No Harm, No Foul? Exploring the Harm Caused by Data Breaches

A Thesis
SUBMITTED TO THE FACULTY OF
UNIVERSITY OF MINNESOTA
BY

George Ashenmacher

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
MASTER OF ARTS

Dr. Amy Kristin Sanders, Adviser

May 2015

ACKNOWLEDGEMENTS

Thank you to Professors Amy Sanders, Bill McGeveran, and Jane Kirtley.

DEDICATION

This is dedicated to my family, and to Julia.

ABSTRACT

This thesis explores the harm that occurs to individuals whose data has been exposed to a third party as a result of a data breach, but which has not been used to commit identity theft or fraud.

The vast majority of Americans disclose their Personally Identifiable Information ("PII") to private entities almost everyday. Yet this information is increasingly insecure in those hands, as a recent rise in data breaches makes evident. Law responded to this problem, in part, by criminalizing hacking and identity theft. But have individuals suffered harm when their data has been made vulnerable? Where the hacker has not used the PII to commit fraud, American courts have concluded that there is simply no harm for them to redress.

This thesis examines the premise that individuals have not suffered harm unless they have sustained a concrete financial injury. Part I engages scholarly literature to explain the concept of autonomy. This Part develops how each of liberty, dignity and privacy protect the value of autonomy in American law. Part II then applies each of these concepts in the data breach context to show that the resulting harm is to an individuals' autonomy. Unlike other instances in which autonomy is vulnerable, here neither privacy nor liberty can be convincingly used as a legal tool to protect it. Instead, the proper tool is the invocation of dignitary harms. Faced with an uncertainty about how their information may be used, victims lose awareness of their negative freedom. This harm deserves legal redress.

Finally, Part III argues for the practical utility of the harm inquiry. Recently, the FTC has been challenged to identify what, if any, injuries befall consumers whose data has been made vulnerable where there has been no identity theft. This thesis urges the recognition of the harm as one to individuals' dignity. Doing so refocuses the inquiry against the companies who hold PII, instead of the hacker who acquires it. Doing so also justifies FTC actions against such companies.

TABLE OF CONTENTS

LIST OF FIGURES

What we have been examining is one facet of man's struggle for a human dimension in a highly structured society, for dignity notwithstanding dependence. Science has vastly complicated this elemental contest.[1]

I. INTRODUCTION

Just before Christmas 2013, Mike and Hallie, a young married couple in Minneapolis, received an e-mail from Target. The e-mail explained that Target's data security system had been breached by an unknown hacker, and that Target customers' personal information was now outside of Target's control. This meant Mike and Hallie's credit card information was now vulnerable to use by the hacker.

"We understand that a situation like this creates stress and anxiety about the safety of your payment card data at Target," the e-mail read.[2] "Our brand has been built on a 50-year foundation of trust with our guests, and we want to assure you that the cause of this issue has been addressed and you can shop with confidence at Target."[3] Target offered a year of credit monitoring to bolster its claim.[4]

Despite Target's assurances, Mike and Hallie felt anything but confidence or trust. "Something like a data breach feels so far removed from the actual consumer that when it happens, you're left feeling a bit helpless," Hallie explained.[5] "[We] just have to

---

[1] Alan Westin, PRIVACY AND FREEDOM xi (Athenaeum, 1967).

[2] E-mail from Target Corporation (Dec. 21, 2013).

[3] *Id*.

[4] *Id*. ("[W]e will offer free credit monitoring services for everyone impacted. We'll be in touch with you soon on how and where to access the service.").

[5] Interview with Mike and Hallie (Feb. 9, 2015).

hope that the system Target put in place is good enough to stop the damage."[6] Unsure of what would happen with their information, the couple kept an eye on their bank statements, waiting to see if their identity would be used to rack up fraudulent charges.

Millions of Americans have been in Mike and Hallie's position. Nearly all Americans operate in today's so-called Information Age, in which personal information is "widely disseminated and easily available" through the use of computer technology.[7] Americans find it increasingly difficult to live in modern society without releasing their "personally identifiable information" ("PII"),[8] such as name, Social Security number, address, and credit card information – information that is valuable insofar as it can be used to commit identity theft or other financial harms to individuals. Email, for instance, "plays an indispensable part in the Information Age" and has become "so pervasive that some persons may consider [it] to be [an] essential means or necessary instrument[ ] for self-expression, even self-identification."[9] Yet one must disclose PII to open a "Gmail"

---

[6] *Id*.

[7] Information Age, MERRIAM WEBSTER ONLINE DICTIONARY. 2015, (last visited Feb. 10, 2015) http://www.merriam webster.com/dictionary/information%20age.

[8] "Personally identifiable information" lacks a uniform definition. *See* Paul M. Schwartz and Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L.Q. REV. 1814, 1816 (2011). The Video Privacy Protection Act defines it as "information which identifies a person." Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2006). The Graham-Leach-Bliley Act (GLBA) defines it as "nonpublic personal information." Gramm-Leach-Bliley Act of 1999, 15 U.S.C. § 6809(4)(A) (2006). Other statutes take a more specific approach, defining specific information as PII. *See, e.g.*, Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 Mass. Code Regs. § 17.04 (2010) (defining PII as a person's first name and last name, or first initial and last name in combination with either a Social Security number, driver's license number, financial account number, or credit or debit card number).

[9] United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010). Over 85% of Americans are online. *See* Kathryn Zickuhr, *Who's Not Online and Why*, PEW RESEARCH CENTER (Sep. 2013), http://www.pewinternet.org/2013/09/25/whos-not-online-and-why/.

account.[10] Or consider banking. More than 93 percent of Americans have a bank account,[11] the use of which requires disclosing PII.[12] And when it comes time to purchase goods, Americans inevitably fork over their PII.[13] Thus, "life today is fueled by information, and it is virtually impossible to live as an Information Age ghost, leaving no trail or residue."[14] Indeed, the enormous amount of individuals affected by data breaches today is testament to the pervasiveness of PII collection. The Target breach alone, for example, affected up to 70 million Americans in addition to Mike and Hallie.[15]

Yet, while individuals must release their PII, it is increasingly insecure in the hands of the entities, like Target, storing it. Anyone who reads the newspaper knows all too well the ubiquity of data breaches. High-profile breaches, like Sony's in late 2014, or breaches in which massive amounts of valuable and sensitive personal information are

---

[10] *See Privacy Policy*, GOOGLE (updated Dec. 2014), http://www.google.com/policies/privacy/ ("[M]any of our services require you to sign up for a Google Account. When you do, we'll ask for personal information, like your name, email address, telephone number or credit card.").

[11] *See 2013 FDIC National Survey of Unbanked and Underbanked Households*, FEDERAL DEPOSIT INS. CORP. (Oct. 2014), *available at* https://www.fdic.gov/householdsurvey/.

[12] To open a Wells Fargo or Bank of America account, one must disclose their Social Security number and driver's license information. *What You'll Need*, WELLS FARGO (last visited Feb. 10, 2015); https://apply.wellsfargo.com/common_auth_start; *Apply Online Frequently Asked Questions*, Bank of America (last visited Feb. 10, 2015) http://www.bankofamerica.com/deposits/checksave/index.cfm?template=lc_faq_applyonline&context=&statecheck=VA&cd_bag=&sa_bag=&ch_bag

[13] Brief for the Fed. Trade Comm. at 2, *Federal Trade Commission v. Wyndham Hotels & Resorts, LLC* (FTC 2014), *available at* https://www.ftc.gov/system/files/documents/cases/141105wyndham_3cir_ftcbrief.pdf. ("Virtually all modern commerce involves the collection and storage of consumers' personal data, such as credit card numbers, passwords, and social security numbers.").

[14] Daniel Solove, THE DIGITAL PERSON: PRIVACY AND TECHNOLOGY IN THE INFORMATION AGE 8 (2004).

[15] According to Target's estimate. *See Data Breach FAQ*, TARGET (Feb. 2015 10:11 AM), *available at* https://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ#q5888.

exposed, like the January 2015 Anthem breach, regularly make headlines.[16] But even smaller breaches are occurring with increasing regularity. The Privacy Rights Clearinghouse began tracking data breaches – defined as "electronic entry by an outside party, malware and spyware" – large and small – in 2005.[17] Since 2012, each year has seen a steady increase.[18] Deemed "the year of the breach," 2014 saw 904 million records exposed within the first 9 months – a 95% increase from the same period in 2013.[19] And as of April 2015, 80,202,541 data breaches have already been recorded – up from 67,009,098 in 2014.[20] These breaches are, by and large, preventable. A number of studies have concluded that anywhere from 90 to 95% of breaches could have been prevented[21]

---

[16] *See* Andrea Peterson, *Lawsuits Against Sony Pictures Could Test Employer Responsibility for Data Breaches*, WASH. POST (Dec. 19, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/12/19/lawsuits-against-sony-pictures-could-test-employer-responsibility-for-data-breaches/; Reed Abelson & Julie Creswell, *Data Breach at Anthem May Forecast a Trend*, N.Y. TIMES (Feb. 6, 2015), http://www.nytimes.com/2015/02/07/business/data-breach-at-anthem-may-lead-to-others.html.

[17] *See Chronology of Data Breaches: Security Breaches 2005 – Present*, PRIVACY RIGHTS CLEARINGHOUSE (last visited Apr. 20, 2015).

[18] *Id. See also 2014 Internet Security Threat Report*, SYMANTEC CORPORATION, *available at* http://www.symantec.com/security_response/publications/threatreport.jsp (finding over 552 million unique identities were exposed because of breaches occurring in 2013 and that there was an increase of 62 percent in 2013 over data breaches reported in 2012).

[19] *2015 Data Protection & Breach Notification Readiness Guide*, THE ONLINE TRUST ALLIANCE 4 (Feb. 12, 2015) *available at* https://otalliance.org/system/files/files/resource/documents/dpd_2015_guide.pdf.

[20] *See supra* note 17.

[21] *See, e.g.*, *supra* note 19 ("While some may claim these breaches are the result of highly technical and sophisticated efforts, the data reported by the FBI and other organizations continually report more than 90 percent were avoidable had widely accepted best practices and security controls been applied."); John Fisher, *Secure My Data or Pay the Price: Consumer Remedy for the Negligent Enablement of Data Breach*, 4 WM. & MARY BUS. L. REV. 215, 220 (2013) (discussing recent data breaches and noting that "such incidents could often have been ameliorated or even entirely avoided by employing a minimal amount of modern information security practices."); Mary Culnan and Cynthia Williams, *How Ethics Can Enhance Organizational Privacy: Lessons from the ChoicePoint and TJX Data Breaches*, 33 MIS QUARTERLY 4, 678 (2009) ("A recent analysis by Verizon Business of more than 500 forensic investigations of U.S.

by the PII recipients with simple mechanisms such as data encryption or the use of Secure Sockets Layer.[22]

These breaches cause concrete, financial harms to the individual. Identity theft and accompanying fraud constitute a growing type of criminal activity in which a cyber thief impersonates the victim to fraudulently spend the victim's money.[23] In the wake of an identity theft, victims spend precious time and money to get their financial house in order.[24] No surprise, then, that law has responded to identity theft victims' plight. Hacking is illegal,[25] and Congress passed the Identity Theft and Assumption Deterrence Act in 1998, which criminalizes the transfer or use of another's identity to commit any other crime.[26] And plaintiffs in all 50 states can bring claims under state law corollaries.[27]

---

breaches involving more than 230 million records found that nearly 90 percent could have been prevented had reasonable security measures been implemented.").

[22] Secured Sockets Layers (SSL) are the standard security technology for establishing an encrypted link between a web server and a browser, which ensures that all data passed between the web server and browsers "remain private and integral." *FAQ: What is SSL?* SSL.COM (last accessed Mar. 8, 2015), http://info.ssl.com/article.aspx?id=10241. SSL "is an industry standard and is used by millions of websites in the protection of their online transactions with their customers." *Id*. For a discussion of some of the "cyber hygiene" practices companies are failing to implement, see Danny Yadron, *Five Simple Steps to Protect Corporate Data: What Companies Should Be Doing to Protect Their Computer Systems – But Aren't*, WALL ST. J. (Apr. 20, 2015), http://www.wsj.com/articles/five-simple-steps-to-protect-corporate-data-1429499477?mg=id-wsj.

[23] Daniel Solove, THE NEW VULNERABILITY: DATA SECURITY AND PERSONAL INFORMATION IN SECURING PRIVACY IN THE INTERNET AGE 112 (Radin & Chander, eds., Stanford University Press, 2008).

[24] *Identify Theft Survey Report* FEDERAL TRADE COMMISSION 6 (Sept. 2006) ("Victims of all types of ID theft spent hours of their time resolving the various problems that result from ID theft. The median value for the number of hours spent resolving problems by all victims was 4. However, 10 percent of all victims spent at least 55 hours resolving their problems. The top 5 percent of victims spent at least 130 hours."). For a discussion of the emotional turmoil identity theft victims face, see Herb Weisbaum, *ID Theft Can Take Heavy Emotional Toll on Victims*, TODAY MONEY (Nov. 20, 2014), http://www.today.com/money/id-theft-can-take-heavy-emotional-toll-victims-1D80305639.

[25] *See* Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

[26] 18 USCS § 1028. The statute makes it a crime to "knowingly transfer or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity

The government is eager to help the millions of identity theft victims reclaim their lost money and identity,[28] and identity theft prosecution is, understandably, highly prioritized.[29]

But have been individuals been harmed even where their PII has not been used to commit fraud? Are customers like Mike and Hallie harmed when the entities that store their information – be it Target, their local bank, or some other entity[30] – fail to protect it, such that the use of their information to commit fraud becomes merely more likely? By and large, American law has responded with an unsympathetic "no." Where there has been a breach without identity theft, plaintiffs have largely been unable to obtain a remedy against the entities who store their PII for failing to protect it against a breach.[31]

---

that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law." *See Identity Theft Overview*, FED. BUREAU OF INVESTIGATION, (last accessed Mar. 8, 2015), *available at* http://www.fbi.gov/about-us/investigate/cyber/identity_theft/identity-theft-overview.

[27] *Identity Theft*, NAT. CONF. OF STATE LEGISLATURES (last accessed Mar. 8, 2015), available at http://www.ncsl.org/research/financial-services-and-commerce/identity-theft-state-statutes.aspx. (providing each State's data breach laws); *See also State Laws: Criminal*, FEDERAL TRADE COMMISSION, available at http://www.ftc.gov/bcp/edu/microsites/idtheft/law-enforcement/state-laws-criminal.html (listing all states and federal territories that classify identity theft as criminal conduct).

[28] *See, e.g.*, *Guide for Assisting Identity Theft Victims*, FEDERAL TRADE COMMISSION (Sept. 2013), available at http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

[29] *See The Department of Justice's Efforts to Combat Identity Theft*, U.S. DEPT. OF JUSTICE OFFICE OF THE INSPECTOR GENERAL AUDIT DIVISION, at iii and iv (Mar. 2010), *available at* http://www.justice.gov/oig/reports/plus/a1021.pdf (discussing "the DOJ's improve[d] . . . efforts to combat identity theft" and noting that "the FBI frequently addresses identity theft through the Cyber Division's criminal intrusion program, which is currently a top FBI priority.").

[30] This thesis will refer to organizations that store individuals' PII as simply "PII recipients" for shorthand.

[31] Fisher, *supra* note 17, at 217. As the Third Circuit recently explained: "In this increasingly digitized world, a number of courts have had occasion to decide whether the risk of future harm posed by data security breaches confers standing on persons whose information may have been accessed. Most courts have held that such plaintiffs lack standing because the harm is too speculative." Reilly v. Ceridian Corp., 664 F.3d 38, 43 (3d Cir. 2011) (internal quotations omitted).

Yet there is a growing sense that individuals are harmed even where their information has not been used to commit identity theft.[32] Scholars have openly questioned the "no harm, no foul" premise that individuals are not harmed in the absence of some use of their PII, but recognize the "specifically acute problem" of identifying how that harm can best be described.[33] Law Professors Daniel Solove and Woodrow Hartzog ask:

> What is the harm when data is leaked? This question has confounded courts, which often don't recognize a harm . . . If people's data are leaked, but they do not suffer from identity theft, are they harmed? Although courts struggle to recognize harm, there clearly seems to be a substantial negative impact on people's lives.[34]

Solove and Hartzog take a literal approach to answering this question. They discuss the physical and financial toils victims must endure to rectify their financial state of affairs.[35] This thesis, in contrast, seeks to answer that question by suggesting a broader conception of harm. What value or legal interest is invaded when the entities that collect our PII fail to protect it? What is the nature of this harm?

---

[32] These types of cases "are those in which the plaintiff's information has been accessed but that information has not been used to open bank accounts, make unauthorized purchases, or otherwise harm the plaintiffs. However, these plaintiffs typically claims that they have been harmed in other ways: incurring costs for credit-monitoring services, paying the costs of cancelling and receiving new bank cards, suffering loss of reward points from cancelled cars, and enduring general anxiety that their information will be used in the future to make unauthorized purchases." Caroline C. Cease, *Giving Out Your Number: A Look at the Current State of Data Breach Litigation*, 66 ALA. L. REV. 395, 399 (2014).

[33] Daniel Solove & Woodrow Hartzog, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 1, 33 (2015).

[34] *Id*.

[35] *Id*. ("The harm of credit card fraud is that it can take a long time to replace all the credit card information in various accounts. People have card data on file with countless businesses and organizations for automatic charges and other transactions. Replacing all this data can be a major chore. People's time has a price. That price will vary, but it rarely is zero . . . A data breach also causes a harm because people are at greater risk for fraud and will feel anxiety and concern. People might reasonably spend money and time to protect themselves.").

This thesis seeks to examine what harm occurs to individuals whose data has been made vulnerable (that is, out of the original receiving party's control) in the wake of a data breach, but who have not yet been victims of identity theft.[36] Two research questions guide the thesis:

> **RQ1**: What harm occurs to individuals whose data has been exposed due to a data breach, but who have not been victims of identify theft? What is the nature of that harm?
>
> **RQ2**: Is this harm the type law should address?

In addressing these questions, the thesis attempts to avoid a marked tendency to resort to so-called "intuitionist" arguments, in which harm is assumed as self-evident but not described.[37] Instead, this thesis examines what harm, if any, occurs at each discrete sequence of events within the data breach context: (1) the transfer of PII from the individual to the PII recipient; (2) the storage and security of the PII; and (3) the breach itself.

