INDIGNITY: REDEFINING THE HARM CAUSED BY DATA BREACHES

George Ashenmacher[*]

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]

INTRODUCTION

Just before Christmas 2013, Mike and Hallie, a young married couple in Minneapolis, received an e-mail from Target.[2] The e-mail explained that an unknown hacker breached Target's data security system and that Target customers' personal information was now outside of Target's control.[3] The hacker could now use Mike and Hallie's credit card information to fraudulently purchase items in their names.[4]

"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.[5] "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."[6] Target offered a year of credit monitoring to bolster its claim.[7]

Despite Target's assurances, Mike and Hallie felt anything but confidence or trust.[8] "Something like a data breach feels so far

---

* B.A., Saint John's University, 2011, J.D., M.A., University of Minnesota, 2015. Thank you to Professors Amy Sanders, Bill McGeveran, and Jane Kirtley, and to the members of the *Wake Forest Law Review*. This is dedicated to my family, and to Julia.

1. ALAN WESTIN, PRIVACY AND FREEDOM, at x (1967).
2. Interview with Mike and Hallie Rogers (Feb. 9, 2015).
3. E-mail from Target Corp. to Mike Rogers (Dec. 21, 2013, 12:03 CST) (on file with author).
4. Interview with Mike and Hallie Rogers, *supra* note 2.
5. E-mail from Target Corp., *supra* note 3.
6. *Id.*
7. *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.").
8. Interview with Mike and Hallie Rogers, *supra* note 2.

removed from the actual consumer that when it happens, you're left feeling a bit helpless," Hallie explained.[9] "[We] just have to hope that the system Target put in place is good enough to stop the damage."[10] Unsure of what would happen with their information, the couple kept an eye on their bank statements, waiting to see if their identities would be used to rack up fraudulent charges.[11]

Millions of Americans have been in Mike and Hallie's position. Nearly all Americans operate in today's Information Age, in which personal information is "widely disseminated and easily available" through the use of computer technology.[12]

Americans find it increasingly difficult to live in modern society without releasing their "personally identifiable information" ("PII"), such as name, Social Security number, address, and credit card information[13]—information that is valuable insofar as it can be used to commit identity theft or other financial harms against individuals. E-mail, 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."[14] Yet one must disclose PII to open a Gmail account.[15] Or consider banking; more than ninety-two percent of American households have a bank

---

9. *Id.*
10. *Id.*
11. *Id.*
12. *Information Age*, MERRIAM-WEBSTER ONLINE DICTIONARY, http://www.merriam-webster.com/dictionary/Information%20Age (last visited Feb. 8, 2016).
13. "Personally identifiable information" lacks a uniform definition. *See* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 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(a)(3) (2012). The Gramm-Leach-Bliley Act defines it as "nonpublic personal information." Gramm-Leach-Bliley Act of 1999, 15 U.S.C. § 6809(4)(A) (2012). 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. § 17.02 (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).
14. United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010). Over eighty-five percent of Americans are online. *See* Kathryn Zickuhr, *Who's Not Online and Why*, PEW RES. CTR. (Sept. 25, 2013), http://www.pewinternet.org/2013/09/25/whos-not-online-and-why/.
15. *See Privacy Policy*, GOOGLE, http://www.google.com/policies/privacy/ (last modified Aug. 19, 2015) ("[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.").

account,[16] the use of which requires disclosing PII.[17] And when it comes time to purchase goods, Americans inevitably fork over their PII.[18] Thus, "[l]ife today is fueled by information, and it is virtually impossible to live as an Information Age ghost, leaving no trail or residue."[19] Indeed, the enormous number 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.[20]

Yet while individuals must release their PII, it is increasingly insecure in the hands of the entities—like Target—storing it. Data breaches are ubiquitous. High-profile breaches, like Sony's in late 2014, or breaches in which massive amounts of sensitive personal information are exposed, like the 2015 Anthem breach, regularly make headlines.[21] But even smaller breaches are occurring with increasing regularity. The Privacy Rights Clearinghouse began tracking data breaches in 2005.[22] Since 2012, each year has seen a steady increase.[23] Deemed "the year of the breach," 2014 saw 904

---

16. *See 2013 FDIC National Survey of Unbanked and Underbanked Households*, FED. DEPOSIT INS. CORP., https://www.fdic.gov/householdsurvey/ (last modified Oct. 28, 2014).

17. To open a Wells Fargo or Bank of America account, one must disclose his Social Security number and driver's license information. *FAQs: Apply for Bank Accounts*, BANK AM. http://www.bankofamerica.com/deposits/checksave/index.cfm?template=lc_faq_applyonline&context=&statecheck=VA&cd_bag=&sa_bag=&ch_bag (last visited Feb. 8, 2016); *Online Banking Enrollment Questions: What Kind of Information Do I Need to Provide During the Sign-up Process?*, WELLS FARGO, https://www.wellsfargo.com/help/faqs/enroll/ (last visited Feb. 8, 2016).

