–24 (arguing that privacy regulators must consider website designs and user interfaces); Paul Ohm, *Forthright Code*, 56 HOUS. L. REV. 471, 472–73 (2018) (calling for legal standards that require companies to be honest, direct, and candid regarding data collection).

[230] *See* discussion *supra* Section III.C.2.

[231] *See* discussion *supra* Section IV.

[232] *See, e.g.*, Wurtzel v. Park Towne Place Assocs. Ltd., No. 3511, 2002 WL 31487894, at *12 (Pa. Ct. Com. Pl. Nov. 5, 2002) (providing a class certification order holding that breach of fiduciary duty claims regarding a limited partnership agreement involved common questions of law and fact); Parsky v. First Union Corp., No. 771, 2001 WL 535786, at *7 (Pa. Ct. Com. Pl. May 8, 2001) (holding that claims for breach of fiduciary duty met the commonality requirement for class certification); O'Neill v. Sovereign Bank, No. 9708-0525, 1998 WL 1543498, at *10 (Pa. Ct. Com. Pl. Dec. 15, 1998) (certifying a class action based in part on breach of fiduciary duty claims). The Pennsylvania Superior Court has held that class certification may be appropriate for fiduciary duty claims since, in such cases, there is no need to prove reliance by class members; however, the Pennsylvania Supreme Court reversed the decision on other grounds. Basile v. H & R Block, Inc., 729 A.2d 574, 584 (Pa. Super. Ct. 1999), *rev'd on other grounds*, 761 A.2d 1115 (Pa. 2000).

windfall for aggressive plaintiffs' lawyers, and raising costs for everyone.[233] How can we assess when the hypothetical "reasonable user" expects a service as novel and sprawling as Google to provide? It may be difficult or even impossible for courts to reliably discern what constitutes objectively reasonable data subject expectations in regard to new digital products, particularly those with very diverse user communities.

We disagree with the notion that companies are incapable of responding to a flexible, contextual duty of care. In the words of Justice Saylor, concurring in *Warehime v. Warehime*, "[t]he complexities associated with compliance with such loosely-defined duties are simply part of the burden borne by one occupying a position of substantial trust."[234] Kenneth Bamberger and Deirdre Mulligan's influential study of corporate privacy officers in the United States and Europe found that a degree of ambiguity "fostered evolution and dynamism" amongst corporate privacy professionals,[235] particularly where firms were required to publicly acknowledge instances of corporate failure and multiple parties could sanction firms for privacy breaches.[236] By contrast, rule-bound governance tends to diminish corporate reliance on internal privacy experts, thereby reducing privacy compliance to a check-off-the-boxes exercise cordoned in the legal department, rather than a matter of concern to executives and designers.[237] A tort regime, such as the one proposed here, may be superior to a top-down, prescriptive regulatory regime, thus empowering privacy professionals, focusing decision-makers' attention to privacy concerns, and ultimately protecting the interests of data subjects.

As for the objection that a theory based on user expectations cannot adequately govern a field characterized by drastic technosocial revolutions, this is another area where the theory's limited scope would come into play. In some cases, courts may not be able to discern what a reasonable data subject would expect from an innovative new information services company vis-à-vis their privacy. In such instances, where there are no reasonable expectations of the subject-collector relationship for courts to defend, our theory would not recognize any legally cognizable harm suffered by data subjects or any liability incurred by data collectors. However, where courts do find that data collectors have taken advantage of data subjects' trust or otherwise violated expectations of the relationship, that is an appropriate subject for redress. The fact that hard cases may come up from time to time

---

[233] *See, e.g.*, JENNIFER HUDDLESTON, AN ANALYSIS OF RECENT FEDERAL DATA PRIVACY LEGISLATION PROPOSALS 4 (2019) (arguing that imposing fiduciary requirements on digital service providers may force them to value privacy over other values that customers may prefer).

[234] Warehime v. Warehime, 761 A.2d 1138, 1143 (Pa. 2000) (Saylor, J., concurring).

[235] KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE 222 (2015).

[236] *Id.* at 231.

[237] *Id.* at 244.

does not justify turning a blind eye to easy cases in which data subjects' justifiable expectations have been plainly violated.

E. *Dynamism*

Data collectors might also argue that adopting a relationship-based standard of care will freeze relationships between data collectors and data subjects in amber, discouraging dynamism, as well as freeze the development of innovative new products and business models.[238] The fact that a novel information practice is surprising to consumers does not necessarily imply that it is injurious to them—sometimes surprises can be pleasant.[239]

Our answer to this possible objection is that, while relationships between data collectors and data subjects can change over time, when the data collector seeks to unilaterally change the relationship, it should bear the onus of explaining the change to data subjects and giving data subjects a meaningful opportunity to consider whether they want to continue the relationship on the new terms offered. Companies that forthrightly explain their policies and implement transparent design, so as to keep the expectations of the reasonable user aligned with their actions, will be able to continually roll out new products and refine their existing offerings; companies that upend user expectations without warning will face deserved sanction. A rule that slows down Silicon Valley's innovations to a pace that can be understood by the people affected by those innovations will indeed impose costs on entrepreneurs seeking to "[m]ove fast and break things,"[240] but we think that those costs are socially justified and that they will even benefit the information industry over the long term by promoting trust between data collectors and data subjects.[241] The tort law principle endorsed in *Dittman*—that "anyone who does an affirmative act is under a duty to others to exercise the care of a reasonable man to protect them against an unreasonable risk of harm to them arising out of the act"[242]—means that sometimes we must slow down, so as not to break things.

---

[238] *See, e.g.*, HUDDLESTON, *supra* note 233, at 6 (arguing that regulatory and compliance costs of privacy legislation will quash innovation).