---

[36] A variety of activities may give rise to data security breaches. "Breaches can result from intentional actions, including hacking; employee theft; theft of equipment (such as laptop computers and hard drives); and deception or misrepresentation to obtain unauthorized data. They can also arise from negligent conduct by the organization that suffered the security breach, including the loss of laptop computers or hard disks, loss of data tapes; unintentional exposure of data on the Internet; and improper disposal of data. Security breaches can also arise from an organization's implementation of software that the organization reasonably believes to be secure, but which contains vulnerabilities that render it insecure." Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation*: *Has the Commission Gone Too Far?* 60 ADMIN. L. REV. 127, 144-45 (2008). This thesis does not draw a distinction between breaches caused by hackers intending to penetrate a security system, and breaches in which some negligence on the part of the PII-recipient itself causes information to be released. From the individual's perspective, both situations place the individual in a state of anxiety about how their information may be used, as discussed more in Part II, *infra*.

[37] *See* James Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1154 (2004) ("Thus, the typical privacy article rests its case precisely on an appeal to its reader's intuitions and anxieties about the evils of privacy violations. Imagine invasions of your privacy, the argument runs. Do they not seem like violations of your very personhood? Since violations of privacy seem intuitively horrible to everybody, the argument continues, safeguarding privacy must be a legal imperative, just as safeguarding property or contract is a legal imperative.").

This thesis begins in Part I by exploring the concept and value of autonomy, and the role it plays as a normative goal in democratic societies. Part I then examines the concepts of liberty, dignity and privacy, which are seen as vanguards of the core value of autonomy. Each of the three are defined by their own characteristics when applied in the legal context, which has important implications for determining how best to describe the harm that befalls individuals in the data breach context.

Turning back to the data breach context in Part II, this thesis applies the understanding of autonomy developed in Part I to each discrete sequence of events that occur throughout a data breach. The thesis answers its research questions by (a) evaluating the values that are affected by each juncture of a data breach; and (b) whether law has typically protected those values in the past, which would justify offering legal redress for data breach victims who do not suffer identity theft. Finally, Part III discusses the practical importance of this inquiry, arguing that a better articulation of harm is necessary, and pointing to recent FTC litigation as an example why.

PART I

II. AUTONOMY

This thesis argues that data breaches violate data breach victims' autonomy. To understand this harm, an understanding of autonomy itself is required. Autonomy is a broad, "notoriously vague" concept.[38] This is in part because the term is used widely, discussed in the realms of philosophy, medicine, law, politics, human rights, and even robotics.[39] To focus on its meaning relevant to this thesis, this section begins by examining the concept of autonomy in philosophy and then moves onto examining its role in liberal political theory.

a. Individual Autonomy

"Autonomy" literally means "self law": the Greek *autonomia* combines *autos* – "self," with *nomos* – "law." The term was first used to describe the Greek city-state; a city had *autonomia* "when its citizens made their own laws, as opposed to being under the control of some conquering power."[40] Thus, the term's original use was political, describing the ability and right of nation-states "to administer their own affairs."[41] Autonomy began to refer to the conduct of individuals only in the nineteenth century.[42]

---

[38] David Strauss, *Persuasion, Autonomy, and Freedom of Expression*, 91 COLUM. L. REV. 334, 354 (1991). *See also* Thomas Hill, *Autonomy and Benevolent Lies*, 18 J. VALUE INQUIRY 251 (1984) ("there is no uniform understanding about what autonomy is.").

[39] Tim Smithers, *Autonomy in Robots and Other Agents*, 34.1 BRAIN AND COGNITION 88 (1997).

[40] Gerald Dworkin, THE THEORY AND PRACTICE OF AUTONOMY 12-13 (Cambridge University Press, 1980).

[41] Stephen Darwall, *The Value of Autonomy and Autonomy of the Will*, 116 ETHICS 263 (2006).

[42] *Id*.

Philosopher Immanuel Kant is widely credited with inspiring a view of individuals as "autonomous, rational decision makers able to reason and make choices."[43] A succinct Kantian definition of autonomy is elusive,[44] but a working definition develops from Kant's examination of will, morality, and rationality.

Kant began by starting from the familiar premise that humans possessed the ability to reason, and that we can use this reason and logic to choose one path of action over another.[45] In examining the paths available, Kant was concerned with determining which human actions could produce objective laws of morality – a "kingdom of ends," in which humans guide their conduct according to some universally held maxims or imperatives.[46] Kant's premise was that actions guided by self-interest or individualized influences cannot produce universal law because then each person's actions would conflict with those of others.[47]

Humans exercise their will, according to Kant, by acting rationally.[48] But rationality itself could be guided by base impulses and animalistic instincts.[49] Whereas

---

[43] Bruce J. Winick, *On Autonomy: Legal and Psychological Perspectives*, 37 VILL. L. REV. 1705, 1714-15 (2000) (quoting Immanuel Kant, Foundations of the Metaphysics of Moral 59-67 (J. Beck trans., 1959)).

[44] The most evident may be "the idea of the will of every rational being as a will giving universal law." Immanuel Kant, Groundwork for the Metaphysics of Morals 50 (A. Wood trans., Yale University Press 2002).

[45] *Id*. at 52.

[46] *Id*.

[47] Thomas Hill explains that these principles "are self-imposed insofar as they stem from one's rational nature." Hill, *supra* note 38 at 255.

[48] Kant, *supra* note 44 at 29.

[49] Kant believed that "feelings, emotions, habits, and other non-intellectual factors are excluded from autonomous decision-making. Any circumstances that particularize us are also excluded from autonomous

choice guided by pure reason is "free choice," choice that can be determined "only by inclination (sensible impulse, stimulus) would be animal choice."[50] Thus, Kant supposed a spectrum of rationality. On one end, we behave purely out of immediate, almost reflexive self-interest, or at the dictate of another. At the other, we act to conform ourselves with principles and maxims because of their moral worth and universality, which exist from their being product of one's unadulterated reason.[51] Acting out of "fear of punishment, desire for approval, blind acceptance of tradition, animal instinct," and other factors is, in one sense, rational, because we divine some benefit from each.[52] But those factors coerce our will because they substitute acting solely to accord with some universal, moral law with the desire to act in a way that benefits only the individual.[53]

Kant's autonomy, then, is the exercise of one's will in accordance with universal law, or higher-order principles and maxims. One is autonomous when he or she acts with pure reason free from constraining factors that would corrupt his or her otherwise purely

---

decision-making." *Moral Autonomy*, THE INTERNET ENCYCLOPEDIA OF PHILOSOPHY (accessed Feb. 16, 2015).

[50] Immanuel Kant, FOUNDATIONS OF THE METAPHYSICS OF MORAL 42 (M. Gregor trans., Cambridge University Press, 1991).

[51] Kant illustrates how the motive for one's actions indicates the presence or lack of autonomy through an example of why two people would refrain from lying. *See* Kant *supra* note 44 at 58-59. Kant explains that the person who refrains from lying out of a desire to "retain [his] honorable reputation" is influenced by self-interest, whereas the person who refrains from lying "even if [he] did not incur the least disgrace" is autonomous. *Id*.

[52] Hill *supra* note 38 at 255.

[53] *Id*.

rational decisions. Thus, autonomy is closely associated with freedom and liberty.[54] Kant himself defined autonomy in terms of negative freedom: acting in accordance with one's will separate from external constraining influences.[55] Negative freedom allows individuals to be "capable of causing events without being causally determined to do so."[56]

Reflecting on Kant's writing, Professor Gerald Dworkin notes that autonomy can be thought of as "a second-order capacity of persons to reflect critically upon their first-order preferences, desires, wishes, and so forth and [as] the capacity to accept or attempt to change these in light of higher-order preferences and values."[57] "By exercising such a capacity," Dworkin writes, "persons define their nature, give meaning and coherence to their lives, and take responsibility for the kinds of person they are."[58] Professor Joseph Raz writes that "autonomous persons are those who can shape their life and determine its course. They are not merely rational agents who can choose between options after evaluating relevant information, but agents who can in addition adopt personal projects,

---

[54] Some scholars suggest Kant viewed them interchangeably. *See, e.g.*, Roger J. Sullivan, IMMANUEL KANT'S MORAL PHILOSOPHY 46 (Cambridge University Press, 1989) ("In Kant's moral theory it is usually possible to use the word "autonomy" in place of freedom.").

[55] Kant *supra* note 44, at 63 ("The concept of freedom is the key to the definition of autonomy of the will. The will is a species of causality of living beings, insofar as they are rational, and freedom would be that quality of this causality by which it can be effective independently of alien causes determining it; just as natural necessity is the quality of the causality of all beings lacking reason, of being determined to activity through the influence of alien causes. The proposed definition of freedom is negative . . .").

[56] Hill, *supra* note 38, at 255.

[57] Dworkin, *supra* note 40, at 20.

[58] *Id*.

develop relationships, and accept commitments to causes, through which their personal integrity and sense of dignity and self-respect are made concrete."[59]

a. Freedom from Coercion, Manipulation, and Deception

Kant's discussion on autonomy has been enormously influential, and scholars have wrestled with his outlay of autonomy since. In so doing, important themes have emerged. Notable among them is that autonomy assumes choice and decision-making – humans exercise autonomy by deciding our best path pursuant to some moral guide.[60] Two important caveats determine the quality of decision, however, and therefore the ability to express autonomy. For one, the choice must not be coerced.[61] In addition, one must operate in an environment in which the quality of options is sufficient for the individual to exercise meaningful choice.[62]

First, coercion is antithetical to autonomy, since "[a]ll coercion invades autonomy by subjecting the will of the coerced."[63]As Raz explains, coercion is A forcing B to do

---

[59] Joseph Raz, THE MORALITY OF FREEDOM 154 (Clarendon Press, 1986). Joel Feinberg broadly defines personal autonomy as "either (i) the capacity to govern oneself, which of course is a matter of degree; or (ii) the actual condition of self-government and its associated virtues; or (iii) an ideal of character derived from that conception; or (iv) (on the analogy to a political state) the sovereign authority to govern oneself, which is absolute within one's own moral "boundaries."" Joel Feinberg, *Autonomy, Sovereignty, and Privacy: Moral Ideals in the Constitution*, 58 NOTRE DAME L. REV. 445, 447 (1983).

[60] Raz, *supra* note 59, at 204 ("A person is autonomous only if he has a variety of acceptable options available to him to choose from, and his life became as it is through his choice of some of these options. A person who has never had any significant choice, or was not aware of it, or never exercised choice in significant matters but simply drifted through life is not an autonomous person.").

[61] *Id*.

[62] *Id*. at 155.

[63] *Id*.

something against B's will.[64] By doing so, A subjects B to A's will, thereby interfering with B's own process for determining B's own best path.[65] Raz notes that coercion can still be present even when the person being coerced does not regret the actions he or she takes; "[i]t is enough that he regrets the circumstances which make him do it."[66] Even if the action seems justified by some apparent logic, the reasoning can still amount to coercion: "It is justified if the reasons for it, including the threat of harm if it is not undertaken, defeat the reasons against it, including the fact that undertaking it amounts to submitting to coercion which violates the agent's autonomy."[67]

The second factor determining the quality of choice is the nature of options available. Raz explains that "[i]f having an autonomous life is an ultimate value, then having a sufficient range of acceptable options is of intrinsic value, for it is constitutive of an autonomous life that it is lived in circumstances where acceptable alternative are present."[68] Professor Thomas Hill similarly argues that even if an individual possesses the requisite features to exercise autonomy – chief among them "the psychological capacities for rational decision making" – the environment in which one operates can nevertheless constrain the ability to actually act autonomously.[69] Individuals, Hill explains, "though rationally disposed to make the best of their situation and unhindered

---

[64] *Id*. A more detailed articulation is provided at page 149.

[65] *Id*. at 154.

[66] *Id*.

[67] *Id*. at 151-52.

[68] *Id*. at 205.

[69] Hill, *supra* note 38, at 260-61.

by threats and manipulation by others . . . might be severely confined in the choices they could make by widespread poverty, disease, overpopulation, and absence of technology and culture."[70] A person's opportunity to live autonomously is reduced if, for example, "one has to labor in the fields all day to survive" even if that reality is no one's fault.[71] "The choice to labor may be perfectly rational, of course; but it may be almost the only rational choice one has a chance to make."[72] Raz argues that to produce meaningful choice, "[t]he criteria of the adequacy of the options available to a person must meet several distinct concerns. They should include options with long-term pervasive consequences as well as short-term options of little consequence, and a fair spread in between."[73]

Together, these two factors help form the contours of a definition of autonomy as a right, and not solely a value: the right to be free from undue coercion or manipulation by another.[74] Manipulation or deception distort the information one receives, thereby frustrating a person's process of determining, with their rationality, how best to respond

---

[70] *Id*.

[71] *Id*.

[72] *Id*. at 261 (1984). Raz expresses the same idea with his parable of the Hounded Woman, in which a woman is deserted on a small island shared only with a "fierce carnivorous beast." In a life of fear from the animal, the woman exerts all her intellectual ingenuity and will power to the struggle of how to survive, and thus lives without autonomy: while she operates with choice – she may have "medium and long-term options all dominated by her one overpowering need and desire to escape being devoured by the beast" – the choice is hollow "because a choice between survival and death is no choice from our perspective . . . For most of the time the choice should not be dominated by the need to protect the life one has." Raz, *supra* note 59, at 376. *See also* Julie Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1424 (2000) ("autonomy is radically contingent upon environment and circumstance.").

[73] Raz*, supra* note 59, at 376.

[74] Thomas Hill, *Autonomy and Agency*, 40 WM. & MARY L. REV. 847, 853 (1999).

and live one's life toward his or her guiding principles. Coercion results when one acts in some way that diverges from how he or she otherwise would act free from the influence.

b. Autonomy as a Normative Value

Humans are endowed with the basic tool of rationality, according to Kant, but autonomy is an end to strive for. To that end, Kant believed the role of government was to foster, protect, and nurture autonomy.[75] Government protects and nurtures autonomy through the enforcement of its laws, ensuring that one persons' self-development and exercise of autonomy do not impede others'.[76] And in codifying its citizens' social norms, moral duties, and expected behaviors, law bears its citizens' imprimatur.[77] Democracies thus seek to ensure that their citizens self-determination flourishes to the extent it does not infringe on others, and that the law and legislation serve as "the communicative framework for a rational political will formation," expressing "the common will of freely associated legal persons."[78]

---

[75] Sullivan, *supra* note 54, at 234.

[76] *See generally* Feinberg, note 59.

[77] Jurgen Habermas, BETWEEN FACTS AND NORMS: CONTRIBUTIONS TO A DISCOURSE THEORY OF LAW AND DEMOCRACY 105-06 (William Rehg trans., MIT Press, 1996) ("Moral theory supplies the overarching concepts: will and free choice, action and incentive, duty and inclination, law and legislation serve in the first place to characterize moral judgment and action . . . democracy should establish a procedure of legitimate lawmaking. Specifically, the democratic principle states that only those statutes may claim legitimacy that can meet with the assent . . . of all citizens in a discursive process of legislation that in turn has been legally constituted. In other words, this principle explains the performative meaning of the practice of self-determination on the part of legal consociates who recognize one another as free and equal members of an association they have joined voluntarily. Thus the principle of democracy lies at another level than the moral principle.").

[78] *Id*. at 111.

Following Kant's writing, western liberal political theory has considered autonomy a normative value for individuals to obtain and for governments to foster.[79] Democracies are founded on the "fundamental belief in the uniqueness of the individual, in his basic dignity and worth . . . and in the need to maintain social processes that safeguard his sacred individuality."[80] This individuality is a necessary ingredient in a democracy, which depends upon its citizens acquiring knowledge, using the knowledge to reason, and in turning their reasoned thoughts into beliefs acted upon to direct society. In order to maintain individuality, citizens must be free from manipulation or coercion.[81] Thus, autonomy is seen as a basic building block from which the whole system of representative democracy is built.

II. AUTONOMY IN AMERICAN LAW: LIBERTY, DIGNITY, AND PRIVACY

The word "autonomy" does not explicitly appear in the Constitution, but it is understood to be both embedded in the constitutional design and valued by the courts.[82]

---

[79] *See, e.g.*, John Rawls, A THEORY OF JUSTICE 513-20 (1971) ("A well ordered society affirms the autonomy of persons."). *See also* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1654 (1999) (democracy "requires individuals with an underlying capacity to form and act on their notions of the good in deciding how to live their lives. This anti-totalitarian principle stands as a bulwark against any coercive standardization of the individual."); Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 455 (1980) (describing "the moral autonomy of the citizen" as "a central requirement of a democracy.")

[80] Westin, *supra* note 1, at 33.

[81] *Id*. ("Psychologists and sociologists have linked the development and maintenance of this sense of individuality to the human need for autonomy – the desire to avoid being manipulated or dominated wholly by others.").

[82] James Fleming, *Securing Deliberative Autonomy*, 48 STAN. L. REV. 1, 3 (1995) (autonomy is "rooted" in "the language and design of our Constitution."); Winick, *supra* note 43, at 1707-08 ("respect for individual autonomy is deeply rooted in American constitutional history and tradition.").

Set amid British tyranny, the early American political thinkers formed a government based on the consent of the governed, in which citizens would form a representative democracy that respected their capacity and ability to govern themselves through a representative system.[83] The major threat to freedom and autonomy, at the nation's founding, "was the inability to have some say in the decisions that affected important aspects of one's life."[84] The Founding Fathers thus crafted a Constitution reflecting humans' innate capacity[85] to determine their best path "in pursuit of happiness."

As such an integral value of American governance, one might expect a robust "autonomy" jurisprudence to have developed.[86] However, no doubt influenced by the fact that the term does not appear in the U.S. Constitution, the Supreme Court has never recognized a specific "right to autonomy" nor developed a clearly bound jurisprudence around the term. As noted above, autonomy is simply too broad a term around which to develop a system of rights.[87]

---

[83] Perhaps the most well known manifestation of this demand for voice and consent was the colonists' cry for "no taxation without representation." *See* Jennifer Nedelsky, LAW'S RELATIONS: A RELATIONAL THEORY OF SELF, AUTONOMY, AND LAW 127 (Oxford University Press, 2011).

[84] *Id*.

[85] Thomas Jefferson, in particular, was influenced by the belief that the law of nature produced innately rational people capable of exercising autonomy. Garrett W. Sheldon, THE POLITICAL PHILOSOPHY OF THOMAS JEFFERSON, 42-6 (Johns Hopkins University Press, 1991).

[86] The Supreme Court has, at times, recognized autonomy as a fundamental value. *See, e.g., Jones v. Barnes*, 463 U.S. 745, 763 (U.S. 1983) (discussing "the values of individual autonomy and dignity central to many constitutional rights, especially those Fifth and Sixth Amendment."). The Supreme Court's jurisprudence of dignity and autonomy interests in the Bill of Rights is discussed more, *infra*.

[87] For instance, the Supreme Court balances "state autonomy" when weighing state versus federal law. *See, e.g., Garcia v. San Antonio Metro. Transit Auth.*, 469 U.S. 528, 549 (U.S. 1985) ("[The] Constitution of the United States . . . recognizes and preserves the autonomy and independence of the States – independence in their legislative and independence in their judicial departments.").