18. Brief for the Federal Trade Commission at 2, FTC v. Wyndham Hotels & Resorts, LLC, (3d Cir. Nov. 5, 2014) (No. 14-3514), 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.").

19. DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 8 (2004).

20. According to Target's estimate. *See Data Breach FAQ*, TARGET, https://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ#q5888 (last visited Feb. 8, 2016).

21. *See* 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; Andrea Peterson, *Lawsuits Against Sony Pictures Could Test Employer Responsibility for Data Breaches*, WASH. POST: THE SWITCH (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/.

22. Defined as "electronic entry by an outside party, malware and spyware." *Chronology of Data Breaches: Security Breaches 2005–Present*, PRIVACY RTS. CLEARINGHOUSE (Apr. 20, 2005), https://www.privacyrights.org/data-breach?title=&page=8.

23. *See id.*; *see also* SYMANTEC CORP., INTERNET SECURITY THREAT REPORT 2014, at 5 (2014), http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf (finding over 552

million records exposed within the first nine months—a ninety-five percent increase from the same period in 2013.[24] Up from 67,057,536 in 2014, 2015 saw 153,003,441 records exposed.[25] These breaches are, by and large, preventable. A number of studies have concluded that anywhere from ninety to ninety-five percent of breaches could have been prevented by the PII recipients with simple mechanisms,[26] such as data encryption or the use of Secure Sockets Layer.[27]

These breaches cause tangible, 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.[28] In the wake of an identity theft, victims spend precious time and money to get

---

million unique identities were exposed because of breaches occurring in 2013 and that there was an increase of sixty-two percent in 2013 over data breaches reported in 2012).

24. ONLINE TR. ALL., 2015 DATA PROTECTION & BREACH READINESS GUIDE 4 (Feb. 13, 2015), https://otalliance.org/system/files/files/resource/documents/dpd_2015_guide.pdf.

25. *See Chronology of Data Breaches*, *supra* note 22 (comparing the number of records in the database in 2014 to the number in 2015).

26. *See, e.g.*, Mary J. Culnan & Cynthia Clark Williams, *How Ethics Can Enhance Organizational Privacy: Lessons from the ChoicePoint and TJX Data Breaches*, 33 MGMT. INFO. SYS. Q. 673, 678 (2009) ("A recent analysis by Verizon Business of more than 500 forensic investigations of U.S. breaches involving more than 230 million records found that nearly 90 percent could have been prevented had reasonable security measures been implemented."); John A. Fisher, *Secure My Data or Pay the Price: Consumer Remedy for the Negligent Enablement of Data Breach*, 4 WM. & MARY BUS. L. REV. 215, 219–20 (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"); 2015 DATA PROTECTION & BREACH READINESS GUIDE, *supra* note 24 ("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.").

27. Secure Sockets Layer ("SSL") is 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." Hamza Khan, *What is SSL?*, SSL.COM (May 26, 2014), https://www.ssl.com/faqs/faq-what-is-ssl/. 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 "cyberhygiene" practices companies are failing to implement, see Danny Yadron, *Five Simple Steps to Protect Corporate Data*, WALL ST. J. (Apr. 19, 2015, 11:46 PM), http://www.wsj.com/articles/five-simple-steps-to-protect-corporate-data-1429499477?mg=id-wsj.

28. Daniel J. Solove, *The New Vulnerability: Data Security and Personal Information*, *in* SECURING PRIVACY IN THE INTERNET AGE 111, 112 (Anupam Chandler et al. eds., 2008).

their financial house in order.[29] No surprise, then, that law has responded to identity theft victims' plight. Hacking is illegal,[30] and Congress passed the Identity Theft and Assumption Deterrence Act in 1998,[31] which criminalizes the transfer or use of another's identity to commit any other crime.[32] And plaintiffs in all fifty states can bring claims under state law corollaries.[33] The government is eager to help the millions of identity theft victims reclaim their lost money and identity,[34] and identity theft prosecution is, understandably, highly prioritized.[35]

But have 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[36]—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

---

29. FED. TRADE COMM'N, 2006 IDENTITY THEFT SURVEY REPORT 6 (2007) ("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, 12:11 PM), http://www.today.com/money/id-theft-can-take-heavy-emotional-toll-victims-1D80305639.

30. *See* Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2012).

31. Identity Theft and Deterrence Act of 1998, Pub. L. No. 105-318, 112 Stat. 3007 (codified as amended at 18 U.S.C. § 1028 (2012)).

32. The statute makes it a crime to "knowingly transfer[], possess[], 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 that constitutes a violation of federal law, or that constitutes a felony under any applicable State or local law." 18 U.S.C. § 1028(a)(7); *see also Identity Theft Overview*, FED. BUREAU INVESTIGATION, http://www.fbi.gov/about-us/investigate/cyber/identity_theft/identity-theft-overview (last visited Feb. 8, 2016).