[239] *See* Calo & Rosenblat, *supra* note 117, at 1688 ("[A] consumer can be surprised (or delighted) without the practice necessarily rising to the level of actionable harm.").

[240] *See* Moshe Y. Vardi, *Move Fast and Break Things*, 61 COMMC'NS ACM 7, 7 (2018) (discussing the concept of disruptive innovation).

[241] *See* Waldman, *Designing*, *supra* note 142, at 712 (discussing how privacy is good for business because it encourages trust between consumers and the businesses that use their data).

[242] RESTATEMENT (SECOND) OF TORTS § 302 cmt. a (AM. L. INST. 1965); Dittman v. UPMC, 196 A.3d 1036, 1044 (Pa. 2018).

F. *Doctrine*

Finally, on a doctrinal level, people may argue that fiduciary duties are often described as contractual or quasi-contractual in nature,[243] whereas the *Dittman* common law duty to care for data "exists independently from any contractual obligations between the parties."[244] However, contract law and fiduciary law fulfill separate functions.[245] Pennsylvania law provides separate statutes of limitation for contract and breach of fiduciary action claims,[246] and the Pennsylvania Supreme Court has referred to breach of fiduciary duty actions as tort actions.[247] Thus, fiduciary law can inform a common law duty of care that is independent of contract liability, or at least sufficiently independent of contract liability to fall within *Dittman*'s conceptual space.

---

[243] *See, e.g.*, FRANKEL, *supra* note 146, at 229–32 (summarizing the arguments for classifying fiduciary rules as contract rules); Henry N. Butler & Larry E. Ribstein, *Opting Out of Fiduciary Duties: A Response to the Anti-Contractarians*, 65 WASH. L. REV. 1, 2–4 (1990) (discussing the background of the debate between contractarian and anti-contractarian views of fiduciary relationships).

[244] *Dittman*, 196 A.3d at 1056.

[245] *See, e.g.*, FRANKEL, *supra* note 146, at 232–35 (summarizing the arguments against classifying fiduciary rules as contract rules); Paul B. Miller, *Justifying Fiduciary Duties*, 58 MCGILL L.J. 969 (2013) (explaining the purpose of the fiduciary relationship as securing the exclusivity of the beneficiary's rights); Daniel Markovits, *Sharing Ex Ante and Sharing Ex Post: The Non-Contractual Basis of Fiduciary Relations*, *in* PHILOSOPHICAL FOUNDATIONS OF FIDUCIARY LAW 209 (Andrew S Gold & Paul B Miller eds., 2014) (arguing that fiduciary law cannot be understood on a contract model because contract law is based on ex ante expectations and fiduciary law is based on ex post expectations); Robert Flannigan, *The Economics of Fiduciary Accountability*, 32 DEL. J. CORP. L. 393, 420 (2007) ("The general law of contract and the general law of fiduciary obligation have distinct social functions."); Margaret M. Blair & Lynn A. Stout, *Trust, Trustworthiness, and the Behavioral Foundations of Corporate Law*, 149 U. PA. L. REV. 1735, 1784 (2001) ("It seems peculiar indeed—given the importance of self-regarding behavior to conventional contract and the centrality of other-regarding behavior to the fiduciary 'contract'—to describe both with the same label."); Criddle, *Fiduciary Foundations*, *supra* note 150, at 133 n.63 ("Anti-contractarians argue that fiduciary duties cannot plausibly be characterized as mere default contract rules because courts routinely enforce these duties as mandatory standards irrespective of the contracting parties' agreements.").

[246] *See* Melley v. Pioneer Bank, N.A., 834 A.2d 1191, 1200–01 (Pa. Super. Ct. 2003) (explaining that a two-year statute of limitations applies to breach of fiduciary actions, whereas a four-year statute of limitations applies to breach of contract actions).

[247] *See* Toney v. Chester Cnty. Hosp., 36 A.3d 83, 84 n.1 (Pa. 2011) ("[I]f an actor has a particular contractual or fiduciary relationship with a victim and it is foreseeable that the actor's carelessness could cause severe emotional harm to the victim, and that harm occurs, a cognizable tort arises which is, in short-form, referred to as a breach of a 'contractual or fiduciary duty' not to inflict foreseeable emotional distress upon a victim."); LaFarge Corp. v. Commonwealth Ins. Dep't, 735 A.2d 74, 77 (Pa. 1999) ("Allegations of breach of fiduciary duty or other corporate torts are properly heard in the courts of common pleas . . . ."); Drain v. Covenant Life Ins. Co., 712 A.2d 273, 277 (Pa. 1998) (holding that a derivative claim seeking relief for an alleged breach of fiduciary duties was a tort claim within the jurisdiction of the Court of Common Pleas); *see also* RESTATEMENT (SECOND) OF TORTS § 874 cmt. b (AM. L. INST. 1979) ("A fiduciary who commits a breach of his duty as a fiduciary is guilty of tortious conduct to the person for whom he should act.")

CONCLUSION

Private tort litigation can play a productive role in shaping an environment that is more attuned to the needs, concerns, and security of data subjects (i.e., all of us), while also respecting the interests of the businesses that collect personal information. Ari Ezra Waldman discussed how private tort litigation encouraged automakers and drug companies to incorporate consumer safety into car and drug design by incentivizing safety improvements, supplementing inadequate regulatory structures, and raising public and corporate awareness.[248] A similar realignment is possible today, but only if courts can first develop a framework of what harm and safety mean in the data privacy context. This Article is a step toward developing that framework and answering the questions inevitably raised by these new developments in data tort law.

[248] Waldman, *Designing*, *supra* note 142, at 708–09.