Instead, autonomy is valued, protected, and nurtured in American law by three separate (though often related) derivative values: liberty, dignity, and privacy. The sections below argue that autonomy manifested in action is considered liberty; that the space required to exercise autonomy is protected as privacy; and that autonomy itself, or self-determination, is protected as dignity. Each of these is similar, yet has key differences both conceptually and in American jurisprudence. Articulating the similarities and differences aids in ultimately identifying the unique harm victims suffer in the wake of data breaches.

a. Liberty

To say liberty is derivative of autonomy is a contentious claim, because Kant himself seemed to view them as similar, if not identical.[88] Yet since his time, philosophers and scholars have articulated important differences.

i. Relation to Autonomy

Liberty, unlike autonomy, is usually used to connote freedom of action as opposed to the process of deciding to do an intended action.[89] It is "a concept that applies to the desires and preferences a person has for particular states of affairs. It focuses on what the person wants to do at the level of action."[90] This is different from autonomy,

[88] *See supra* note 38.

[89] *See, e.g.*, Dworkin, *supra* note 40, at 105 (Liberty is "the ability to of a person to effectuate his decisions in action.").

[90] *Id*.

which is citizens' "capacity to reflect upon and adopt attitudes toward their desires, wishes, and values."[91]

Dworkin illustrates this difference by way of example. When we deceive a prisoner, we are interfering with his autonomy but not his liberty. The person who is "put into a cell and convinced that all the doors are locked (when, in fact, one is left unlocked) is free to leave the cell."[92] But "because he cannot – given his information – avail himself of this opportunity, his ability to do what he wishes is limited."[93] The prisoner is technically at liberty to leave, but by being duped into thinking all doors were locked, his autonomy is reduced, affecting his ability to be free.[94]

Conversely, an individual's liberty can be interfered with without violating that person's autonomy. Although examples of this dynamic may be difficult to imagine,[95] Dworkin offers another example, this time from *The Iliad*:

> Not wanting to be lured onto the rocks by the siren, Odysseus commands his men to tie him to the mast and refuse all later orders he might give to be set free. He wants to have his liberty limited so that he and his men will survive. Although his behavior at the time he hears the siren is not free – he struggles against his bonds and orders his men to free him – there is another aspect of his conduct that must be understood . . . He has a preference about his preferences, a desire not to act upon certain desires. He views the desire to steer his ship toward the sirens, and the rocks, as an alien desire. In limiting his liberty in accordance with his wishes we

---

[91] *Id*.

[92] *Id*.

[93] *Id*. at 14.

[94] *Id*.

[95] Perhaps because "we are used to focusing on cases where a person wishes to be free from interference, resents having his liberty taken away." *Id*. at 106.

> promote, not hinder, his efforts to define the contours of his life. We promote his autonomy by denying him liberty.[96]

This example clarifies the division between liberty (or freedom) and autonomy: liberty can be thought of as the freedom to act a certain way. Autonomy, on the other hand, can be described as the antecedent process one must undergo in order to freely decide whether to do a certain thing. In this way, freedom is dependent upon autonomy, and can be seen as a second-order value.[97] Conceptually, then, autonomy is often coupled with liberty, because one often decides some course of conduct (thereby exercising autonomy) and then actually acts upon that decision (exercising liberty). When applied to law, liberty can be seen as protecting autonomy by protecting whichever act stems from a decision-making process – in short, by protecting autonomy's physical manifestation.

ii. Liberty in American Law

It is difficult to understate the value of liberty in American law. The Constitution itself is intended to secure the "[b]lessings of [l]iberty,"[98] and the Fifth Amendment guarantees that citizens' liberty will not be deprived without due process of law.[99]

---

[96] *Id*. Joseph Feinberg offers another example: "The alcoholic . . . may have an intense desire to choose not to have another drink, but when his host returns with the bottle, he finds himself, to his despair, choosing contrary to his own wishes. Such a person may have freedom of action (for whatever that is worth), including political liberty (the law neither required nor prohibited another drink), but he lacked freedom of choice. He was free to act as he chose, but not free to choose as he wished." Feinberg, *supra* note 59, at 462.

[97] *Id*. ("The extent of our *defacto* freedom of action is determined not by any characteristics or powers of ourselves. Rather it is entirely a function of the circumstances in which we find ourselves. Insofar as those circumstances contain open options, just to that extent do we have freedom of action . . . A person has an open option in respect to some possible action, x, when nothing in his objective circumstances prevents him from doing x if he should choose, and nothing in his objective circumstances requires him to do x if he should choose not to.") (internal quotations omitted).

[98] U.S. Const., preamble.

[99] U.S. Const. amend IV.

Because of this explicit endorsement of liberty, it is fair to say Americans operate as though they can act in whichever way pleases them, so long as their actions cannot be said to infringe on another's autonomy or liberty.[100] The government protects this default presumption – that individuals are free to act according to their own desires – against the actions of other private actors through myriad laws, codes, regulations, and rules designed to deter harmful conduct. Against government coercion itself, the Due Process clause of the Fifth and Fourteenth Amendment commands that legislation tending to impinge liberty be "rationally related" to some "legitimate" government objective.[101]

Autonomy interests are especially evident, in the guise of liberty protections, when particularly significant decisions are made regarding how to conduct one's life. The Supreme Court's "due process" and "equal protection" decisions bear this out. The Fifth Amendment, prohibiting the government from depriving any person of life, liberty or property without "due process of law" was originally thought of as providing procedural protections only.[102] But the concept "expanded, particularly after the adoption of the Fourteenth Amendment in 1868, to protect substantive liberty and property interests from arbitrary governmental deprivation."[103] "Liberty," in particular, was expanded to protect

---

[100] This basic premise is echoed in John Stuart Mill's *On Liberty*, which influenced the Fourteenth Amendment, passed 9 years later. *See* John Stuart Mill, ON LIBERTY 13 (C. Shields ed., 1956) ("[T]he only purpose for which power can be rightfully exercised over any member of a civilized community, against his will, is to prevent harm to others. His own good, either physical or moral, is not a sufficient warrant . . . Over himself, over his body and mind, the individual is sovereign.").

[101] Heller v. Doe, 509 U.S. 312 (U.S. 1993).

[102] Winick, *supra* note 43, at 1717.

[103] *Id*.

various economic and personal liberties.[104] These included the upbringing of children, marriage, procreation, and other areas of personal life.[105] As Professor Bruce Winick notes, "[b]etween government and the individual, substantive due process carves out an area in which the individual is left substantially free to control important aspects of his or her own life."[106] In each of these realms of life – marriage, education, relationships – "liberty" interest protect both the capacity and ability for people to decide how to live their lives, while also protecting the concomitant action itself.

For example, in *Allgeyer v. Louisiana*,[107] decided shortly after the passage of the Fourteenth Amendment, the Supreme Court struck down a Louisiana statute on the grounds that it violated the plaintiff's "right to contract."[108] The Court held that the Fourteenth Amendment's "liberty" protected the plaintiff's right to "be free in the enjoyment of all his faculties," including the right "to use them in all lawful ways; to live and work where he will; to earn his livelihood by any lawful calling; [and] to pursue any livelihood or avocation."[109] Thus, liberty protected both the right to use one's faculties to

---

[104] *Id*. *See also* Immanuel Kant, PRACTICAL PHILOSOPHY 387 (ed. and trans. M. Gregor, 1996).

[105] Winick, *supra* note 43, at 1737 ("In a number of areas . . . by invoking either the rubric of "privacy" or the concept of "liberty" the Supreme Court has recognized that due process protects a zone of autonomous decision making in matters that are personal and intimate and of extreme importance to the individual – those matters dealing with marriage, procreation, contraception, abortion, family relationships, child rearing and education, occupation, residence, travel, and health.").

[106] *Id*. at 1743.

[107] Allgeyer v. Louisiana, 165 U.S. 578 (U.S. 1897).

[108] *Id*. at 591.

[109] *Id*. at 589.

decide how to live one's life – specifically, which profession to enter into – and the concomitant right to work in that profession free from certain constraints.

The right to autonomy is thus "a unifying theme that shows the coherence and structure of certain substantive liberties on a list of familiar unenumerated fundamental rights" such as those articulated under the Supreme Court's substantive due process jurisprudence.[110] The protection of autonomy through "liberty" is not confined to the Bill of Rights.[111] The foundation of private contract law, for example, is built on the notion of private autonomy and individual self-determination.[112] The government "recognize[s] the desirability of allowing individuals to regulate, to a large extent, their own affairs," granting individuals "the power to bind themselves by expression of their intent to be bound."[113]

b. Privacy

Privacy is also derivative of autonomy. Privacy joins autonomy and dignity as being notoriously difficult to define.[114] However, most definitions focus on secrecy, anonymity, or seclusion.[115] Each of these relate to the control a person has over his or her

---

[110] Winick, *supra* note 43, at 1743 (internal quotations omitted).

[111] *Id*. at 1753 ("the principle of autonomy also permeates much of American law outside of the Constitution.")

[112] *Id*. (noting the "strong commitment to individual autonomy . . . reflected in the history and development of the law of contracts.")

[113] *Id*.

[114] Judith Thomson quipped that "[N]obody seems to have any very clear idea what [it] is." *See* Judith Jarvis Thomson, *The Right to Privacy*, 4.4 PHIL. & PUB. AFFAIRS, 295 (1975).

[115] Ruth Gavison defined privacy as secrecy, anonymity, or seclusion. *See* Ruth Gavison, *Privacy and the Limits of Law* 89 YALE L. J. 421, 479 (1980).

accessibility to the outside world.[116] Secrecy and anonymity keep information and identity about oneself from others, while seclusion concerns the ability to keep some zone of self – either spatial or mental – to oneself.

i. Relation to Autonomy

Privacy protects and nurtures autonomy by giving people the space (secrecy, anonymity, or seclusion) needed to make decisions according to their own beliefs, and thereby engage in self-determination.[117] Professor Alan Westin spoke of privacy as a sort of cloak that protects the inner core of a person's autonomy: "only grave social need can ever justify destruction of the privacy which guards the individual's ultimate autonomy."[118] Professor Julie Cohen describes privacy as "shorthand for breathing room to engage in the processes of boundary management that enable and constitute self-development" thereby "foster[ing] (partial) self-determination."[119] Professor Clinton Rossiter speaks of privacy as a "special kind of independence, which can be understood as an attempt to secure autonomy in at least a few personal and spiritual concerns, if necessary in defiance of all the pressures of modern society."[120] Professor Ruth Gavison

---

[116] *See, e.g.*, Dworkin, *supra* note 40, at 103 ("Privacy consists of the ability of an individual to maintain control of the information about himself that is available to others."); Mark Alfino & G. Randolph Mayes, *Reconstructing the Right to Privacy*, 29 SOC. THEORY & PRACTICE 1, 8 (2003) ("Our basic view is that privacy is the condition of having secured personal space, personal space is the space a person requires to reason, and individuals have a fundamental moral right to reason as a means of securing personal autonomy.").

[117] *Id*. at 6 ("Privacy plays a fundamental and ineliminable role in constructing personal autonomy.").

[118] Westin, *supra* note 1, at 292. *See also id*. at 296 (referring to privacy as a "function" performed for personal autonomy).

[119] Julie Cohen, *What Privacy is For*, 126 HARV. L. REV. 1904, 1906 (2012).

[120] Clinton Rossiter, *The Pattern of Liberty, in* ASPECTS OF LIBERTY 15 (Konvitz and Rossiter eds., Cornell University Press, 1958).

too believes autonomy is furthered through the protection of privacy.[121] Professor Helen Nissenbaum writes that "insofar as privacy, understood as a constraint on access to people through information, frees us from the stultifying effects of scrutiny and approbation (or disapprobation), it contributes to material conditions for the development and exercise of autonomy and freedom in thought and action."[122]

Though privacy protects autonomy, the two are conceptually distinct.[123] This is because of the way privacy has been conceptualized, and the characteristics of privacy that have developed over time, such as anonymity, seclusion, or secrecy. For example, as Dworkin notes, deception can invade autonomy but not a person's privacy.[124] Deception corrupts information that a person receives, thereby interfering with that person's ability to decide upon a certain path – but it does not invade a person's privacy. Accordingly, deception is "just the opposite kind from that involved in interference with privacy. What is controlled is the information coming to you, not the information coming from you. I do not know something about you that you might wish to conceal [which would implicate

---

[121] *See* Gavison, *supra* note 115, at 423 (describing privacy as promoting "liberty, autonomy, selfhood, and human relations, and furthering the existence of a free society.").

[122] Helen Nissenbaum, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 82 (Stanford University Press, 2010). Conceptually, "if privacy is understood as the claim or right to control or determine access to information about oneself, and autonomy is understood as self-determination embodied in the individual whose actions are governed by principles that are his own, and who subjects his principles to critical review, rather than taking them over unexamined form his social environment, then privacy is, in fact, partially constitutive of autonomy . . . privacy is to be understood as a form of autonomy, [as] self-determination with respect to information about oneself." *Id*. at 81 (internal quotations omitted).

[123] Dworkin, *supra* note 40, at 104 ("[A]lthough privacy may be related to autonomy in a number of ways it is not identical with it.").

[124] *Id*.

privacy]. I conceal something from you that you might wish to know."[125] Thus, autonomy is diminished, but not privacy.

ii. Privacy in American Law

Privacy is not mentioned in the Constitution. Yet, the Constitution grants a right to privacy, the invasion of privacy is a well-recognized tort, and myriad legislation has been enacted in the name of privacy. This robust presence can be fairly traced to one law review article.

Samuel Warren and Louis Brandeis' *The Right to Privacy*[126] has been considered the spring of privacy law in the United States.[127] Writing in 1890, Warren and Brandeis set forth an argument for why man enjoyed a "right to be let alone," and explained how this right was being infringed upon by "[i]nstantaneous photographs and newspaper enterprise" that were invading "the sacred precincts of private and domestic life."[128] The authors argued that man, "under the refining influence of culture," had become "more sensitive to publicity" such that "solitude and privacy" had become more valuable.[129] At the same time, society, with its new technology and gossip press, was encroaching on this privacy interest as it had not before. The authors argued that common law, in its "eternal

---

[125] *Id*. at 105.

[126] Samuel Warren and Louis Brandies, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890)

[127] *See, e.g.*, Benjamin E. Bratman, *Brandeis and Warren's The Right to Privacy and the Birth of the Right to Privacy*, 69 TENN. L. REV. 623, 624 (2002) (framing "The Right to Privacy" as the "seminal force in the development of a 'right to privacy' in American law.") *But see* Daniel J. Solove & Neil M. Richards, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123 (2007) (arguing that "The Right to Privacy" reflected a divergence from the privacy-protecting law of confidentiality).

[128] Warren & Brandeis, *supra* note 126, at 195.

[129] *Id*. at 193, 196.

youth" had evolved to protect not merely physical property and liberty interests, but also intellectual ones.[130] So too, they argued, could it protect individuals' "right to be let alone."[131]

Since their influential writing, courts slowly began to develop jurisprudence around this newfound "right to privacy." In 1960, Dean Prosser, an influential legal scholar, grouped together the cases and eventually formulated the "Invasion of Privacy" tort, itself composed of four distinct torts: Intrusion upon seclusion or solitude, or into private affairs; public disclosure of embarrassing private facts; publicity which places a person in a false light in the public eye; and appropriation of name or likeness.[132] These torts exist at common law today in many states, and continue to be used in myriad scenarios to protect individuals' privacy interests – including in the data breach context. Prosser stated that the interest protected in each tort was, in the intrusion cases, the interest in freedom from mental distress; in the public disclosure and "false light" cases, the interest in reputation; and in the appropriation cases, the proprietary interest in name and likeness.[133]

---

[130] *Id*. at 194 ("[I]n very early times, the law gave a remedy only for physical interference with life and property, for *trespasses vi et arrmis*. Then the "right to life" served only to protect the subject from battery in its various forms; liberty meant freedom from actual restraint; and the right to property secured to the individual his lands and his cattle. Later, there came a recognition of man's spiritual nature, of his feelings and his intellect. Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life -the right to be let alone.").

[131] *Id*.

[132] *See* Prosser, *Privacy*, 48 CALIF. L. REV. 383 (1960).

[133] Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 967 (1964) (citing Prosser, *supra* note 132).

Although the Constitution does not explicitly contain the term "privacy," the Supreme Court has found that the Constitution bestows a right to privacy. In *Griswold v. Connecticut*, the Supreme Court held that Bill of Rights contained "penumbras," creating "zones of privacy."[134] These penumbral privacy zones included the First Amendment's right of association, the Third Amendment's prohibition against the quartering of soldiers, the Fourth Amendment's right to be secure against unreasonable searches and seizures, and the Fifth Amendment's Self-Incrimination Clause, "enable[ing] the citizen to create a zone of privacy which government may not force him to surrender to his detriment."[135]

This Constitutional right to privacy arguably extends to so-called "informational privacy." In *Whalen v. Roe*, plaintiffs challenged a government program that retained identifying information of patients who had been prescribed certain drugs in a centralized file.[136] The plaintiffs argued that the program violated their Constitutional right to privacy.[137] The Court held that the program did not constitute an invasion "of any right or liberty protected by the Fourteenth Amendment."[138] In so doing, the Court noted that the government had the authority to collect certain sensitive information, but that the power is "typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures" and that the duty also "arguably has its roots in the

---

[134] Griswold v. Connecticut, 381 U.S. 479, 484 (U.S. 1965).

[135] *Id*.

[136] Whalen v. Roe, 429 U.S. 589 (U.S. 1977).

[137] *Id.* at 598.

[138] *Id.* at 603-04.

Constitution."[139] Since *Whalen*, the circuit courts have taken various stances toward this right to informational privacy.[140]

Finally, various statutes have been enacted with the goal of protecting peoples' privacy. These include those designed to maintain the confidentiality of certain information,[141] to prevent wiretapping and eavesdropping,[142] and to protect personal zones of seclusion, free from interference by the outside world.[143]

c. Dignity

The final derivative value of autonomy is dignity. Dignity is an ethereal, capacious concept, but its basis lies "in the autonomy of self and a self-worth that is reflected in every human being's right to individual self-determination."[144]

Dignity is ancient, tracing back to Cicero who believed "all human beings were endowed with *dignitas*, and that therefore all mankind is worthy of respect for the sole

---

[139] *Id.* at 605. *See also* National Aeronautics and Space Administration v. Nelson, 131 S. Ct. 746 (2011) ("We assume, without deciding, that the Constitution protects a privacy right of the sort mentioned in *Whalen* . . .").