33. *Identity Theft*, NAT'L CONF. ST. LEGISLATURES, http://www.ncsl.org/research/financial-services-and-commerce/identity-theft-state-statutes.aspx (last visited Feb. 8, 2016) (providing each State's data breach laws); *see also State Resources*, IDENTITY THEFT RES. CTR., http://www.idtheftcenter.org/id-theft/state-resources.html (last visited Feb. 8, 2016) (providing specific rules and regulations concerning identity theft in each state).

34. *See, e.g.*, FED. TRADE COMM'N, GUIDE FOR ASSISTING IDENTITY THEFT VICTIMS 1, 3–4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

35. *See* OFF. OF THE INSPECTOR GEN., U.S. DEP'T OF JUST., THE DEPARTMENT OF JUSTICE'S EFFORTS TO COMBAT IDENTITY THEFT, at iii, vi (2010) 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").

36. This Article will refer to organizations that store individuals' PII as simply "PII recipients" for shorthand.

unsympathetic "no." Where there has been a breach without identity theft, plaintiffs have largely been unable to obtain a remedy against the entities that store their PII for failing to protect it against a breach.[37]

Yet, there is a growing sense that individuals are harmed even where their information has not been used to commit identity theft.[38] 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 these scholars recognize the "specifically acute problem" of identifying how that harm can best be described.[39] 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.[40]

Hartzog and Solove take a narrow approach to answering this question. They discuss the physical and financial toils victims must endure to rectify their financial state of affairs.[41] This Article, in

---

37. Fisher, *supra* note 26, at 217. As the Third Circuit 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).

38. These types of cases

> are those in which the plaintiffs' 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 claim 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 cards, 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).

39. Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2279 (2015).

40. *Id.*

41. *See 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.").

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?

This Article examines what harm occurs to individuals whose data have 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.[42] In addition, this Article discusses whether the law responds to any harm that does not occur. In addressing these questions, the Article attempts to avoid a marked tendency to resort to so-called intuitionist arguments, in which harm is assumed as self-evident but not described.[43] Instead, this Article examines what harm 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.

Part I explores the concept 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

---

42. A number of activities can give rise to a breach:

> 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 Article 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*.

43. *See* James Q. 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.").

to describe the harm that befalls individuals in the data breach context.

Equipped with an understanding of autonomy, Part II examines each sequence of a data breach to determine which of dignity, privacy, or liberty is affected and at which stage, and whether this harm merits legal redress. This is done by evaluating (a) the values affected in each juncture of a data breach and (b) whether law has typically protected those values in the past. Finally, Part III argues that this more accurate understanding of the harm is necessary, and points to recent FTC litigation as an example why.

I. AUTONOMY

This Article argues that data breaches violate victims' autonomy. To understand this harm, an understanding of autonomy itself is required. Autonomy is a broad, "notoriously vague" concept.[44] This is in part because the term is used widely, discussed in the realms of philosophy, medicine, law, politics, human rights, and even robotics.[45] To focus on the meaning relevant to this Article, this Part begins by examining the concept of autonomy in philosophy and then its role in liberal political theory.

A. Individual Autonomy

"Autonomy" literally means "self law": the Greek *autonomia* combines *autos*—"self," with *nomos*—"law."[46] 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."[47] Thus, the term's original use was political, describing the ability and right of nation-states "to administer their own affairs."[48] Autonomy began to refer to the conduct of individuals only in the nineteenth century.[49]

Philosopher Immanuel Kant is widely credited with inspiring a view of individuals as "autonomous, rational decision makers able to reason and make choices."[50] A succinct Kantian definition of

---

44. David A. Strauss, *Persuasion, Autonomy, and Freedom of Expression*, 91 COLUM. L. REV. 334, 354 (1991); *see also* Thomas E. Hill, Jr., *Autonomy and Benevolent Lies*, 18 J. VALUE INQUIRY 251, 251 (1984) ("[T]here is no uniform understanding about what autonomy is.").

45. *See* Tim Smithers, *Autonomy in Robots and Other Agents*, 34 BRAIN & COGNITION 88, 89, 95–96 (1997) (discussing autonomy and robotics, as well as autonomy's treatment in other fields).

46. GERALD DWORKIN, THE THEORY AND PRACTICE OF AUTONOMY 12–13 (1988).

47. *Id.* at 13.

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

49. *Id.*

50. Bruce J. Winick, *On Autonomy: Legal and Psychological Perspectives*, 37 VILL. L. REV. 1705, 1714–15 (1992).

autonomy is elusive,[51] but a working definition develops from Kant's examination of will, morality, and rationality.

Kant started with the familiar premise that humans possess the ability to reason, and that we can use this reason and logic to choose one path of action over another.[52] In examining the paths available, Kant was concerned with determining which human actions could produce objective laws of morality—a "realm of ends," in which humans guide their conduct according to some universally held maxims or imperatives.[53] 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.[54]

Humans exercise their will, according to Kant, by acting rationally.[55] But rationality itself could be guided by base impulses and animalistic instincts.[56] Whereas choice guided by pure reason is "free choice," decision determined "only by inclination (sensible impulse, stimulus) would be animal choice."[57] 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 products of one's unadulterated reason.[58] 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.[59] But

---

51. The most evident may be "the idea of the will of every rational being as *a universally legislative will*." IMMANUEL KANT, GROUNDWORK FOR THE METAPHYSICS OF MORALS 50 (Allen W. Wood ed. & trans., Yale Univ. Press 2002) (1785).

52. *See id.* at 52 (discussing rational, reasonable beings' ability to choose one action or law over others).

53. *Id.* at 51.

54. Thomas Hill explains that these principles "are self-imposed insofar as they stem from one's rational nature." Hill, *supra* note 44, at 255.

55. KANT, *supra* note 51, at 29.

56. Kant believed that "[f]eelings, emotions, habits, and other non-intellectual factors are excluded from autonomous decision-making. Any circumstances that particularize us are also excluded from autonomous decision-making." Jane Dryden, *Autonomy*, INTERNET ENCYCLOPEDIA PHIL., http://www.iep.utm.edu/autonomy/ (last visited Feb. 8, 2016).

57. IMMANUEL KANT, THE METAPHYSICS OF MORALS 42 (Mary Gregor ed. & trans., Cambridge Univ. Press, 1991) (1785).

58. Specific examples of "free choice" are elusive, but Kant does illustrate how one's motives indicate the presence or absence of autonomy by discussing why two people would refrain from lying. *See* KANT, *supra* note 51, 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.*

59. Hill, *supra* note 44, at 255.

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.[60]

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 acts with pure reason, free from constraining factors that would corrupt his otherwise purely rational decisions. Thus, autonomy is closely associated with freedom and liberty.[61] Kant himself defined autonomy in terms of negative freedom: acting in accordance with one's will separate from external constraining influences.[62] Negative freedom allows individuals to be "capable of causing events without being causally determined to do so."[63]

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."[64] "By exercising such a capacity," Dworkin writes, "persons define their nature, give meaning and coherence to their lives, and take responsibility for the kind of person they are."[65] 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, develop relationships, and accept commitments to causes, through which their personal integrity and sense of dignity and self-respect are made concrete.[66]

---

60. *Id.*

61. Some scholars suggest Kant viewed freedom and liberty interchangeably. *See, e.g.*, ROGER J. SULLIVAN, IMMANUEL KANT'S MORAL THEORY 46 (1989) ("In Kant's moral theory it is usually possible to use the word 'autonomy' in place of 'freedom.'").

62. KANT, *supra* note 51, 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 . . . .").

63. Hill, *supra* note 44, at 255.

64. DWORKIN, *supra* note 46, at 20.

65. *Id.*

66. JOSEPH RAZ, THE MORALITY OF FREEDOM 154 (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

B. *Freedom from Coercion, Manipulation, and Deception*

Kant's discussion on autonomy has been enormously influential, and scholars have wrestled with his description 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 the best path pursuant to some moral guide.[67] Two important caveats determine the quality of decision, however, and therefore determine the ability to express autonomy. For one, the choice must not be coerced.[68] In addition, one must operate in an environment in which the quality of options is sufficient for the individual to exercise meaningful choice.[69]

First, coercion is antithetical to autonomy, since "[a]ll coercion invades autonomy by subjecting the will of the coerced."[70] As Raz explains, coercion means *A* forcing *B* to do something against *B*'s will.[71] By doing so, *A* subjects *B* to *A*'s will, thereby interfering with *B*'s own process for determining *B*'s best path.[72] 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."[73] 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."[74]

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

---

> 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).

67. RAZ, *supra* note 66, 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.").

68. *Id.* at 155.

69. *Id.* at 155, 204–05.

70. *Id.* at 155.

71. *Id.* at 148–49, 155 (providing a more detailed articulation).

72. *See id.* at 154.

73. *Id.* at 152.

74. *Id.*

alternative are present."[75] 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 act autonomously.[76] Individuals, Hill explains, "though rationally disposed to make the best of their situation and unhindered 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."[77] 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.[78] "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."[79] 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."[80]

Together, these two factors help form the contours of a definition of autonomy: freedom from undue coercion or manipulation by another.[81] Manipulation or deception distort the information one receives, thereby frustrating a person's process of determining how best to respond and live one's life toward his guiding principles. Coercion results when one acts in some way that diverges from how he otherwise would act free from the influence.

---

75. *Id.* at 205.

76. *See* Hill, *supra* note 44, at 260–61.

77. *Id.* at 261.

78. *Id.*

79. *Id.* 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. RAZ, *supra* note 66, at 376. In a life of fear from the animal, the woman exerts all her intellectual ingenuity and willpower 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." *Id.; see also* Julie Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1424 (2000) ("[A]utonomy is radically contingent upon environment and circumstance.").