[140] *Compare* AFL-CIO v. Dept. of Housing & Urban Dev., 118 F.3d 786 (D.C. Cir. 1997) (expressing "grave doubts as to the existence of a constitutional right of privacy in the nondisclosure of personal information.") *with* United States v. Westinghouse Elec. Corp., 638 F.2d 570, 578 (3d Cir.1980) (recognizing the right and applying a multifactor test to determine whether the government has invaded it).

[141] *See, e.g.*, Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2006) (protecting confidentiality of video rental records); Gramm-Leach-Bliley Act of 1999, 15 U.S.C. § 6809(4)(A) (2006) (protecting the confidentiality of financial information.)

[142] *See, e.g.*, Stored Communications Act, 18 U.S.C. § 2701.

[143] *See, e.g.*, Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227 (Congressional finding that "Unrestricted telemarketing . . . can be an intrusive invasion of privacy.").

[144] Rex Glensy, *The Right to Dignity*, 43 COLUM. HUM. RTS. L. REV. 65, 68 (2011). *See also* Immanuel Kant, FOUNDATIONS OF THE METAPHYSICS OF METAPHYSICS OF MORALS 54 (Lewis White Beck trans., 1983) ("Autonomy is thus the basis of the dignity of both human nature and every rational nature.").

fact of its existence."[145] *All* humans were endowed with dignity, according to Cicero, simply because of our "superior minds" which allowed for our self-awareness.[146] Through the ages, Cicero's view was eclipsed first by the Roman elite, which had vested interests in conceptualizing dignity not as a universal trait but as an acquired one, indicative of "high social or political status."[147] Then during the Renaissance, religious authorities regarded dignity as endowed in each of us, but as a gift from God, as humans made in His image.[148]

i. Relation to Autonomy

Kant, regarded as the father of the modern concept of dignity, secularized the concept of dignity and articulated it "as a normative legal ideal."[149] Like Cicero, Kant believed humans possessed dignity stemming from rationality, but differed from Cicero in that he "formulated reason as the ability of humans to appreciate the implications or universality of their actions."[150]

Kant believed dignity was an outgrowth of autonomy, and that an affront to autonomy would therefore be an indignity. His first Categorical Imperative instructs people to "act only according to principles which can be conceived and willed as a

---

[145] Glensy, *supra* note 144, at 76 (citing Cicero, DE OFFICIIS I 30 (William McCartney ed., Edinburgh 1798) (1481)).

[146] Glensy, *supra* note 144, at 76.

[147] *Id*.

[148] *Id*. at 74-5. This remains a core belief. *See, e.g.*, Catholic Church, *The Dignity of the Human Person*, *in* THE CATECHISM OF THE CATHOLIC CHURCH (2nd ed., 1700) ("The dignity of the human person is rooted in his creation in the image and likeness of God.").

[149] Glensy, *supra* note 144, at 76.

[150] John D. Castiglione, *Human Dignity Under the Fourth Amendment*, 2008 WISC. L. REV. 655, 678.

universal law."[151] Derivatively, his second implores individuals to "[a]ct in such a way that you treat humanity, whether in your own person or in the person of any other, always at the same time as an end and never simply as a means."[152] As John Castiglione notes, violating the second precept affronts human dignity "because every individual has a right to be treated as an end, not as a means."[153] Thus, dignity "can be conceived as the inherent right of all men to be treated by others in accordance with the categorical imperative. Failure to be so treated is an offense against dignity."[154] Roger Sullivan casts Kant's second imperative as the Formula of Respect for the Dignity of Persons.[155]

In addition to being a status inhering in each person as a product of his or her rationality, dignity also accrues from the exercise of that rationality free from undue interference – in short, from the exercise of autonomy.[156] Thus, actions that restrict the exercise of autonomy – coercion, deception, or manipulation – are said to violate a person's dignity.

---

[151] Immanuel Kant, FOUNDATIONS OF THE METAPHYSICS OF MORALS 54 (Lewis White Beck trans., 1983).

[152] *Id*.

[153] Castiglione, *supra* note 150, at 678.

[154] *Id*.

[155] Sullivan, *supra* note 54, at 195. Sullivan writes that "The imperative that we should act only maxims capable of being universal laws, [according to Kant], inevitably will lead to our recognizing that we must respect every human person as having objective and intrinsic worth or dignity." *Id*. at 193.

[156] Darwall, *supra* note 41, at 275 ("The very idea of a claim to autonomy thus implies the authority to make the claim second-personally. And if we see this claim as inherent in the equal *dignity* of persons, we are consequently committed to accepting that dignity includes a second-personal authority, specifically, that it *includes the authority to demand respect for autonomy* and to hold one another accountable for complying with this demand. We must see ourselves as accountable to one another as members of the moral community for respecting others' autonomy and as distinctively accountable to those whose autonomy we threaten or violate.") (emphasis added).

ii. Dignity in American Law

Unlike liberty, "dignity" does not appear in the Constitution.[157] Nonetheless, the Supreme Court has used the term often,[158] and proclaimed that "[f]rom its founding the Nation's basic commitment has been to foster the dignity and well-being of all persons within its borders."[159]

Professor Maxine Goodman, in a survey of the Supreme Court's use of the term, found that the Court had "expressly linked human dignity to certain constitutional claims, either by grounding the Court's decision in the need to advance human dignity or by expressly rejecting human dignity concerns in favor of competing state interests."[160] As Professor Rex Glensy notes, the Supreme Court's use of the term seems to point to two separate conceptualizations of dignity – each of which can be tied to Kantian conception

---

[157] Notably, though, the very first Federalist Paper called for the Constitution to ensure "liberty," "dignity" and "happiness" of the people. *See* Glensy, *supra* note 144, at 77 (quoting THE FEDERALIST NO. 1, 4 (Alexander Hamilton) (Clinton Rossiter ed., 1999)).

[158] *See generally* Maxine D. Goodman, *Human Dignity in Supreme Court Constitutional Jurisprudence*, 84 NEB. L. REV. 740 (2006).

[159] *Goldberg v. Kelly*, 397 U.S. 254 (1970).

[160] Goodman found that the cases fell into eight categories: "1. Fourteenth Amendment liberty interest, and corresponding right to privacy, regarding marriage, contraception, intimate acts, and procreation; 2. Fourteenth Amendment equal protection under the law regarding equal access to education and accommodations; 3. Fifth Amendment protection against a person in a criminal case serving as a witness against himself; 4. Fourth Amendment protection against unreasonable searches and seizures; 5. Eighth Amendment protection against cruel and unusual punishment; 6. An individual's ability under the Fourteenth Amendment Due Process or Equal Protection Clause to choose how and when to die when death is imminent; 7. Fourteenth Amendment due process or equal protection right to economic assistance from the government; and 8. First Amendment freedom of expression and the opposing right of an individual to protect his public image, as against another's First Amendment freedom of speech." Goodman, *supra* note 158, at 757.

of dignity as (a) a fundamental byproduct of human rationality; and (b) a status achieved through self-determination.[161]

1. Treating a person with decency

First, dignity is employed in the Fourth and Eighth Amendment contexts as a measure of a minimum threshold of respect each individual is due, often with a physical aspect. In *Hope v. Pelzer*, the Supreme Court ruled that tying a prisoner to a hitching post in the sun for more than seven hours, supplying him with little water, and preventing him from going to the toilet was a violation of the Eighth Amendment protection against cruel and unusual punishment.[162] The punishment was "antithetical to human dignity" because it was "degrading and dangerous."[163] As Glensy notes, the Court "focused on the demeaning aspect of the punishment, which included taunting and wanton humiliation of the prisoner."[164] This sense of dignity is Kantian in its dictate that people – even heinous criminals – "not be treated as objects."[165] But it does not seem to implicate the Kantian imperative of free choice so central to autonomy. The prisoner who is tied up to the post has his liberty restricted, to be sure, but he is arguably as autonomous as he was before being tied up.[166]

---

[161] Glensy, *supra* note 144, at 89.

[162] Hope v. Pelzer*,* 536 U.S. 730, 745 (2002).

[163] *Id*.

[164] *Id*.

[165] *Id*.

[166] *See supra*, note 89.

The same goes for the Court's conception of dignity in the Fourth Amendment context. The Court has framed the Fourth Amendment's "overriding function" as being "to protect privacy and dignity against unwarranted intrusion by the State" and "characterize[s] police behavior as offensive to human dignity when it [rises] to the level of shocking even those of hardened sensibilities."[167] Here too, the dignity the Court refers to seems less about being free to decide one's best course of action – autonomy as self-definition – and more about the government displaying a basic modicum of respect to individuals. This conception of dignity, as Glensy notes, is "dignity as basic decency."[168] Glensy makes the point that in each of these cases, "the actions complained of actually invaded the physical body of the individual – indeed, in each case, the actions included forcibly going *inside* the body of the person. Thus, dignity in this context is paired with physical integrity."[169]

2. Freedom from coercion or deception

The second use of "dignity" in the Court's jurisprudence is more closely linked to self-determination and the freedom to determine one's path in life. In its substantive due process cases, the Court "equates dignity with the respect owed to the core characteristics of an individual's personality and . . . the expression of those characteristics."[170] Most

---

[167] Glensy, *supra* note 144, at 89 (quoting Rochin v. California, 342 U.S. 165, 172, 174 (1952)) (quotations omitted).

[168] *Id*. at 93.

[169] *Id*. at 90. This is similar to the German conception of dignity as "respect of physical identity and integrity," delineated in Article 2(2) of the German Constitution. *See* Edward J. Eberle, *Human Dignity, Privacy, and Personality in German and American Constitutional Law*, 4 UTAH L. REV. 963, 975 (1997).

[170] Glensy, *supra* note 144, at 90.

notably, in *Lawrence v. Texas*, the Court invalidated an anti–sodomy statute on due process grounds.[171] The majority could have ruled on other grounds, but instead invoked dignity by holding that the statute interfered with "the most intimate and personal choices a person may make in a lifetime, choices central to personal dignity and autonomy," protected by the Fourteenth Amendment.[172] In contrast to the dignity as basic decency, described above, these dignity invocations can be seen as protecting people's ability to conduct their life as they see fit.[173]

Invocations of dignity harms appear in other situations where a person's decisional autonomy is at stake. Among state constitutions, the Montana Constitution is unique in recognizing dignity, stating in Article II, section 4 that "the dignity of the human being is inviolable."[174] Plaintiffs most frequently cite to this "dignity clause" to argue that the state government has not protected basic decency requirements for prisoners – reflecting the conception of dignity related to self-respect but less to do with decision-making and control of one's choices.[175] However, in *Oberg v. City of Billings*, a police officer challenged the Department's requirement that he take a polygraph test for

[171] Lawrence v. Texas, 539 U.S. 558, 558 (2003).

[172] *Id.* at 574.

[173] Glensy, *supra* note 144, at 93 (describing this as "dignity as autonomy").

[174] Mont. Const., Art. II § 4. Two other state constitutions explicitly reference dignity: Illinois and Louisiana. The language is "purely hortatory," however, and not used to create a cause of action as it has been in Montana. *See* Vicki C. Jackson, *Constitutional Dialogue and Human Dignity: States and Transnational Constitutional Discourse*, 65 MONT. L. REV. 15, 21, fn. 21 (2004).

[175] *Id*.

employment as violating the dignity clause.[176] The court sided with the officer, striking down the lie-detector test on other grounds,[177] but also noted that the requirement could have been invalidated under the dignity clause because "subjecting one to a lie detector test is an affront to one's dignity."[178] Although the court's rationale was unexplained, this conclusion would seem to align with a Kantian conception of indignity as violating one's self-determination; restricting a person's right to control which information they withhold and extracting their own thoughts from him or her violates self-determination.[179]

Dignity also appears as a value to be protected, not just against government action (as in the Eighth and Fourth Amendment context described above) but also against private actors. The most prominent example may be so-called "Death with Dignity" laws, which, generally speaking, allow a person to permit physicians to prescribe lethal medications to him or her, such that the person controls the decision to end his or her own life.[180] Dignity also pervades the legal concept of informed consent, wherein a person is

---

[176] Oberg v. Billings, 207 Mont. 277, 285 (Mont. 1983).

[177] *Id*.

[178] *Id*.

[179] *See Criminal Justice, New Technologies, and the Constitution*, U.S. CONGRESS, OFFICE OF TECHNOLOGY ASSESSMENT, 9 (May 1988) ("Emerging technologies based on molecular biology may reveal some of the causes of violent, aggressive, and antisocial behavior. They could also be used to manipulate or control behavior, and this would risk violations of individual autonomy.").

[180] *See, e.g.*, Oregon Death with Dignity Act, ORS § 127.800 *et seq*. For an overview of Death with Dignity legislation, see Mike DeBonis, *Death With Dignity' laws are proposed, bringing national debate to D.C. and Md.*, WASH. POST (Jan. 16, 2015), http://www.washingtonpost.com/local/dc-politics/death-with-dignity-laws-are-proposed-bringing-national-debate-to-dc-and-md/2015/01/16/8354bba8-9d09-11e4-a7ee-526210d665b4_story.html.

entitled to all relevant information that could influence his or her decision to agree to something.[181]

d. Dignity and Privacy: Similar, But Not the Same

The above sections have endeavored to explain how liberty, privacy, and dignity are conceptualized, and how each appears in American law. To review, liberty can be seen as autonomy in action; privacy, as a protective condition conducive to the exercise of autonomy; and dignity as autonomy itself, in terms of being both (a) a byproduct of peoples' rationality (mandating a threshold level of respect due each person) and (b) a status achieved through the exercise of rationality to make autonomous choices (mandating non-interference with peoples' decision-making processes).

In concluding this section, two further points are necessary, which are important to the later analysis of data breach harms. First, every violation of privacy is also an invasion of a person's autonomy, but the converse is not true. Second, compared to liberty and privacy, dignitary harms are more difficult to identify. Each of these points causes privacy harms to be more easily recognized than dignitary harms.

i. Dignity Harms Are The Least Observable

Liberty and privacy violations are easily observable. The freedom to do some thing or act in a certain way, when restricted, is visible. To take a well-known example, the freedom to "bear arms" when circumscribed, or denied outright, is fairly obvious: the

[181] Dworkin, *supra* note 40, at 5 ("All discussions of the nature of informed consent and its rationale refer to patient (or subject) autonomy. Conflicts between autonomy and paternalism occur in cases involving civil commitment, lying to patients, refusals of life-saving treatment, suicide intervention, and patient care.").

person is no longer (legally) able to carry a certain firearm in a certain location[182] or to carry one at all.[183] Privacy invasions, while more abstract, are also relatively easy to perceive. When a person invades another's home, the homeowner's spatial seclusion is trespassed.[184] When a person discloses some information about another the latter desired to keep secret, that person has exposed that person against his or her wishes.[185] These characteristics of liberty and privacy make them easily protectable in law.

Violations of dignity (or "indignities") are comparatively opaque. Unlike liberty, person A can violate person B's dignity without restraining some action or conduct of B's.[186] Similarly, person A can violate person B's dignity without harming their privacy.[187] Because indignities often involve coercion, deception, or manipulation – none of which are necessarily physical or spatial – indignities can be comparatively more difficult to identify.

---

[182] *See, e.g.*, Minn. Stat. 641.165 (forbidding the carrying of a firearm in any jail, lockup, or correctional facility).

[183] *See, e.g.*, Minn. Stat. 609.67 (restricting the right to own certain types of assault weapons and shotguns).

[184] Time, Inc. v. Hill, 385 U.S. 374, 413 (U.S. 1967) ("[t]his Court held that the doctrines of the Fourth and Fifth Amendments apply to all invasions on the part of the government and its employees of the sanctity of a man's home and the privacies of life.").

[185] Espinoza v. Hewlett-Packard Co., No. 6000-VCP 2011 Del. Ch. LEXIS 45, at *22 (Del. Ch. Mar. 17, 2011) ("California common law recognizes the tort of public disclosure, one of four distinct torts that fall within the collective rubric of invasion of privacy. This tort is distinct from a suit for libel or "false light" because the claimant need not challenge the accuracy of the information disclosed to the public, but rather, must show that the disclosure is so intimate and unwarranted as to outrage the community's notion of decency.").

[186] For example, through the use of deception, which interferes with a person's decision-making process but does not necessarily restrain their action in anyway.

[187] For example, through the use of coercion, deception, or manipulation, one can hinder a person's autonomy that in no way affects that person's privacy.

ii. Every Privacy Invasion Violates Autonomy

As noted above, privacy is a seen as related to autonomy in the sense that, without privacy, one can be frustrated in his or her ability to live his or her life free from undue external influences – in short, to live autonomously. Because of this relationship, wherein "privacy is constitutive of autonomy,"[188] every violation of privacy is a therefore a violation of autonomy. If one's control of oneself is invaded, either in a spatial or intellectual sense, he or she is less able to determine his or her best path free from an unwanted influence.

It is worth noting that philosophy and law diverge on this point. Dworkin, for example, would disagree with the notion that every privacy violation also violates one's autonomy. Dworkin proffers the example of wiretapping or eavesdropping: "[i]f someone taps your phone conversations without your knowledge he interferes with your privacy. But your decisions, your actions, your values, are in no way changed or altered from what they might be otherwise. You are as self-determining as ever."[189] At a conceptual level, it may be true to say privacy has been invaded in this situation. Legally, however, this is not the case, because one must be aware of the surveillance in order for the invasion to occur.[190] Of course, as a matter of pure logic, in order to bring a complaint, a person who

---

[188] Nissenbaum, *supra* note 122, at 81 (describing the view that "privacy is, in fact, partially constitutive of autonomy . . . privacy is to be understood as a form of autonomy, [as] self-determination with respect to information about oneself.").

[189] Dworkin, supra note 40, at 104.

[190] *See* Gavison, *supra* note 115, at 457 ("It is . . . difficult to know when one's communications have been intercepted, when one is being observed or followed, or when others are reading one's dossier. This absence of awareness is a serious problem in a legal system that relies primarily on complaints initiated by victims.").

feels that his or her privacy was invaded must be aware of the invasion. But this understanding of privacy has also been codified and is well understood in privacy law. The Privacy Act of 1974,[191] for instance, prohibits the government from sharing information about citizens, but it requires that a third party actually view the information in order to trigger rights of the subject to sue.[192] And courts generally hold that privacy invasions require actual viewership of the information one seeks to protect.[193]

These points are raised because they point to a reality that is relevant in the data breach context: invasions or violations of privacy are more visible harms than affronts to dignity. The trappings of privacy law that make privacy harm easy to observe – such as spatial seclusion or publication of private facts – are not necessary for one's dignity to be violated.

[191] 5 U.S.C. § 552a.

[192] 5 C.F.R. § 297.102 (Under the Privacy Act, "[d]isclosure means providing *personal review* of a record, or a copy thereof, to someone other than the data subject or the data subject's authorized representative, parent, or legal guardian.") (emphasis added).