80. RAZ, *supra* note 66, at 374.

81. Thomas E. Hill, Jr., *Autonomy and Agency*, 40 WM. & MARY L. REV. 847, 851–52 (1999).

C. *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.[82] To that end, Kant believed the role of government was to foster, protect, and nurture autonomy.[83] Government protects and nurtures autonomy through the enforcement of its laws, ensuring that one person's self-development and exercise of autonomy do not impede others' autonomy.[84] And in codifying its citizens' social norms, moral duties, and expected behaviors, law bears its citizens' imprimatur.[85] Democracies thus seek to ensure that their citizens' self-determination flourishes to the extent that 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."[86]

Following Kant's writing, western liberal political theory has considered autonomy a normative value for individuals to obtain and for governments to foster.[87]

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

---

82. Humans possess a degree of autonomy by virtue of our ability to reason, but context and circumstance influence the degree to which autonomy is exercised. For an elaboration of this point—and its grounding in Kantian thought—see Yochai Benkler, *Siren Songs and Amish Children: Autonomy, Information, and Law*, 76 N.Y.U. L. REV. 23, 33 (2001) ("[A]utonomy is both a capacity and a condition of which people can have more or less.").

83. SULLIVAN, *supra* note 61, at 233.

84. *See* Feinberg, *supra* note 66, at 455–56.

85. JÜRGEN HABERMAS, BETWEEN FACTS AND NORMS: CONTRIBUTIONS TO A DISCOURSE THEORY OF LAW AND DEMOCRACY 105, 110 (William Rehg trans., MIT Press 1996) (1992) ("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.").

86. *Id.* at 111.

87. *See, e.g.*, JOHN RAWLS, A THEORY OF JUSTICE 520 (1971) ("[A] well ordered society affirms the autonomy of persons."); *see also* 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"); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1654–55 (1999) ("[D]emocracy 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.").

individuality."[88] This individuality is a necessary ingredient in a democracy, which depends upon its citizens acquiring knowledge, using the knowledge to reason, and acting upon their beliefs to direct society. In order to maintain individuality, citizens must be free from manipulation or coercion.[89] Thus, autonomy is a basic building block upon which the whole system of representative democracy is built.

D. Autonomy in American Law: Liberty, Dignity, and Privacy

The word "autonomy" does not explicitly appear in the Constitution, but it is understood to be embedded in the constitutional design and is recognized by the courts.[90] 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.[91] At the nation's founding, the major threat to freedom and autonomy "was the inability to have some say in the decisions that affected important aspects of one's life."[92] The Founding Fathers thus crafted a constitution reflecting humans' innate capacity to determine their best path "in pursuit of happiness."[93]

As such an integral value of American governance, one might expect a robust "autonomy" jurisprudence to have developed.[94] However, most likely 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

---

88. WESTIN, *supra* note 1, at 33.

89. *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.").

90. James E. Fleming, *Securing Deliberative Autonomy*, 48 STAN. L. REV. 1, 3 (1995) ("[A]utonomy is rooted . . . in the language and design of our Constitution."); Winick, *supra* note 50, at 1707–08 ("[R]espect for individual autonomy is deeply rooted in American constitutional history and tradition.").

91. 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 (2011).

92. *Id.*

93. Thomas Jefferson, in particular, was influenced by the belief that the law of nature produced innately rational people capable of exercising autonomy. *See* GARRETT WARD SHELDON, THE POLITICAL PHILOSOPHY OF THOMAS JEFFERSON 42–46 (1991).

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

simply too broad a term around which to develop a system of rights.[95]

Instead, autonomy is valued, protected, and nurtured in American law by three separate (though often related) derivative values: liberty, privacy, and dignity. The subparts 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.

1. Liberty

To say liberty is derivative of autonomy is a contentious claim. Although Kant viewed them as similar, if not identical, many philosophers since his time have articulated important differences.[96]

a. Relation to Autonomy

Liberty, unlike autonomy, usually connotes freedom of action as opposed to the process of deciding to do an intended action.[97] 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."[98] This is different from autonomy, which is citizens' "capacity to reflect upon and adopt attitudes toward their desires, wishes, and values."[99]

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."[100] But "because he cannot—given his information—avail himself of this opportunity, his ability to do what he wishes is limited."[101] The prisoner is technically at liberty to leave, but by

95. For instance, autonomy can also describe independence of nonhuman actors, as where 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 (1985) ("[T]he 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.") (quoting Erie R.R. Co. v. Tompkins, 304 U.S. 64, 78–79 (1938)).

96. *See supra* note 61.

97. *See, e.g.*, DWORKIN, *supra* note 46, at 105 ("[Liberty is] the ability of a person to effectuate his decisions in action.").

98. *Id.* at 106.

99. *Id.*

100. *Id.* at 14.

101. *Id.*

being duped into thinking all doors were locked, his autonomy is reduced, affecting his ability to be free.[102]

Conversely, a person's liberty can be interfered with without violating that person's autonomy. Although examples of this dynamic may be difficult to imagine,[103] 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 promote, not hinder, his efforts to define the contours of his life. We promote his autonomy by denying him liberty.[104]

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.[105]

---

102. *Id.*

103. 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.