[193] In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 28 (D.D.C. 2014) ("For a person's privacy to be invaded, their personal information must, at a minimum, be disclosed to a third party. Existing case law and legislation support that common-sense intuition: If no one has viewed your private information (or is about to view it imminently), then your privacy has not been violated.").

FIGURE 1

	Definition	Unique from 1	Unique from 2	Unique from 3
1. Liberty	The ability to effectuate decision in action[194]		Privacy elements are not required.	Requires restraint of some human action.
2. Privacy	Secrecy, anonymity, seclusion[195]	Does not require restraint of some human action.		Privacy elements are required; privacy harms require victims awarneness.
3. Dignity	(a.) Decency; treating a person as an end, not a means;[196] (b.) Freedom from coercion, manipulation, or deception.[197]	Does not require restraint of some human action.	Privacy elements are not required.	

e. Summary

In concluding, this Part seeks to demonstrate that liberty, dignity, and privacy are three values or normative goals in American law that protect and nurture autonomy. Liberty is explicitly stated as a normative value in the Constitution. Privacy has also been established as a fundamental right through the Supreme Court's substantive due process jurisprudence and the development of the Invasion of Privacy tort. Lastly, dignity has

[194] Dworkin, *supra* note 40, at 105.

[195] Gavison, *supra* note 115, at 438.

[196] Castiglione, *supra* note 150, at 688-89.

[197] Hill, *supra* note 74, at 853.

also been recognized as a fundamental value and as protective of autonomy. Unlike liberty, however, it is not concerned with the ability of a person to take some action. In addition, the familiar trappings of privacy, as laid out in the invasion of privacy tort – secrecy, anonymity, and spatial seclusion – are absent.

In the following Part, this thesis argues that data breaches vividly expose this dynamic. Having one's PII made vulnerable (but not used) does not keep one from doing something he or she would otherwise do. It is not accurate to say a person's liberty has been robbed. In addition, privacy is not usually a contestable legal issue because viewership of the data is often difficult, if not impossible to prove. But dignity, as has been shown, does not require the restraint of action nor the distinct privacy characteristics. Data breaches are unique in causing a dignitary harm which, as explained below, occurs in being placed in a vulnerable, weakened state.

PART II

III. ANALYSIS: DATA BREACH HARM

This thesis now seeks to apply this understanding of autonomy to the data breach context, returning to answer the Research Questions: What is the harm that occurs to individuals where their data has been made vulnerable because of a breach, but who have not become victims of identity theft? What is the nature of that harm? Secondly, does this harm merit legal redress? In answering these questions, this Part dissects each sequence of events that compose a data breach: (1) the disclosure of the PII; (2) the security or insecurity of the PII; and (3) the breach itself.

a. The Disclosure of PII

A data breach can't happen without data, and cyber thieves wouldn't bother with hacking were it not for the value of the information. The first meaningful element of a data breach is disclosure of individuals' PII. Is this release of PII harmful in and of itself? This section argues that consent to the release of PII is dubious where it is coerced by practical necessity. However, while consent is important, non-consent is normally not grounds for legal redress in and of itself; instead, non-consent is dependent on some later harm to occur.

i. Consent and Coercion

The release of PII is, at least in a basic sense, completely free and voluntary. Indeed, release of PII is an almost mundane part of everyday life – and some individuals

eagerly release PII in return for whatever benefit might attach.[198] The Information Age is, after all, fuelled by the benefits it provides to both company and consumer. The collection, aggregation, and analysis of individuals' personal information allow companies to direct their marketing to specific demographics and target audiences, thereby increasing revenue.[199] But it also provides better services to the individual customer, creating consumer preference and loyalty.[200]

Yet, although individuals may agree to disclose their PII, two prerequisites of autonomy, discussed above, come into play: freedom from coercion and quality of choice. Are people actually acting autonomously when the choices they make occur in an environment with few or no practical alternatives? Consent implies the possibility of refusal,[201] and refusal to release PII today, while technically possible, would leave

---

[198] A. Michael Froomkin, *The Death of Privacy*, 52 STAN. L. REV. 1461, 1502 (2000) ("[E]ven Americans who place a high value on information privacy will sell their privacy bit by bit for frequent flyer miles."). *See also* Julie Cohen, *What Privacy is For*, 126 HARV. L. REV. 1904, 1916 (2012). Donald Michael noted as early as 1963 that individuals would likely desire "central data files" so that they can "acquire quickly those conveniences that flow from a reliable credit rating and an acceptable social character" and that "we can expect a great deal of information about the social, personal, and economic characteristics of individuals to be supplied voluntarily – often eagerly." *See* Westin, *supra* note 1, at 313 (quoting Donald Michael, *Speculations on the Relation of the Computer to Individual Freedom and the Right to Privacy*, GEO. WASH. 33 L. REV. 275 (1964)).

[199] Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1403-09 (2001) (discussing the rise of individualized marketing).

[200] *See* Kent Walker, *Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange* 2000 STAN. TECH. L. REV. 2, 39, 46, 48 (2000) ("Having some information about ourself out there in the world offers real convenience that goes beyond dollars and cents. Many people benefit from warehousing information - billing and shipping addresses, credit card numbers, individual preferences, and the like - with third parties. Such storage of information can dramatically simplify the purchasing experience…").

[201] Edward Jange & Paul Schwartz, *Notice, Autonomy, and Enforcement of Data Privacy Legislation: The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1248 (2002).

individuals in an untenable position, without a bank account or the use of modern forms of payment like credit cards, for example.

The current environment, in which merchants, banks, Internet providers, constantly collect personal information, also limits the quality of choice.[202] Professor Paul Schwartz presciently explained, more than a decade ago, how the Information Age architecture can impede meaningful consent to the release of PII. Schwartz noted how the "liberal ideal" perspective assumed that individuals could protect their privacy (and thus autonomy) by controlling access to their personal information.[203] The reality, Schwartz was beginning to see, was that a power imbalance between the individual and the entities who collected the information produced an environment in which individuals had little choice but to reveal certain information to private actors.[204] The ability to keep data secure to oneself, Schwartz noted, "quickly proves illusory because of the demands of the Information Age."[205]

Schwartz illustrated this point by outlining four problems with meaningful control of PII. First, the "knowledge gap": a "widespread ignorance regarding the terms that regulate disclosure or nondisclosure of personal information."[206] Second, the "consent

---

[202] Cohen, *supra* note 119, at 1430 ("Certain industries do require the exchange of personally-identified data in order to function. Prominent examples include the credit reporting, health care and biomedical research, insurance and financial services, and higher education industries.").

[203] Schwartz, *supra* note 79, at 1662.

[204] *Id*.

[205] *Id*.

[206] *Id*. at 1660.

fallacy" which consists of "weaknesses in the nature of agreement to data use."[207] And third, the "autonomy trap."[208] Schwartz' discussion of the autonomy trap is particularly relevant in the context of data breaches. Schwartz noted that "the organization of information privacy through individual control of personal data rests on a view of autonomy as a given, preexisting quality."[209] The problem with privacy-control in the Information Age, though, "is that individual self-determination is itself shaped by the processing of personal data."[210]

As an example, Schwartz discussed the online "click wrap" agreement. As Schwartz explained, clicking through a consent page "may be considered by some observers to be an exercise of self-reliant choice" online.[211] But the screen could (and often does) contain boilerplate language permitting "all further processing and transmission of one's personal data."[212] Faced with a choice between consenting to the recipients' desired use of their information, and being blocked from, say, using a credit card, individuals inevitably provide consent – but the consent reflects the power imbalance between the parties. In Schwartz' example, this produces a "legal fiction that all who visit [a] Web site have expressed informed consent to its data processing

---

[207] *Id*.

[208] *Id*.

[209] *Id*.

[210] *Id*.

[211] *Id*. at 1661.

[212] *Id*.

practices."[213] Thus, Schwartz' autonomy trap refers to the quality of choice and the implications for consent.

Schwartz originally wrote about individuals' consent to data processing and use, but his argument easily carries over, in the data breach context, to how information is protected. As with the use of their PII, individuals also consent to the release of their PII but, currently, have little to no leverage in demanding certain levels of protection. Some federal statutes – notably, the Health Insurance Portability and Accountability Act (HIPPA), the Gramm-Leach-Bliley Act, and the Federal Information Security Management Act (FISMA) – *do* require certain security standards.[214] But these statutes operate as exceptions, instead of the rule – unless the information fits within one of the relatively narrow categories, no single law grants citizens the power to demand a certain level of protection.[215] Perhaps not suprisingly, Americans seem to be losing faith in the degree to which their information actually is adequately protected. A recent Pew survey, for example, found that "[a]cross the board, there is a universal lack of confidence among adults in the security of everyday communications channels—particularly when it comes to the use of online tools."[216]

---

[213] *Id*.

[214] *See* 45 CFR parts 160, 162, and 164 (security rule relating to HIPPA); 16 CFR Part 314 ("Safeguards Rule" applying to Gramm-Leach-Bliley Act); 44 U.S.C. § 3542 (requiring federal agencies to develop and implement security programs for the protection of data).

[215] Although some federal laws do mandate "reasonable" levels of security, enforceable by the FCC (*see* Communications Act, 47 U.S.C. §§ 201, 222) and FTC (15 U.S.C. § 45). The FTC's action in this realm is discussed below.

[216] Mary Madden, *Public Perception of Privacy and Security in the Post-Snowden Era*, PEW RESEARCH CENTER (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/.

ii. Should Law Respond?

Because individuals face unattractive choices if they opt never to share their PII, their ultimate choice to do so is, at least in a small degree, coerced. Although they make the choice voluntarily (and thereby exercise liberty), the reality that they practically must make the choice to enjoy fundamental benefits, and that the alternatives to disclosure are undesirable, both work together to dilute the autonomy that would otherwise be exercised. In this way, the choice is coerced.

But coercion does not automatically require a legal response. Coercion "exists on a spectrum."[217] At one end, extreme and physical coercion, such as torture or rape, is widely condemned.[218] The law also acts to prevent subtler, psychological forms of coercion, as well – for instance, through laws criminalizing blackmail and extortion.[219] With torture, the act itself constitutes battery, a physical harm illegal in and of itself. With blackmail, the act itself – revealing information – is usually legal in and of itself, but the effect of the blackmailer's threat is deemed to be harmful and worthy of punishment because it forces – it coerces – the victim into a position in which he or she is likely to do

[217] Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L. J. 1131, 1150 (2011).

[218] David Sussman, *What's Wrong With Torture?* 33 PHIL. & PUB. AFF. 2 (2005) ("Since at least Beccaria there has been a broad and confident consensus that torture is uniquely barbaric and inhuman: the most profound violation possible of the dignity of a human being.") (internal quotations omitted); Ivanna Radacic, *Does International Human Rights Law Adequately Protect the Dignity of Women? in* Humiliation, DEGRADATION, DEHUMANIZATION: HUMAN DIGNITY VIOLATED 119 (Springer, 2011) ("rape has long been thought of as a prime example of a violation of human dignity").

[219] *See, e.g.*, 18 U.S. Code § 873 (criminalizing blackmail) ("Whoever, under a threat of informing, or as a consideration for not informing, against any violation of any law of the United States, demands or receives any money or other valuable thing, shall be fined under this title or imprisoned not more than one year, or both.").

something independently illegal (for instance, steal from a third party), and thus harm society.[220]

The transfer of PII does not share these traits. The disclosure is neither a physical wrong in itself nor does it coerce the "victim" to do something society discourages. In fact, society is dependent upon and even encourages individuals to feel comfortable disclosing their PII, for a variety of beneficial purposes such as increased ease of commercial transactions or simple convenience. Relatedly, what coercion does exist is relatively slight and perhaps even unnoticed by most Americans.[221]

Instead, what we associate negatively with this particular type of coercion is the attendant reality that the PII-recipient then does not protect peoples' PII as well as it could, thereby putting people in the path to future harm. Although that harm is real, the disclosure of PII is not harmful in itself because it (at least typically) neither involves physical coercion nor does the act coerce people to do something independently harmful. This counsels toward legal regulation of the degree to which information is protected – but not toward regulation to limit disclosure.

b. The (In)security of the PII

The second meaningful event in the timeline of a data breach is the storage of the PII by its recipient. The storage places the PII in a fixed state such that it is capable of being acquired by the third party hacker. The issue here is not the storage *per se*, but how

---

[220] *See* Henry E. Smith, *The Harm in Blackmail*, 92 NW. U. L. REV. 861, 868 (1998).

[221] Madden, *supra* note 216 ("In the commercial context, consumers are skeptical about some of the benefits of personal data sharing, but are willing to make tradeoffs in certain circumstances when their sharing of information provides access to free services.")

the recipient protects the information from third parties whom the individual did not intend to share the PII with. Does failing to uphold a certain level of security inflict harm on the individual who disclosed his or her PII?

i. Harm Requires Awareness

Solove argues that insecurity, or "carelessness in protecting stored information," *does* constitute an injury and describes it as "being placed in a weakened state, of being made more vulnerable to a range of future harms."[222] However, if and until a person is *aware* of the insecurity of their PII, no harm has occurred. Data insecurity may lay the groundwork for future harm in the form of the breach itself, but until an individual is aware of his vulnerability – or if he is lied to about the security of the data[223] – he has not been harmed.

The classic case *DeMay v. Roberts* serves as an example.[224] There, a man falsely presented himself as a physician while a woman gave birth. The plaintiff sued, claiming an invasion of privacy, but only after she discovered his actual identity.[225] Had she never learned of his identity, her sense of being violated – her harm – would have never accrued.[226] Similarly, the tort of assault exemplifies the same concern for harm only

---

[222] Daniel Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 518 (2006).

[223] This would implicate deception, which reduces autonomy. This point is discussed in the context of FTC Section 5 actions, *infra*, in Part III.

[224] DeMay v Roberts, 46 Mich. 160 (1881).

[225] *Id*. at 161.

[226] Ryan Calo articulates this point in his discussion of subjective privacy harms, noting that the harmful feeling of unwanted observation can occur in one brief moment, can linger, or can even be delayed. Calo, *supra* note 217, at 1145.

where the victims is aware of it, as assault requires the knowledge of the offensive action; a person getting ready to strike another cannot be liable for assault if the person cannot see his attacker.[227]

So too is the situation in the data breach context. Lax security standards present a problem insofar as they make a future harm possible, but the data insecurity cannot be said to harm the individual unless the relevant individuals are aware of the insecurity, or the lack of security has been misrepresented. As explained above, deception reduces autonomy in the sense that it interferes with an individual's decision-making and self-determination. This violation of autonomy is recognized in law as harmful. Again, the *DeMay v. Roberts* case is illustrative. The plaintiff brought an invasion of privacy claim and, because the defendant invaded her personal space and saw her giving birth – a sight she sought to protect – the defendant did, in fact, invade her privacy.[228] As the court recognized, though, the wrong stemmed from the defendant's deceit in failing to disclose that he was neither medically trained nor the doctor's aide, but merely a layman.[229] This deceit impaired the plaintiff's decision-making and consent to his presence in the room.

ii. Should Law Respond?

---

[227] *See* Restatement (Second) of Torts, § 21 Assault, AMERICAN LAW INSTITUTE (requiring "imminent apprehension" of "harmful or offensive contact.").

[228] Today, the plaintiff would have likely prevailed with the intrusion upon seclusion tort.

[229] *See* DeMay at 166. ("In obtaining admission at such a time and under such circumstances without fully disclosing his true character, [the doctor and the defendant] *were guilty of deceit*, and the wrong thus done entitles the injured party to recover the damages afterwards sustained, from shame and mortification upon discovering the true character of the defendants.") (emphasis added).

Though inadequate security does not, in and of itself, harm individuals, both law and private sector standards and regulations recognize the harm that it invites. In this sense, the law already does respond to the problem of inadequate security.

Some federal statutes, as noted above, do require certain entities to implement security programs for the protection of PII.[230] Even where the law does not formally require a particular level of security, however, certain private sector standards and rules come into play. Recognizing the potential harm to its reputation (and bottom line), certain industry groups impose security standards upon their members.[231] And when a company does decide to publish how it protects PII through its data security or privacy policy, the FTC can and does hold those companies to their word through the use of its Section 5 authority to police "deceptive" practices.[232]

Companies are not required to implement privacy policies, nor is adherence to industry guidelines legally required *per se*. Perhaps this reflects the reality that harms to individuals do not accrue through poor security standards until a breach actually occurs. Nonetheless, recognizing the prospect of future harm, some industry standards do protect against insecure storage of PII.

c. The Data Breach

The third important juncture in a data breach is the breach itself, including the period between the breach and any ultimate resolution to the breach. When a third party

---

[230] *See supra* note 214.

[231] For instance, the Payment Card Industry Security Standards Council imposes "Data Security Standards" on vendors who use credit and debit cards. *See* PCI Security Standards Council Releases Version 1.2 of PCI Data Security, Security Standards Council (Oct. 1 2008).

[232] This is discussed more *infra*, in Part III.

pierces a security system, this surely violates law in that the third party was not granted access to the information. But what harm has occurred to the individual whose PII is now under the control of the third party, and not solely the intended recipient? Does the individual suffer any harm when her PII has not actually been used to commit fraud? This section argues that such a harm manifests in an individuals' loss of autonomy, specifically through the loss of knowledge regarding the choices available to him or herself. This loss of negative freedom inhibits the individual's actions such to the extent that a concrete harm has occurred.

i. Vulnerability: The Loss of Negative Freedom

At the point of data breach, courts and commentators alike focus on the risk of future harm through identity theft and fraud, as though the risk itself encapsulated the harm. To be sure, this potential occurrence would certainly be harmful. The actual misuse of the information reduces freedom, or liberty itself, in its raw form: identity theft and fraud literally restricts a person from spending money he or she otherwise would be able to. Not surprisingly, this harm, in the form of a loss of liberty, is easily recognizable and criminalized.[233]

In addition, though, another harm exists regardless of whether the overt harm of identity theft ever occurs:[234] a lack of knowledge about freedom. At the point of data breach, the individual knows that his information could be used without her consent to

[233] *See supra*, Part II.