104. *Id.* Joel 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 66, at 462; *see also* Morris Lipson, *Autonomy and Democracy*, 104 YALE L.J. 2249, 2249 (1995) ("[A]n autonomous agent is one who possesses negative liberty in the sense that he is free from any *externally imposed* constraints. . . . That is, a person need not, at every turn, be 'free' to choose or act precisely as he is inclined at that moment. A constrained choice or act can be an autonomous one, as long as, and insofar as, the source of the constraints is the person himself.").

105. Feinberg, *supra* note 66, at 462 ("The extent of our *de facto* 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

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 nurturing autonomy by protecting whichever act stems from a decision-making process—in short, by protecting autonomy's physical manifestation.

b. 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,"[106] and the Fifth Amendment guarantees that citizens' liberty will not be deprived without due process of law.[107] Because of this explicit grant 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.[108] 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 Amendments commands that legislation tending to impinge liberty be "rationally related" to some "legitimate" government objective.[109]

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 perceived as providing procedural protections only.[110] 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."[111]

---

x if he should choose, and nothing in his objective circumstances requires him to do *x* if he should choose not to.").

106. U.S. CONST. pmbl.

107. U.S. CONST. amend. V.

108. This basic premise is echoed in John Stuart Mill's *On Liberty*, which influenced the Fourteenth Amendment, passed nine years later. JOHN STUART MILL, ON LIBERTY 13 (C. Shields ed., Liberal Arts Press, Inc. 1956) (1859) ("[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.").

109. City of Cleburne v. Cleburne Living Cent., Inc., 473 U.S. 432, 440 (1985).

110. Winick, *supra* note 50, at 1715.

111. *Id.* at 1716.

"Liberty," in particular, was expanded to protect various economic and personal liberties.[112] These included the upbringing of children, marriage, procreation, and other areas of personal life.[113] As Professor Bruce Winick notes, "Between 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."[114] In each of these realms of life—marriage, education, and relationships—"liberty" interests 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*,[115] 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."[116] 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."[117] Thus, liberty protected both the right to use one's faculties to 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.[118] Liberty also protects autonomy outside of the Bill of Rights context.[119] The foundation of private contract law, for example, is built on the notion of private autonomy and individual self-determination.[120] The government "recognize[s] the desirability of allowing individuals to regulate, to a large extent, their own

---

112. *Id.* at 1716–17; *see also* IMMANUEL KANT, *The Metaphysics of Morals*, *in* PRACTICAL PHILOSOPHY 353, 387 (Mary Gregor ed. & trans., 1996).

113. Winick, *supra* note 51, 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 decisionmaking 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.").

114. *Id.* at 1743.

115. 165 U.S. 578 (1897).

116. *Id.* at 591.

117. *Id.* at 589.

118. Fleming, *supra* note 90, at 6.

119. Winick, *supra* note 50, at 1753 ("The principle of autonomy also permeates much of American law outside the domain of the Constitution.").

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

affairs," granting individuals "the power to bind themselves by expression of their intent to be bound."[121]

2. Privacy

Privacy is also derivative of autonomy. Privacy joins autonomy and dignity as being notoriously difficult to define.[122] Most definitions, however, focus on elements of secrecy, anonymity, or seclusion.[123] Each of these relate to the control a person has over his or her accessibility to the outside world.[124] Secrecy and anonymity keep information about oneself from others, while seclusion concerns the ability to keep some zone of self—either spatial or mental—to oneself.

a. 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.[125] 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."[126] 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."[127] 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

121. *Id.* (quoting JOHN D. CALAMARI & JOSEPH M. PERILLO, THE LAW OF CONTRACTS § 1-3, at 5–6 (3d ed. 1987)).

122. Judith Thomson famously quipped that, "[N]obody seems to have any very clear idea what it is." Judith Jarvis Thomson, *The Right to Privacy*, 4 PHIL. & PUB. AFF. 295, 295 (1975).

123. Ruth Gavison defined privacy as secrecy, anonymity, or seclusion. *See* Gavison, *supra* note 87, at 428–29 (1980).

124. *See, e.g.*, DWORKIN, *supra* note 46, 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 & PRAC. 1, 10 (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.").

125. Alfino & Mayes, *supra* note 124, at 6 ("Privacy plays a fundamental and ineliminable role in constructing personal autonomy.").

126. WESTIN, *supra* note 1, at 34; *see also id.* at 32–33 (referring to privacy as a "function" performed for personal autonomy).

127. Julie Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1906 (2013).

society."[128] Professor Ruth Gavison also believes autonomy is furthered through the protection of privacy.[129] 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."[130]

Though privacy protects autonomy, the two are conceptually distinct.[131] 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.[132] 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 privacy]. I conceal something from you that you might wish to know.[133]

Thus, autonomy is diminished, but not privacy.

b. 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

---

128. Clinton Rossiter, *The Pattern of Liberty*, *in* ASPECTS OF LIBERTY 15 (Konvitz & Rossiter eds., 1958).

129. *See* Gavison, *supra* note 87, at 423 (describing privacy as promoting "liberty, autonomy, selfhood, and human relations, and furthering the existence of a free society").

130. HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 82 (2010). Conceptually,

> [i]f 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. . . . [P]rivacy is to be understood as a form of autonomy, [as] self-determination with respect to information about oneself. *Id.* at 81 (citation omitted).

131. DWORKIN, *supra* note 46, at 104 ("[A]lthough privacy may be related to autonomy in a number of ways it is not identical with it.").

132. *Id.*

133. *Id.*

name of privacy.[134] This robust presence can in large part be traced to one law review article.

Many scholars consider Samuel Warren and Louis Brandeis's *The Right to Privacy*[135] to be the birth of privacy law in the United States.[136] 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."[137] 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.[138] 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 youth," had evolved to protect not merely physical property and liberty interests, but also intellectual ones.[139] So too, they argued, it could protect individuals' "right to be let alone."[140]

Since Warren and Brandeis' influential writing, courts have slowly began to develop jurisprudence around this newfound "right to privacy." In 1960, Dean Prosser, an influential legal scholar, gathered cases and eventually formulated the "Invasion of Privacy" tort, itself composed of four distinct torts: (1) intrusion upon seclusion or solitude, or into private affairs; (2) public disclosure of embarrassing private facts; (3) publicity which places a person in a false light in the public eye; and (4) appropriation of name or

---

134. *See, e.g.*, Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2012); Griswold v. Connecticut, 381 U.S. 479, 482–84 (1965); William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).

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

136. *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* Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 125 (2007) (arguing that *The Right to Privacy* reflected a divergence from the privacy-protecting law of confidentiality).

137. Warren & Brandeis, *supra* note 135, at 195.

138. *Id.* at 196.

139. *Id.* at 193 ("[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 . . . .").

140. *Id.*

likeness.[141] 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.[142] 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.[143]

In addition to the privacy torts, the Supreme Court has found that the Constitution bestows a right to privacy, despite any mention of "privacy" within it.[144] In *Griswold v. Connecticut*,[145] the Supreme Court held that the Bill of Rights contained "penumbras," creating "zones of privacy."[146] 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, "enabl[ing] the citizen to create a zone of privacy which government may not force him to surrender to his detriment."[147]

This constitutional right to privacy arguably extends to so-called "informational privacy." In *Whalen v. Roe*,[148] plaintiffs challenged a government program that retained identifying information of patients who had been prescribed certain drugs in a centralized file.[149] The plaintiffs argued that the program violated their Constitutional right to privacy.[150] The Court held that the program did not constitute an invasion "of any right or liberty protected by the Fourteenth Amendment."[151] 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

141. Prosser, *supra* note 134, at 389.
142. *See, e.g.*, Randolph v. ING Life Ins. & Annuity Co., 973 A.2d 702, 710 (D.C. 2009).
143. Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 965 (1964) (citing Prosser, *supra* note 134).
144. Griswold v. Connecticut, 381 U.S. 479, 482–84 (1965).
145. *Id.*
146. *Id.* at 484.
147. *Id.*
148. 429 U.S. 589 (1977).
149. *Id.* at 591.
150. *Id.* at 598.
151. *Id.* at 603–04.

Constitution."[152] Since *Whalen*, the circuit courts have taken various stances toward this right to informational privacy.[153]

Finally, various statutes have been enacted with the goal of protecting people's privacy. These include those designed to maintain the confidentiality of certain information,[154] to prevent wiretapping and eavesdropping,[155] and to protect personal zones of seclusion free from interference by the outside world.[156]

3. Dignity

The final derivative value of autonomy is dignity. Dignity is an ethereal, capacious concept, but it is most closely linked to autonomy, as 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."[157]

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 fact of its existence."[158] *All* humans were endowed with dignity, according to Cicero, simply because of our "superior minds" which allowed for our self-awareness.[159] 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."[160] Then during the Renaissance,

---

152. *Id.* at 605; *see also* NASA v. Nelson, 562 U.S. 134, 138 (2011) ("We assume, without deciding, that the Constitution protects a privacy right of the sort mentioned in *Whalen* . . . .").

153. *Compare* Am. Fed'n of Gov't Emps. v. Dep't of Hous. & Urban Dev., 118 F.3d 786, 788 (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).

154. *See, e.g.*, Gramm-Leach-Bliley Act of 1999, 15 U.S.C. § 6809(4)(A) (2012) (protecting the confidentiality of financial information); Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2012) (protecting confidentiality of video rental records).

155. *See, e.g.*, Stored Communications Act, 18 U.S.C. § 2701 (2012).

156. *See, e.g.*, Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227 (2012) ("Unrestricted telemarketing . . . can be an intrusive invasion of privacy.").