[234] Often, breaches expose information without any resulting identity theft. *See Data Breaches Are Frequent, But Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown*, U.S. GOV'T. ACCOUNTABILITY OFFICE, Report (2007) (noting that "available data and interviews with researchers, law enforcement officials, and industry representatives indicated that most breaches have not resulted in detected incidents of identity theft").

commit fraud or another crime. This knowledge arrests the victims' rational decision-making because she cannot be sure what the criminal may or may not do with his or her information. Professor Boudewijn de Bruin offers an example of this process in information security context:

> disclosure of private information may harm the subject [in] that it decreases her known freedom: the person's beliefs about her freedom and unfreedom deteriorate. What is important now is that the inadequacy of these beliefs is far from hypothetical. They are faulty, not in a hypothetical future, but at the very moment of the data breach, and a direct consequence of that is that the person's present decision-making capacities are frustrated. She is less well positioned than she was before the data breach to engage in responsible planning and decision making, because she will have to incorporate, in her current planning, the fact that her beliefs about certain freedoms and unfreedoms are less adequate than before the breach.[235]

This lack of known freedom manifests in a feeling of vulnerability, anxiety, and fear, placing the individual in a weaker state than before. As Solove explains, "[t]he potential for secondary use generates fear and uncertainty over how one's information will be used in the future, creating a sense of powerlessness and vulnerability."[236]

This feeling of powerlessness and vulnerability constitutes harm in itself. Further, it can cause individuals to act in ways they would not have otherwise. In the wake of a data breach, for instance, individuals might purchase identity theft insurance, or begin a

---

[235] Boudewijn de Bruin, *The Liberal Value of Privacy*, 29.5 LAW AND PHIL., 505, 532-33 (2010). De Bruin offers another example of how data disclosure can cause a loss of knowledge about one's freedom in the release of travel itineraries to a third party, such as an airline carrier: "Not knowing much about the criteria that underlie no-fly lists, but knowing that my travel itineraries may be thought of as 'suspicious,' I do not know for sure that I will be barred from flying. But neither am I sure that I will not, so I have to suspend my initial belief that I can fly to London. This constitutes a genuine reduction of known freedom." *Id*. at 529.

[236] Solove, *supra* note 222 at 520.

process of identity reclamation with the government.[237] Such physical acts incur financial costs, and the law currently already recognizes this financial burden as a cognizable harm. The question is then: should the law wait to act until a financial injury accrues?

ii. Should Law Respond?

A person's autonomy is violated in everyday life by seemingly innocuous events.[238] A white lie, for instance, can be considered a violation of the listener's autonomy, yet the law does not respond. Why should law respond to the loss of autonomy that results from a data breach?[239] The harm merits redress for two reasons: the harm is widely and similarly felt, and failure to respond could cause Americans to become more hesitant to share data, which would frustrate stated policy goals.

As has been discussed, democracies generally seek to protect and further their citizens' autonomy.[240] At a fundamental level, each person deserves to be treated with dignity: free from undue manipulation and coercion, and "as an end and not a means" generally. This maxim can translate in the Information Age to a mandate that consumers

---

[237] *Id*. at 509-10 (2010) (Explaining how the theft of a bank server can induce individuals to purchase identity theft insurance: "I do not know whether the burglar wanted to get the computer hardware or the financial records stored on it, and hence my knowledge about future interference is reduced. I am less sure than I was prior to the burglary about, say, the chance that criminals will try to obtain credit in my name, constituting a decrease of knowledge about negative freedom that may find reflection in the fact that I decide to buy insurance against identity theft.").

[238] Complete autonomy, like total privacy, "does not exist in this world except in a desert, and anyone who is not a hermit must expect and endure the ordinary incidents of the community life of which he is a part." Hill v. National Collegiate Athletic Assn., 7 Cal. 4th 1, 37 (Cal. 1994) (citing Rest.2d Torts, supra, § 652D, com. c.).

[239] Solove, *supra* note 222, at 484 ("Declaring that an activity is harmful or problematic does not automatically imply that there should be legal redress, since there may be valid reasons why the law should not get involved or why countervailing interests should prevail.").

[240] *See supra* Part I.

not be "used" for their PII[241] without a concomitant duty to protect that PII from future misuse and harm. This reflects a threshold level of respect for the consumer and the harms they may feel, such as vulnerability, anxiety, and nervousness, discussed above, if their PII becomes vulnerable in the wake of a breach.

What makes legal action more compelling, however, is the fact that the harm is so widely felt. Unlike minor infringements of autonomy that occur in day to day interactions with fellow citizens, data breaches cause harms that affect literally millions of people.[242] Not surprising given the increased prevalence of data breaches, more Americans are reporting themselves as victims of breaches.[243] Unlike losses of autonomy occurring in everyday private interactions, data breaches cause uniform, widely felt harms, ripe for government redress.

In addition, scholars and politicians alike understand the consequences of dignitary harms in the data security context – the feelings of insecurity and vulnerability can result in distrust of the companies who store Americans' information. As the White House recently noted in support of cybersecurity legislation: "As cybersecurity threats

---

[241] Especially within the data trade and behavioral advertising contexts, it is not unfair to view consumers as being "used" for their PII. *See* Corey Ciocchetti, *Just Click Submit: The Collection, Dissemination, and Tagging of Personally Identifying Information*, 10 VAND. J. ENT. & TECH. L. 553, 556-557 (2008) (noting companies' practice of collecting PII "and stor[ing] it in sophisticated databases where it can: (1) fulfill a transaction; (2) supplement an internal marketing profile; (3) be mined to predict future purchases; and (4) be sold to unrelated third parties for a profit.").

[242] *See supra* Introduction.

[243] Mary Madden, *More Online Americans Say They've Experienced a Data Breach*, PEW RESEARCH CENTER (Apr. 14, 2014) (reporting on a survey which suggested "growing numbers of online Americans have had important personal information stolen and many have had an account compromised. Findings from a January 2014 survey show that: 18% of online adults have had important personal information stolen such as their Social Security Number, credit card, or bank account information. That's an increase from the 11% who reported personal information theft in July 2013.").

and identity theft continue to rise, recent polls show that nine in 10 Americans feel they have in some way lost control of their personal information — and that can lead to less interaction with technology, less innovation and a less productive economy."[244] Although few doubt the endurance and vitality of the Information Age, the continued spate of data breaches surely does not alleviate any reticence or chilling effects individuals may feel about sharing information online.[245]

d. Liberty and Privacy

Data breaches withhold knowledge of who is in possession of an individuals' PII, and how the unknown party may use it. This loss of knowledge about one's freedom arrests decision-making, interfering with one's exercise of autonomy and producing feelings of anxiety and distress. Because important information is withheld, individuals' suffer a loss of autonomy. This loss is most akin to an indignity.

Victims' privacy and liberty, in contrast, remain intact. First, where victims' PII has not been used to commit identity theft and fraudulent purchases, their actions have not been restrained. If the Target hacker had used Mike and Hallie's credit card

---

[244] *See* Michael Shear and Natasha Singer, *Obama to Call for Laws Covering Data Hacking and Student Privacy*, N.Y. TIMES (Jan. 11, 2015), http://www.nytimes.com/2015/01/12/us/politics/obama-to-call-for-laws-covering-data-hacking-and-student-privacy.html?ref=politics. A recent report of medical data breaches found that "a majority of patients (54 percent) are "moderately" or "very likely" to change doctors as a result of a patient data breach" and that "early one-quarter of patients (21 percent) withhold personal health information from their doctors due to data security concerns." Gaby Loria, *Software Advice Report: HIPPA Breaches: Minimizing Risks and Patient Fears*, SOFTWARE ADVICE (2015), available at http://www.softwareadvice.com/medical/industryview/hipaa-breaches-report-2015/.

[245] *See, e.g.,* Hearing on Data Security Before the H. Subcomm. on Commerce, Mfg., and Trade of the H. Comm. on Energy and Commerce, 112th Cong., 1 (2011) (statement of David C. Vladeck, Dir. of the Bureau of Consumer Prot. at the Fed. Trade Comm'n) ("Data security is of critical importance to consumers. If companies do not protect the personal information they collect and store, that information could fall into the wrong hands, resulting in fraud and other harm, and consumers could lose confidence in the marketplace.").

information to rack up fraudulent purchases on their account, then Mike and Hallie's liberty would be restrained, at least conceptually, because they would no longer be free to rely on credit that was otherwise available. But until their PII is used, the main harm Mike and Hallie suffer is a subjective one – a dignitary harm – stemming from the uncertainty as to what may eventually happen.

Privacy, as opposed to liberty, is a more popular interest invoked in this context. Individual victims whose PII has been made vulnerable, but not misused, commonly invoke state common law invasion of privacy claims when suing in court.[246] Because privacy is often conceptualized in terms of the degree to which one controls information about him or herself, it seems intuitive that privacy is invaded where one's PII becomes vulnerable due to a breach – the victim no longer is in control of who may view (or, worse) use the PII. Yet, in many data breaches, whether the hacker has actually viewed the PII is unclear (and perhaps un-provable). Many data breaches do not result in identity theft.[247] And until the hacker actually uses the PII to commit a further crime, it is difficult, if not impossible, to show that any third party actually viewed the PII.

---

[246] *See* Paul Karlsgodt, *Key Issues in Consumer Data Breach Litigation*, PRACTICE LAW: THE JOURNAL, 51 (2014), available at https://www.bakerlaw.com/files/uploads/News/Articles/LITIGATION/2014/Karlsgodt-Lit_OctNov14_DataBreachFeature.pdf; Sasha Romanosky, David Hoffman, Alessandro Acquisti, *Empirical Analysis of Data Breach Litigation*, 11.1 J. OF EMPIRICAL LEG. STUDIES, 25 (Finding only state unfair business practices act and Fair Credit Reporting Act claims being brought more than Privacy Act and Privacy Tort claims). *See also* Cease, *supra* note 32 at 405 ("Oftentimes, the plaintiff will also allege that the defendant violated state consumer protection laws, breached some fiduciary duty owed to the plaintiff, or infringed on some state constitutional or statutory guarantee of the right to privacy.").

[247] *See supra*, note 233.

This was very recently on display in *Storm v. Paytime, Inc.*[248] In that case, a consolidation of two class actions, the defendant computer company suffered a data breach at the hand of unknown hackers, gaining access to over 230,000 peoples' PII.[249] The plaintiffs alleged, *inter alia*, that they had suffered a "harm to their privacy interest."[250] But the court was skeptical. "For a person's privacy to be invaded, their personal information must, at a minimum, be disclosed to a third party . . . if no one has viewed your private information (or is about to view it imminently), then your privacy has not been violated."[251] Because the Plaintiffs could not show that the hacker was actually able to "view, read, or otherwise understand the data it accessed" the Court held that they had not alleged a privacy harm.[252] Despite some courts' feeling that a PII recipient has wronged the individual then, courts simply cannot let a suit succeed on an invasion of privacy claim.[253]

---

[248] No: 14-cv-1138, 2015 U.S. Dist. LEXIS 31286 (M.D. Pa. Mar. 13, 2015).

[249] *Id*. at *23.

[250] *Id*.

[251] *Id*.

[252] *Id*.

[253] *See, e.g*, Randolph v. ING Life Ins. & Annuity Co., 973 A.2d 702, 710 (D.C. 2009) ("In this age of identity theft and other wrongful conduct through the unauthorized use of electronically-stored data, we have little difficulty agreeing that conduct giving rise to unauthorized viewing of personal information such as a plaintiff's Social Security number and other identifying information can constitute an intrusion that is highly offensive to any reasonable person, and may support an action for invasion of privacy (irrespective of whether the plaintiff alleges that economic or other resultant injuries have already come to pass). We nonetheless affirm the dismissal of appellants' invasion-of-privacy count, because the amended complaint fails to allege all of the elements of the tort of invasion of privacy.").

e. Summary

This Part has attempted to show that individuals do suffer a loss of autonomy as a result of a data breach. Victims like Mike and Hallie feel a sense of vulnerability, stemming from their inability to determine exactly how their PII may be used at some future time by an unknown hacker. This insecurity can best be described as a loss of negative freedom. This is not a privacy or liberty harm, because victims' actions are not restrained, nor are they sure their PII has been viewed, which would arguably violate their privacy. Instead, their loss of autonomy is an indignity.

PART III

IV. PRACTICAL UTILITY: WHY IDENTIFYING THE HARM MATTERS

Part I explained the concept of autonomy, and Part II discussed how data breaches can violate dignity, constituting a harm worthy of legal redress. Part III argues that the FTC is uniquely positioned to respond to this harm. To maintain its jurisdiction to do so, however, the FTC should recognize the harm it redresses as one to consumers' dignity, and not to their privacy.

a. The FTC's Section 5 Authority

Congress passed the Federal Trade Commission Act in 1914.[254] As conceived, the FTC was intended to recapture legislative control of antitrust from the judiciary,[255] but in 1938 Congress passed the Wheeler-Lea Amendment,[256] which broadened the FTC's authority to police companies' "unfair or deceptive acts or practices," on behalf of consumers. The Bureau of Consumer Protection currently brings actions against private entities it has reason to believe violate Section 5.

Deceptive practices are defined as "material representation[s], omission[s] or practice[s] that [are] likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment."[257] Actions in which the FTC challenges a company's practice as deceptive are relatively straightforward in the data security

[254] 15 U.S.C §§ 41-58.

[255] *See* Neil W. Averitt, *The Meaning of "Unfair Methods of Competition" in Section 5 of the Federal Trade Commission Act*, 21 B.C. L. REV. 227, 233 (1980) ("The initial task for the legislature was to recover the power to control antitrust policies.")

[256] Pub. L. No. 75-447,52 Stat. 111 (1938) (codified as amended at 15 U.S.C. § 45(a)(1)).

[257] 15 U.S.C. § 45(a)(1).

context: a company promised it would protect consumers' PII in a certain way, and then failed to do so. By breaking its promise, the company deceived the consumer.[258] The FTC has successfully brought actions against companies that state in their privacy or security policies that they protect or use their customers' information in one way, but then diverge from that promised path.[259]

"Unfair," however, is notoriously broad.[260] At the time of Wheeler-Lea's passage, Congress declined to narrow its scope, purposefully maintaining vagueness so the FTC could respond to future as yet unanticipated acts.[261] In 1980, the FTC released a policy statement in which it attempted to "delineate . . . a concrete framework for future application of the Commission's unfairness authority."[262] The statement began by noting that "unjustified consumer injury is the primary focus of the FTC Act."[263] The

---

[258] See Michael D. Scott, *The FTC, The Unfairness Doctrine, and Data Security Litigation: Has the Commission Gone Too Far?* 60 ADMIN L. REV. 127, 132 (2008).

[259] *See, e.g.*, Complaint at 8-9, In the Matter of Snapchat, Inc. (FTC Dec. 31, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/141231snapchatcmpt.pdf ("Snapchat has represented, expressly or by implication, that it employs reasonable security measures to protect personal information from misuse and unauthorized disclosure. In truth and in fact . . . in many instances, Snapchat did not employ reasonable security measures to protect personal information from misuse and unauthorized disclosure. Therefore, the representation . . . is false or misleading. The acts and practices of respondent as alleged in this complaint constitute deceptive acts or practices . . . in violation of Section 5(a) . . .").

[260] Not long after the FTC Act's passing, the Supreme Court recognized that "unfairness" "belongs to that class of phrases which do not admit of precise definition, but the meaning and application of which must be arrived at by . . . the gradual process of judicial inclusion and exclusion." FTC v. Raladam Co., 283 U.S. 643, 648 (1931) (internal quotations and citations omitted).

[261] *See* FTC Policy Statement on Unfairness, FED. TRADE COMM. (Dec. 17 1980), available at https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness. ("The statute was deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion. The task of identifying unfair trade practices was therefore assigned to the Commission, subject to judicial review, in the expectation that the underlying criteria would evolve and develop over time.").

[262] *Id*.

[263] *Id*.

Commission decided that any harm must be "substantial" and not "trivial or merely speculative."[264] An injury can be sufficiently substantial, though, "if it does a small harm to a large number of people, or if it raises a significant risk of concrete harm."[265] "In most cases," the FTC explained, "a substantial injury involves monetary harm."[266] "Emotional impact and other more subjective types of harm, on the other hand, will not ordinarily make a practice unfair."[267]

The FTC acknowledged that "[m]ost business practices entail a mixture of economic and other costs and benefits for purchasers."[268] Such tradeoffs, the Commission reasoned, justified that only those practices which are "injurious in [their] net effects" warranted action.[269] Thus, the FTC's second consideration was that "the injury must not be outweighed by any offsetting consumer or competitive benefits that the sales practice also produces."[270]

---

[264] *Id*.

[265] *Id*. The FTC is required to show only that a companies' practices "cause or are likely to cause" injury to any class of consumers. 15 U.S.C. § 45(a).

[266] As when "sellers coerce consumers into purchasing unwanted goods or services or when consumers buy defective goods or services on credit but are unable to assert against the creditor claims or defenses arising from the transaction." FTC Policy Statement, *supra* note 259. The FTC does not always require monetary harm, though. *See* FTC v. Neovi, Inc., 598 F. Supp. 2d 1104, 1115 (S.D. Cal. 2008) ("harm need not be monetary to qualify as an injury") (citing

[267] *Id*.

[268] *Id*. For example, "[a] seller's failure to present complex technical data on his product may lessen a consumer's ability to choose . . . but may also reduce the initial price he must pay for the article." *Id*.

[269] *Id*.

[270] *Id*.

Lastly, the FTC explained, "the injury must be one which consumers could not reasonably have avoided."[271] Consumers could be expected in most circumstances, "to make their own private purchasing decisions without regulatory intervention."[272] But "it has long been recognized that certain types of sales techniques may prevent consumers from effectively making their own decisions, and that corrective action may then become necessary."[273] Most unfairness actions are brought under this rubric; "not to second-guess the wisdom of particular consumer decisions, but rather to halt some form of seller behavior that unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decision making."[274]

Congress codified the Policy Statement in 1994,[275] and specified that a practice may be deemed unfair only if it "[1] causes or is likely to cause substantial injury to consumers which is [2] not reasonably avoidable by consumers themselves and [3] not outweighed by countervailing benefits to consumers or to competition."[276] That three-part cost benefit test "is the most precise definition of unfairness articulated by either the Commission or Congress."[277]

---

[271] *Id*.

[272] *Id*.

[273] *Id*.

[274] *Id*.

[275] *See* H.R. Rep. 103-617, 12 (1994).

[276] 15 U.S.C. § 45(n).

[277] Brief for the Fed. Trade Comm. at 2, Fed. Trade Comm. v. Wyndham Hotels & Resorts, LLC, (FTC Dec. 2014), *available at* https://www.ftc.gov/system/files/documents/cases/141105wyndham_3cir_ftcbrief.pdf. (citing Am. Fin. Servs. Ass'n v. FTC, 767 F.2d 957, 972 (D.C. Cir. 1985).

b. The FTC's Unique Position to Respond

As this thesis has argued, people whose PII has been made vulnerable by a breach are harmed. To date, however, plaintiffs have largely been unable to find relief where the PII has not been used to commit identity theft. This section argues that the FTC is better able to respond to data breach harm for two reasons: it is not hindered by the standing requirement, and it can redress a small harm widely felt.

i. The FTC Does Not Have to Show Standing

Data breaches cause dignity harms to the victims whose information is made vulnerable, manifest in feelings of anxiety, vulnerability, and distress. Yet, federal courts have thus far not recognized a private remedy for consumers where the PII-recipients' failure to adequately protect the PII results in a breach, but the PII has not yet been misused, at least to the consumers' knowledge.[278] This is because the federal court's standing doctrine requires plaintiffs to show that an injury that is "concrete and particularized" and "actual or imminent and not conjectural or hypothetical."[279] In *Clapper v. Amnesty International*, the Supreme Court considered plaintiffs' claims that the government's surveillance program constituted an unconstitutional search and seizure – but they couldn't show that their particular communications had been viewed, only that such surveillance was likely because of their particular actions.[280] The Court held that

[278] Brief of Amici Curiae Public Citizen, Inc., Center for Digital Democracy, and Consumer Action at 4-5 Federal Trade Commission v. Wyndham (FTC Nov. 12 2014), *available at* http://www.citizen.org/documents/FTC-v%20-Wyndham-Third-Circuit-Amicus.pdf

[279] Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147 (U.S. 2013).

[280] *Id*.

fear of some future harm was not sufficient, in itself, to achieve standing.[281] In *Clapper's* wake, most federal courts are holding that an increased *risk* of future harm – the future harm being identity theft – is not enough to confer standing.[282]

Data breach victims' dignitary harms do not fit within this standing jurisprudence. As discussed, dignitary harms are not necessarily physical ones. Thus, unlike curtailments of liberty, there is no physical manifestation of the harm. Second, and more fundamentally, dignitary harms do not necessarily entail a loss of money. They produce fear, anxiety, distress – but not always any concrete financial loss. Data breach victims usually claim that, because they feared identity theft, they purchased identity theft protection or spent money in other ways to protect themselves.[283] But courts simply cite to *Clapper* for the proposition that the plaintiffs cannot "manufacture" their injury in fear of a speculative future harm.[284]

Acting on behalf of millions of consumers nationwide, the FTC is not burdened by the individualized standing requirement. In passing the FTC Act, Congress specifically granted the Commission the authority to act on behalf of consumers as a whole – not as individualized parties. The FTC can bring adjudicative claims against companies it suspects of violating Section 5's prohibition of "unfair or deceptive" trade

---

[281] *Id*.

[282] *See supra* note 31.

[283] *See, e.g.*, Peters v. St. Joseph Servs. Corp., No. 4:14-CV-2872, 2015 U.S. Dist. LEXIS 16451, at *6 (S.D. Tex. Feb. 11, 2015).

[284] *Id*. at 15 (citing *Clapper, supra* note 278).

practices, or it may file in federal court.[285] If the party receiving the complaint disputes the FTC's authority or the complaint against it, it may appeal to an adjudicatory board and, if it disputes that Court's finding, may appeal to federal court.

Thus, as an agency instead of an individualized party, the FTC is granted the authority to act on behalf of the millions of people affected by data breaches through its administrative complaints. As such, the federal courts' standing requirement does not block FTC redress. While the FTC will never be able to levy actions against every PII recipient with unreasonable security standards, it has enormous power even in selectively targeting companies that store large amounts of PII or those whose errors in data security were especially egregious.[286] These actions are valuable insofar as they induce other companies to react accordingly out of fear of receiving their own FTC complaint.[287]

ii. Small Harms, Widely Felt

Second, the FTC is equipped to respond to small harms so long as they are widely felt. As noted above, an injury can be sufficiently substantial under the FTC's unfairness criterion "if it does a small harm to a large number of people, or if it raises a significant risk of concrete harm."[288] This is especially appropriate in the data breach context where,

---

[285] For a summary of the FTC's enforcement authority, see *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, FED. TRADE COMM. (July 2008), *available at* https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.

[286] Daniel Solove & Woodrow Hartzog, *The FTC And the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 607 (2014) (discussing how privacy lawyers scrutinize the FTC's publications in its actions to determine how best to advise their own clients).

[287] *Id*. at 606.

[288] *Supra* note 263. The FTC is required to show only that a companies' practices "cause or are likely to cause" injury to any class of consumers. 15 U.S.C. § 45(a).

though the harm may be slight or even barely felt by some consumers, it affects millions. As in a class action, then, each individual – while only suffering a small amount of harm individually – can still achieve redress because of the commonality and pervasiveness of the harm.[289] Unlike a class action, plaintiffs do not receive a monetary award, but vindication in the form of FTC monitoring of the companies' security programs and other structures designed to ensure that the failure does not recur.[290]

c. The FTC's Harm Dilemma

While the FTC is uniquely situated to respond to this harm, it is currently engaged in a challenge to its authority. Specifically, the FTC has been challenged to identify how allegedly "unreasonable" data security standards constitute "consumer injuries" under the FTC's unfairness standards. This section argues that the FTC should frame the harm in the data breach context – at least where there is no identity theft – as one to victims' dignity, as opposed to privacy, for two reasons, explained further below. First, conceptually such framing is simply more accurate. Second, in an environment in which the FTC's authority is being challenged, the FTC can more credibly argue that it has always protected consumers' dignity, more so than privacy. Such an argument can justify its actions in currently pending cases.

---

[289] *See* Thomas B. Leary, *The FTC and Class Actions*, FED. TRADE COMM. (June 26, 2003), *available at* https://www.ftc.gov/public-statements/2003/06/ftc-and-class-actions (discussing FTC actions in comparison to class actions, and downsides of the latter).

[290] *See* Solove & Hartzog, *supra* note 284, at 607 (discussing the usual requirements of consent decrees).

i. The FTC's Data Security Actions

Since 2005, the FTC has levied its authority against companies for failing to reasonably protect consumers' PII even where the company never proclaimed a certain security protection. Thus, the FTC is regulating data security through the use of its "unfairness" authority instead of its "deception" authority.

In 2005 the FTC filed an "unfairness" complaint against B&J Company when B&J failed to encrypt its customers' information and use other "readily available security measures."[291] Hackers were able to pierce B&J's security system and use its customers' PII to rack up $13 million in fraudulent charges.[292] Instead of challenging the FTC that "unreasonable" security standards were not "unfair," as defined by Section 5, B&J settled, entering a consent decree. In the decade since, 20 companies who have received FTC complaints for "unfair" data security practices have ended up doing the same.[293]

However, each of these breaches resulted in identity theft and consequent financial loss. The FTC seemed to be limiting its authority to only those instances where financial harm occurred – thus, indirectly defining "unfairness" and consumer injury as financial loss. With this approach, the FTC would avoid responding to breaches, like Anthem's in 2015, that affected massive amounts of Americans' PII simply because no identity theft immediately resulted. As this thesis has sought to show, the FTC would

---

[291] Complaint, BJ's Wholesale Club, Inc. (FTC Sept. 20, 2005), *available at* http://www.**ftc**.gov/os/caselist/0423160/092305comp0423160.pdf.

[292] *Id*.

[293] *See* Response of Fed. Trade Comm. in Opposition to Respondent's Motion to Dismiss Complaint with Prejudice to Stay Administrative Proceedings at 9 *In the Matter of LabMD, Inc.*, (FTC Nov. 2013), *available at* https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter (listing the FTC's unfairness cases).

therefore be failing to respond to the harm that occurs even where there is no alleged identity theft or financial loss.

Very recently, the FTC seems to have changed its approach. In 2013 the FTC filed an administrative complaint against LabMD, a healthcare organization, alleging that LabMD engaged in an "unfair" act when it allowed its patients' PII to be available on a peer-to-peer file-sharing network.[294] The information was later found in the possession of individuals who pleaded no contest to identity theft charges.[295] Importantly, the FTC did not base its action on the occurrence of identity theft; instead, the FTC's allegation seems to imply that the allegedly "unreasonable" security program which made the patients' information vulnerable, in and of itself, constituted an unfair practice.[296] The FTC concluded that LabMD's "failure to employ reasonable and appropriate measures to prevent unauthorized access to personal information" caused "substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is

[294] Complaint, In the Matter of LabMD, Inc. (FTC Aug. 2013) *available at* https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter. "Peer-to-peer ("P2P") file sharing applications are often used to share music, videos, pictures, and other materials between persons and entities using computers with the same or a compatible P2P application ("P2P network"). P2P applications allow a user to both designate files on the user's computer that are available to others on a P2P network and search for and access designated files on other computers on the P2P network. After a designated file is shared with another computer, it can be passed along among other P2P network users without being downloaded again from the original source. Generally, once shared, a file cannot with certainty be removed permanently from a P2P network." *Id*. at 4.

[295] *Id*. at 3.

[296] The FTC noted that "a number of the SSNs in the Day Sheets are being, or have been, used by people with different names, which *may indicate* that the SSNs have been used by identity thieves." *Id*. at 8 (emphasis added).

not reasonably avoidable by consumers. This practice was, and is, an unfair act or practice."[297]

Because of a separate administrative proceeding against LabMD's CEO, the dispute regarding FTC's authority to police cyber security standards is currently on hold until the separate proceeding comes to an end.[298] If the case is reviewed in federal court, the court will have to determine whether the FTC has abused its discretion in alleging that "unreasonable" security practices cause consumers "substantial injuries" – even where no identity theft has occurred.[299]

d. Why the FTC Should Frame the Harm as One to Dignity

LabMD has challenged the FTC: how are consumers harmed if their PII has not been used to commit identity theft? Some, including LabMD, believe the FTC may be exceeding the role set for it by Congress.[300] The FTC's authority over deceptive practices is clearly defined, but critics charge that Congress never intended for the FTC to regulate data security practices it considers to be "unfair." The FTC should respond that injuries occur in the form of a dignitary harm, putting consumers in the unfortunate position of doubting the security of their PII. Doing so stays true to the common understandings of

---

[297] *Id*.

[298] *See 11th Circuit Allows FTC Data Breach Case Against LabMD to Proceed*, NAT. L. REV. (Jan. 22, 2015), http://www.natlawreview.com/article/11th-circuit-allows-ftc-data-breach-case-against-labmd-to-proceed.

[299] A federal court would review the agency's interpretation for abuse of discretion. FTC v. R.F. Keppel & Bro., Inc., 291 U.S. 304, 314 (1934) (holding that courts can review agency unfairness determinations).

[300] *See, e.g.*, David Allen Zetoony, *The 10 Year Anniversary of the FTC's Data Security Program: Has the Commission Finally Gotten Too Big for its Breaches?* 2011 STAN. TECH. L. REV. 12 (2011).

privacy and dignity, while also positioning itself in a traditional role as protector of consumer dignity.

i. Conceptual Accuracy

There is an inherent tendency to assume that the interest protected by the FTC's data-security actions is privacy. Indeed, the FTC itself constantly speaks in terms of privacy.[301] This is to some degree, no doubt, influenced by the reality that privacy-related claims are popular among plaintiffs suing in private actions.[302]

Privacy, however, is not the interest at stake where no identity theft has occurred. Individuals' privacy is arguably invaded when their PII is outside of the control of the intended recipient. This is especially true if one defines privacy in terms of control; the personal information the individual desired to keep secure is now outside of that person's control. But privacy requires some viewership of the information desired to be kept secret.[303] Although viewing of the information for use to commit a further crime certainly occurs in some breaches, it does not in all. Thus, if harm is defined only in terms of privacy, any harm an individual experiences, if the individual (or FTC) cannot prove viewership of the PII, would be neglected. In contrast, dignitary harm is not dependent on actual viewership of the information or use of the information to commit a further crime. The mere knowledge that viewership and use could occur places the individual in a

[301] *See, e.g.*, Statement of Director Joshua Wright, Order Denying Respondent LabMD's Motion to Dismiss at 7, In the Matter of LabMD, Inc. (FTC Nov. 2013) (noting that "[t]he Commission has been involved in addressing online privacy issues for almost as long as there has been an online marketplace.").

[302] *See supra* note 244.

[303] *See* Part I.

suspended state of anxiety and fear stemming from the loss of negative freedom regarding what the unknown hacker may do with the information.

Conceptual clarity is necessary to both affirm common understandings of what each of privacy and dignity means, but also to understand how best to remedy invasions of each. As Daniel Solove notes, "[u]sing the general term "privacy" can result in the conflation of different kinds of problems and can lead to understandings of the meaning of "privacy" that distract courts and policymakers from addressing the issues before them."[304] Confusing dignity for privacy does both a disservice in that it elides distinctions between the two, affecting the way society responds. For that reason alone, the harm should be identified as one to dignity.

ii. The FTC Has Traditionally Protected Dignity

At a more practical level, identifying the harm as one to dignity better positions the FTC to respond. Critics charge the FTC is engaging in "boundless" power-grabs to redefine what constitutes "unfair" acts, stretching its authority into the data security context where Congress has heretofore never directed it to go.[305] True, the FTC has no Congressional authorization to police data security on which it can rely. But the FTC can convincingly argue that it is simply engaging in an unremarkable and, in fact, traditional FTC power to protect consumer dignity – even if the company has not deceived consumers by holding out a security policy it then failed to abide by.

---

[304] Solove, *supra* note 222. *See also*, Calo, *supra* note 217, at 1137 (the "overuse" of privacy "risks its diffusion into a meaningless catchall.").

[305] *See, e.g.*, Brief of Wyndham Worldwide Corp., Inc. at 1, *Fed. Trade Comm. vs. Wyndham Worldwide Corp*. (FTC Dec. 2014) ("The FTC's brief proposes a breathtaking expansion of agency authority.").

The Bureau of Consumer Protection has historically protected consumers' autonomy and dignity by policing unscrupulous deceptive acts. As noted above, deception interferes with individuals' development of autonomy, because it distorts or corrupts the input of information needed to make certain decisions about how to conduct ones' life. The FTC has a history of pursuing actions against companies for deceiving consumers into believing their information was secure or would be used only for a limited purpose, and then failing to maintain the promised security standards or using the information in an unforeseen way.[306] In addition, the FTC also has a long history of protecting consumer dignity by pursuing deception through the form of false advertising.[307] And even its unfairness claims have historically focused on the protection of consumer dignity, by guarding against deception and the interference with people's decision-making process. Traditional (i.e., non-data security) FTC "unfairness" jurisprudence (derived from complaints and consent orders) consisted of four categories: "(1) coercive or high-pressure selling; (2) withholding material information; (3) unsubstantiated claims; and (4) post-purchase rights and remedies."[308] The first three of these fit well within the traditional conception of autonomy as freedom from coercion, deception, and manipulation. Each focuses on freedom from undue influence such that a

[306] *See supra* note 257.

[307] *See The Role of Advertising and Advertising Regulation in the Free Market*, FED. TRADE COMM. (Apr. 1997), *available at* https://www.ftc.gov/public-statements/1997/04/role-advertising-and-advertising-regulation-free-market (discussing the FTC's authority to police "advertising that distorts the market by disseminating false or deceptive claims. These claims may induce consumers to purchase goods or services that, had the consumers not been misled by the deceptive advertising, they would not have chosen to buy.").

[308] Stephen Calkins, *FTC Unfairness: An Essay*, 46 WAYNE L. REV. 1935, 1961 (2000).

consumer can come to his or her own decision as to how to act or which product to purchase.

The dignitary interest in "unfairness" actions is subtly different than "deceptive" ones, to be sure. In the former, deception interferes with individuals' decision making processes – a classic method of interfering with a person's quality of choice, and hence autonomy. In data breaches, in contrast, autonomy is affected through a loss in one's knowledge of their negative freedom – what one can and cannot do. The problem is not that information was misleading (deception), it is that the information is withheld, and unknown. This places the individual in a vulnerable state, causing anxiety, aggravation, and some of the other subjective physical harms discussed by courts and scholars. Although the two are different forms of eroding autonomy, they nonetheless reach the same end: a person's autonomy is reduced, resulting in dignitary harm.

This recognition – that the FTC can advance consumer autonomy and dignity with its "unfairness" authority and not solely "deception" authority acts – may be occurring. In 2003, FTC director J. Howard Beales noted in a speech on the Commission's unfairness actions that "[t]he primary purpose of the Commission's modern unfairness authority continues to be to protect consumer sovereignty by attacking practices that impede consumers' ability to make informed choices."[309] By speaking in terms of consumers' decision-making abilities, Beales was implicating autonomy and consumers' dignity interests. And in 2008, then-Director David Vladeck noted the FTC's need to re-

[309] *See* J. Howard Beales, III, Director, Bureau of Consumer Prot., Fed. Trade Comm'n, Speech to the American Bar Association: *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, Speech (June 2003), available at http://www.ftc.gov/speeches/beales/unfair0603.shtm.

conceptualize its role in the Information Age, expanding its conception of harm beyond being seen as privacy invasions and as tied to the specific loss of money or identity theft.[310] Vladeck noted how behavioral advertising could cause consumer distress, but that the distress was born not from an invasion of one's privacy, but "an affront to dignity": "there's a huge dignity interest wrapped up in having somebody looking at your financial records when they have no business doing that."[311] The FTC would be well served in continuing to vocalize this conception of harm, and in advancing it in its legal arguments. Doing so would both direct the focus to the PII recipient instead of the hacker, as well as fit more within the FTC's traditional role.

[310] *An Interview with David Vladeck*, N.Y. TIMES (Aug. 5, 2009), http://mediadecoder.blogs.nytimes.com/2009/08/05/an-interview-with-david-vladeck-of-the-ftc/ (noting how the FTC had to "look for a new framework to approach privacy issues in this incredibly dynamic environment. One thing that was needed was someone in a position of authority to basically say, the frameworks that we've been using historically for privacy are no longer sufficient in this incredibly dynamic marketing.").

[311] *Id*.

V. CONCLUSION

We live in an age where the disclosure of mass amounts of PII is practically necessary. Data breaches are, unfortunately, a now common occurrence. To date, however, our legal system has largely ignored the harm that individuals – people like Mike and Hallie – experience when they receive an e-mail informing them that their information is no longer secured. When individuals learn their PII is insecure, they no longer operate under the same assumptions they once did, and their knowledge of how their PII may be used is kept from them. This loss of negative freedom manifests in feelings of anxiety, vulnerability, and distress. This harm is worthy of legal redress, because so many individuals must cope with it in our increasingly data-driven world.

The Federal Trade Commission is the appropriate vehicle for this redress. The FTC acts on behalf of consumers nationwide, and is thus not burdened by showings of particularized injury. In addition, Congress gave the Commission authority to redress even slight consumer harm if where it is widely felt, which aptly describes data breach harm where no identity theft has occurred. But the FTC must do more to assert its position in the data security enforcement context. It must frame consumer injury as one to dignity. Doing so maintains clear conceptual boundaries, while positioning itself as fulfilling the role it always has: protecting consumer dignity.

BIBLIOGRAPHY

5 C.F.R. § 297.102

5 U.S.C. § 552a

11th Circuit Allows FTC Data Breach Case Against LabMD to Proceed, NAT. L. REV. (Jan. 22, 2015), http://www.natlawreview.com/article/11th-circuit-allows-ftc-data-breach-case-against-labmd-to-proceed.

15 U.S.C. § 45(n)

15 U.S.C. §§ 41-58

18 USCS § 1028

18 U.S.C. § 873

201 Mass. Code Regs. § 17.04 (2010)

2014 Internet Security Threat Report, SYMANTEC CORPORATION (last accessed Feb. 19, 2015), http://www.symantec.com/security_response/publications/threatreport.jsp

Reed Abelson & Julie Creswell, *Data Breach at Anthem May Forecast a Trend*, N.Y. TIMES (Feb. 6, 2015), http://www.nytimes.com/2015/02/07/business/data-breach-at-anthem-may-lead-to-others.html

AFL-CIO v. Dept. of Housing & Urban Dev., 118 F.3d 786 (D.C. Cir. 1997)

Mark Alfino & G. Randolph Mayes, *Reconstructing the Right to Privacy*, 29 SOC. THEORY & PRACTICE 1 (2003)

An Interview with David Vladeck, N.Y. TIMES (Aug. 5, 2009), http://mediadecoder.blogs.nytimes.com/2009/08/05/an-interview-with-david-vladeck-of-the-ftc/

Apply Online Frequently Asked Questions, BANK OF AMERICA http://www.bankofamerica.com/deposits/checksave/index.cfm?template=lc_faq_applyonline&context=&statecheck=VA&cd_bag=&sa_bag=&ch_bag (last visited Feb. 10, 2015).

Autonomy, THE INTERNET ENCYCLOPEDIA OF PHILOSOPHY (last accessed Feb. 16, 2015).

Neil W. Averitt, *The Meaning of "Unfair Methods of Competition" in Section 5 of the Federal Trade Commission Act*, 21 B.C. L. REV. 227 (1980)

J. Howard Beales, III, Director, Bureau of Consumer Prot., Fed. Trade Comm'n, Speech to the American Bar Association: *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection* (June 2003), http://www.ftc.gov/speeches/beales/unfair0603.shtm.

Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962 (1964)

Benjamin E. Bratman, *Brandeis and Warren's The Right to Privacy and the Birth of the Right to Privacy*, 69 TENN. L. REV. 623 (2002)

Brief of Amici Curiae Public Citizen, Inc., Center for Digital Democracy, and Consumer Action, *Fed. Trade Comm. v. Wyndham Hotels & Resorts, LLC* (FTC Nov. 12, 2014), *available at* http://www.citizen.org/documents/FTC-v%20-Wyndham-Third-Circuit-Amicus.pdf

Brief for the Fed. Trade Comm., *Fed. Trade Comm. v. Wyndham Hotels & Resorts, LLC* (FTC Nov. 5, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/141105wyndham_3cir_ftcbrief.pdf.

Brief for the Fed. Trade Comm., *Fed. Trade Comm. v. Wyndham Hotels & Resorts, LLC* (FTC Dec. 2, 2013), *available at* https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter

Brief of Wyndham Worldwide Corp., Inc., *Fed. Trade Comm. v. Wyndham Worldwide Corp. LLC* (FTC Dec. 2014)

Boudewijn de Bruin, *The Liberal Value of Privacy*, 29.5 LAW AND PHIL., 505 (2010)

Stephen Calkins, *FTC Unfairness: An Essay*, 46 WAYNE L. REV. 1935 (2000)

Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L. J. 1131 (2011)

Catholic Church, *The Dignity of the Human Person*, *in* THE CATECHISM OF THE CATHOLIC CHURCH (2nd ed., 1700)

Caroline C. Cease, *Giving Out Your Number: A Look at the Current State of Data Breach Litigation*, 66 ALA. L. REV. 395 (2014)

John D. Castiglione, *Human Dignity Under the Fourth Amendment*, 2008 WISC. L. REV. 655

Chronology of Data Breaches: Security Breaches 2005 – Present, PRIVACY RIGHTS CLEARINGHOUSE (last visited Apr. 20, 2015)

Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (U.S. 2013)

Julie Cohen, *What Privacy is For*, 126 HARV. L. REV. 1904 (2012)

Communications Act, 47 U.S.C. § 201

Complaint of the Fed. Trade Comm., *BJ's Wholesale Club, Inc*. (FTC Sept. 20, 2005), *available at* http://www.**ftc**.gov/os/caselist/0423160/092305comp0423160.pdf.

Complaint for Civil Penalties, Injunctive and Other Equitable Relief, *United States v. Rental Research Servs., Inc.*, FTC File No. 072 3228 (D. Minn. Mar. 5, 2009)

Complaint of the Fed. Trade Comm., *In the Matter of LabMD, Inc.* (FTC Aug. 2013)

Computer Fraud and Abuse Act, 18 U.S.C. § 1030

Criminal Justice, New Technologies, and the Constitution, U.S. CONGRESS, OFFICE OF TECHNOLOGY ASSESSMENT (May 1988)

Mary Culnan and Cynthia Williams, *How Ethics Can Enhance Organizational Privacy*, 33 MIS QUARTERLY 673 (2009)

Stephen Darwall, *The Value of Autonomy and Autonomy of the Will*, 116 ETHICS 263 (2006)

Data Breaches Are Frequent, But Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown, U.S. GOV'T. ACCOUNTABILITY OFFICE, Report (2007)

Data Breach FAQ, TARGET.COM (Feb. 2015), https://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ#q5888

Data Protection & Breach Notification Readiness Guide, THE ONLINE TRUST ALLIANCE (2015)

Mike DeBonis, *'Death With Dignity' laws are proposed, bringing national debate to D.C. and Md.*, WASH. POST (Jan. 16, 2015), http://www.washingtonpost.com/local/dc-politics/death-with-dignity-laws-are-proposed-bringing-national-debate-to-dc-and-md/2015/01/16/8354bba8-9d09-11e4-a7ee-526210d665b4_story.html

DeMay v Roberts, 46 Mich. 160 (1881)

Director Joshua Wright, Order Denying Respondent LabMD's Motion to Dismiss (Nov. 2013)

Gerald Dworkin, THE THEORY AND PRACTICE OF AUTONOMY (Cambridge University Press, 1980)

Edward J. Eberle, *Human Dignity, Privacy, and Personality in German and American Constitutional Law*, 4 UTAH L. REV. 963 (1997)

E-mail from Target Corporation (Dec. 21, 2013)

FAQ: What is SSL? SSL.COM (last accessed Mar. 8, 2015), http://info.ssl.com/article.aspx?id=10241.

FCC Plans $10M Fine for Carriers That Breached Consumer Privacy, FED. TRADE COMM. (Oct. 24, 2014), *available at* http://www.fcc.gov/document/fcc-plans-10m-fine-carriers-breached-consumer-privacy

FDIC National Survey of Unbanked and Underbanked Households, FED. DEPOSIT INS. CORP. (2013), *available at* https://www.fdic.gov/householdsurvey/2013report.pdf

Joel Feinberg, *Autonomy, Sovereignty, and Privacy: Moral Ideals in the Constitution*, 58 NOTRE DAME L. REV. 445 (1983)

John Fisher, *Secure My Data or Pay the Price*, 4 WM. & MARY BUS. L. REV. 215 (2013)

James Fleming, *Securing Deliberative Autonomy*, 48 STAN. L. REV. 1 (1995)

A. Michael Froomkin, *The Death of Privacy*, 52 STAN. L. REV. 1461 (2000)

FTC Policy Statement on Unfairness, FED. TRADE COMM. (Dec. 17 1980), *available at* https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

FTC v. Neovi, Inc., 598 F. Supp. 2d 1104 (S.D. Cal. 2008)

FTC v. Raladam Co., 283 U.S. 643 (1931)

FTC v. R.F. Keppel & Bro., Inc., 291 U.S. 304 (1934)

Garcia v. San Antonio Metro. Transit Auth., 469 U.S. 528 (U.S. 1985)

Ruth Gavison, *Privacy and the Limits of Law* 89 YALE L. J. 421 (1980)

Rex Glensy, *The Right to Dignity*, 43 COLUM. HUM. RTS. L. REV. 65 (2011)

Goldberg v. Kelly, 397 U.S. 254 (1970)

Maxine D. Goodman, *Human Dignity in Supreme Court Constitutional Jurisprudence*, 84 NEB. L. REV. 740 (2006)

Allison Grande, *FCC Fills Data Security Gap With Record Fine Against AT&T*, LAW360 (Apr. 8, 2015)

Gramm-Leach-Bliley Act of 1999, 15 U.S.C. § 6809(4)(A) (2006)

Griswold v. Connecticut, 381 U.S. 479 (U.S. 1965)

Guide for Assisting Identity Theft Victims, FED. TRADE COMM. (Sept. 2013), *available at* http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

Jurgen Habermas, BETWEEN FACTS AND NORMS: CONTRIBUTIONS TO A DISCOURSE THEORY OF LAW AND DEMOCRACY (William Rehg trans., MIT Press, 1996)

Alexander Hamilton, THE FEDERALIST NO. 1 (Clinton Rossiter ed., 1999)

Hearing on Data Security Before the H. Subcomm. on Commerce, Mfg., and Trade of the H. Comm. on Energy and Commerce, 112th Cong., 1 (2011) (statement of David C. Vladeck, Dir. of the Bureau of Consumer Prot. at the Fed. Trade Comm'n)

Heller v. Doe, 509 U.S. 312 (U.S. 1993)

Thomas Hill, *Autonomy and Benevolent Lies*, 18 J. VALUE INQUIRY 251 (1984)

H.R. REP. 103-617 (1994)

Identity Theft, NAT. CONF. OF STATE LEGISLATURES (last accessed Mar. 8, 2015), http://www.ncsl.org/research/financial-services-and-commerce/identity-theft-state-statutes.aspx.

Identity Theft Overview, FED. BUREAU OF INVESTIGATION (last accessed Mar. 8, 2015), *available at* http://www.fbi.gov/about-us/investigate/cyber/identity_theft/identity-theft-overview.

Identify Theft Survey Report, FED. TRADE COMM. (Sept. 2006)

Information Age, MERRIAM WEBSTER ONLINE DICTIONARY 2015, http://www.merriam webster.com/dictionary/information%20age (last visited Feb. 10, 2015).

In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14 (D.D.C. 2014)

Interview with Mike and Hallie [surname omitted to preserve privacy] (Feb. 9, 2015)

Edward Jange & Paul Schwartz, *Notice, Autonomy, and Enforcement of Data Privacy Legislation: The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219 (2002)

Jones v. Barnes, 463 U.S. 745 (U.S. 1983)

Immanuel Kant, FOUNDATIONS OF THE METAPHYSICS OF MORAL (J. Beck trans., 1959)

Immanuel Kant, FOUNDATIONS OF THE METAPHYSICS OF MORALS (Lewis White Beck trans., 1983)

Immanuel Kant, FOUNDATIONS OF THE METAPHYSICS OF MORALS (M. Gregor trans., 1991)

Immanuel Kant, GROUNDWORK FOR THE METAPHYSICS OF MORALS (A. Wood trans., 2002)

Paul Karlsgodt, *Key Issues in Consumer Data Breach Litigation*, PRACTICE LAW: THE JOURNAL (2014)

Lawrence v. Texas, 539 U.S. 558 (2003)

Gaby Loria, *Software Advice Report: HIPPA Breaches: Minimizing Risks and Patient Fears*, SOFTWARE ADVICE (2015), http://www.softwareadvice.com/medical/industryview/hipaa-breaches-report-2015/

Lujan v. Defenders of Wildlife, 504 U.S. 555 (1992)

Mary Madden, "More Online Americans Say They've Experienced a Data Breach" PEW RESEARCH CENTER (Apr. 14, 2014), http://www.pewresearch.org/fact-tank/2014/04/14/more-online-americans-say-theyve-experienced-a-personal-data-breach/

Mary Madden, "Public Perception of Privacy and Security in the Post-Snowden Era" Pew Research Center (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/

Donald Michael, *Speculations on the Relation of the Computer to Individual Freedom and the Right to Privacy*, 33 GEO. WASH. L. REV. 275 (1964)

Mont. Const., Art. II § 4

National Aeronautics and Space Administration v. Nelson, 131 S. Ct. 746 (2011)

Jennifer Nedelsky, LAW'S RELATIONS: A RELATIONAL THEORY OF SELF, AUTONOMY, AND LAW (Oxford, 2011)

Helen Nissenbaum PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (Stanford University Press, 2010)

Oberg v. Billings, 207 Mont. 277 (Mont. 1983)

Oregon Death With Dignity Act, ORS § 127.800 *et seq*.

PCI Security Standards Council Releases Version 1.2 of PCI Data Security, SECURITY STANDARDS COUNCIL (Oct. 1 2008)

Andrea Peterson, *Lawsuits Against Sony Pictures Could Test Employer Responsibility for Data Breaches*, WASH POST (Dec. 19, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/12/19/lawsuits-against-sony-pictures-could-test-employer-responsibility-for-data-breaches/

Peters v. St. Joseph Servs. Corp., No. 4:14-CV-2872, U.S. Dist. LEXIS 16451 (S.D. Tex. Feb. 11, 2015)

Privacy Policy, GOOGLE (updated Dec. 2014), *available at* http://www.google.com/policies/privacy/

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

Ivanna Radacic, *Does International Human Rights Law Adequately Protect the Dignity of Women? in* HUMILIATION, DEGRADATION, DEHUMANIZATION: HUMAN DIGNITY VIOLATED 119 (Springer, 2011)

Randolph v. ING Life Ins. & Annuity Co., 973 A.2d 702 (D.C. 2009)

John Rawls, A THEORY OF JUSTICE (Belknap Press, 1971)

Joseph Raz, THE MORALITY OF FREEDOM (Clarendon Press, 1986)

Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011)

Restatement (Second) of Torts, § 21 Assault, AMERICAN LAW INSTITUTE

Rochin v. California, 342 U.S. 165 (1952)

Clinton Rossiter, *The Pattern of Liberty in* ASPECTS OF LIBERTY (Konvitz and Rossiter, eds., Cornell University Press 1958).

Sasha Romanosky, David Hoffman, Alessandro Acquisti, *Empirical Analysis of Data Breach Litigation*, 11.1 J. OF EMPIRICAL LEGAL STUDIES (2014)

Garrett W. Sheldon, THE POLITICAL PHILOSOPHY OF THOMAS JEFFERSON (Johns Hopkins University Press, 1991)

State Laws: Criminal, FED. TRADE COMM. (last accessed Feb. 19, 2015) http://www.ftc.gov/bcp/edu/microsites/idtheft/law-enforcement/state-laws-criminal.html

Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999)

Paul M. Schwartz and Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L.Q. REV. 1814 (2011)

Michael D. Scott, *The FTC, The Unfairness Doctrine, and Data Security Litigation: Has the Commission Gone Too Far?* 60 ADMIN L. REV. 127 (2008)

Michael Shear and Natasha Singer, *Obama to Call for Laws Covering Data Hacking and Student Privacy*, N.Y. TIMES (Jan. 11, 2015) http://www.nytimes.com/2015/01/12/us/politics/obama-to-call-for-laws-covering-data-hacking-and-student-privacy.html?ref=politics.

Henry E. Smith, *The Harm in Blackmail*, 92 NW. U. L. REV. 861 (1998)

Tim Smithers, *Autonomy in Robots and Other Agents*, 34.1 BRAIN AND COGNITION 88 (1997)

Daniel Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006)

Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393 (2001)

Daniel Solove, THE DIGITAL PERSON: PRIVACY AND TECHNOLOGY IN THE INFORMATION AGE (NYU Press 2004)

Daniel Solove, THE NEW VULNERABILITY: DATA SECURITY AND PERSONAL INFORMATION IN SECURING PRIVACY IN THE INTERNET AGE (Radin & Chander, eds., Stanford University Press, 2008)

Daniel J. Solove & Neil M. Richards, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123 (2007)

Daniel Solove & Woodrow Hartzog, *The FTC And the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014)

Daniel Solove & Woodrow Hartzog, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 1 (2015)

Stored Communications Act, 18 U.S.C. § 2701

Storm v. Paytime, Inc., No: 14-cv-1138, 2015 U.S. Dist. LEXIS 31286 (M.D. Pa. Mar. 13, 2015)

David Strauss, *Persuasion, Autonomy, and Freedom of Expression*, 91 COLUM. L. REV. 334 (1991)

Roger J. Sullivan, IMMANUEL KANT'S MORAL PHILOSOPHY (Cambridge University Press, 1989)

David Sussman, *What's Wrong With Torture?* 33 PHIL. & PUB. AFF. 2 (2005)

Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227

The Department of Justice's Efforts to Combat Identity Theft, U.S. DEPT. OF JUSTICE OFFICE OF THE INSPECTOR GENERAL AUDIT DIVISION (Mar. 2010)

Judith Jarvis Thomson, *The Right to Privacy*, 4.4 PHIL. & PUB. AFFAIRS (1975)

The Role of Advertising and Advertising Regulation in the Free Market, FED. TRADE COMM. (Apr. 1997), https://www.ftc.gov/public-statements/1997/04/role-advertising-and-advertising-regulation-free-market

United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

United States v. Westinghouse Elec. Corp., 638 F.2d 570 (3d Cir.1980)

U.S. Const., preamble

U.S. Const., amend. V

Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2006)

Kent Walker, *Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange* 2000 STAN. TECH. L. REV. (2000)

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

Alan Westin, PRIVACY AND FREEDOM (Athenaeum, 1967)

What You'll Need, WELLS FARGO (last visited Feb. 10, 2015), https://apply.wellsfargo.com/common_auth_start

Whalen v. Roe, 429 U.S. 589 (U.S. 1977).

Herb Weisbaum, *ID Theft Can Take Heavy Emotional Toll on Victims*, TODAY MONEY (Nov. 20, 2014)

James Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151 (2004)

Bruce J. Winick, *On Autonomy: Legal and Psychological Perspectives*, 37 VILL. L. REV. 1705 (2000)

Danny Yadron, *Five Simple Steps to Protect Corporate Data: What Companies Should Be Doing to Protect Their Computer Systems – But Aren't*, WALL ST. J. (Apr. 20, 2015), http://www.wsj.com/articles/five-simple-steps-to-protect-corporate-data-1429499477?mg=id-wsj.

David Allen Zetoony, *The 10 Year Anniversary of the FTC's Data Security Program: Has the Commission Finally Gotten Too Big for its Breaches?* 2011 STAN. TECH. L. REV. 12 (2011)

Kathryn Zickuhr, *Who's Not Online and Why*, PEW RESEARCH CENTER (Sep. 2013), http://www.pewinternet.org/2013/09/25/whos-not-online-and-why/