157. Rex D. Glensy, *The Right to Dignity*, 43 COLUM. HUM. RTS. L. REV. 65, 67–68 (2011); *see also* IMMANUEL KANT, FOUNDATIONS OF THE 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.").

158. Glensy, *supra* note 157, at 74.

159. *Id.*

160. *Id.*

religious authorities regarded dignity as endowed in each of us, but as a gift from God, as humans made in His image.[161]

a. Relation to Autonomy

Regarded as the father of the modern concept of dignity, Kant secularized dignity and articulated it "as a normative legal ideal."[162] As with Cicero, Kant believed humans possessed dignity stemming from rationality.[163] Since dignity was an outgrowth of autonomy, an affront to autonomy would therefore be an indignity. Kant's first Categorical Imperative, described in his *Foundations of the Metaphysics of Morals*, instructs people to act "only according to principles which can be conceived and willed as a universal law."[164] 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."[165] 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."[166] 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."[167]

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.[168] Thus, actions that restrict the

---

161. *Id.* This remains a core belief. *See, e.g.*, CATHOLIC CHURCH, *The Dignity of the Human Person*, *in* THE CATECHISM OF THE CATHOLIC CHURCH (2d ed., 1700) ("The dignity of the human person is rooted in his creation in the image and likeness of God.").

162. Glensy, *supra* note 157, at 76.

163. John D. Castiglione, *Human Dignity Under the Fourth Amendment*, 2008 WIS. L. REV. 655, 678.

164. KANT, *supra* note 157, at 54.

165. *Id.*

166. Castiglione, *supra* note 163, at 678.

167. *Id.* In agreement, Roger Sullivan casts Kant's second imperative as the Formula of Respect for the Dignity of Persons. SULLIVAN, *supra* note 61, at 193. Sullivan writes that "[t]he 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.*

168. Darwall, *supra* note 48, 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)).

exercise of autonomy—coercion, deception, or manipulation—are said to violate a person's dignity.

b. Dignity in American Law

Unlike liberty, "dignity" does not appear in the Constitution.[169] Nonetheless, the Supreme Court has used the term often,[170] 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."[171]

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."[172] 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 of dignity as (a) a fundamental byproduct of human rationality and (b) a status achieved through self-determination.[173]

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*,[174] the Supreme Court ruled that tying a prisoner to a hitching post in

---

169. Notably, though, the very first Federalist Paper called for the Constitution to ensure "liberty," "dignity," and "happiness" of the people. *See* Glensy, *supra* note 156, at 77 (quoting THE FEDERALIST NO. 1, at 4 (Alexander Hamilton) (Clinton Rossiter ed., 1999)).

170. *See generally* Maxine D. Goodman, *Human Dignity in Supreme Court Constitutional Jurisprudence*, 84 NEB. L. REV. 740 (2006) (discussing the role of dignity in the decision making of the Supreme Court).

171. Goldberg v. Kelly, 397 U.S. 254, 264–65 (1970).

172. 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 170, at 757.

173. *See* Glensy, *supra* note 157, at 90.

174. 536 U.S. 730 (2002).

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.[175] The punishment was "antithetical to human dignity" because it was "degrading and dangerous."[176] As Glensy notes, the Court "focused on the demeaning aspect of the punishment, which included taunting and wanton humiliation of the prisoner."[177] This sense of dignity is Kantian in its dictate that people—even criminals—"not be treated as objects."[178] 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.[179]

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[d] police behavior as offensive to human dignity when it [rises] to the level of shocking even those of hardened sensibilities."[180] 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."[181] 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."[182] Dignity in this context, then, is associated with physical integrity.[183]

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

175. *Id.* at 738.
176. *Id.* at 745.
177. Glensy, *supra* note 157, at 88.
178. *Id.*
179. *See supra* notes 100–04 and accompanying text.
180. Glensy, *supra* note 157, at 89 (quoting Rochin v. California, 342 U.S. 165, 172, 174 (1952)) (quotations omitted).
181. *Id.* at 93.
182. *Id.* at 90.
183. *Id.* 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*, 1997 UTAH L. REV. 963, 975 (1997).

characteristics."[184] Most notably, in *Lawrence v. Texas*,[185] the Court invalidated an antisodomy statute on due process grounds.[186] 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.[187] And in its recent landmark rulings regarding same-sex marriage in *United States v. Windsor*[188] and *Obergefell v. Hodges*,[189] the Supreme Court leaned heavily on individuals' dignity in affirming the right to same-sex marriage. In the Sixth Amendment right-to-trial context, the Court has held that a "defendant's appearance in the status of one conducting his own defense is important in a criminal trial, since the right to appear *pro se* exists to affirm the accused's individual dignity and autonomy."[190] In contrast to 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.[191]

Invocations of dignity harms appear in other situations where a person's decisional autonomy is at stake. Among state constitutions, Montana's is unique in recognizing dignity, stating in Article II, Section 4 that "[t]he dignity of the human being is inviolable."[192] 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.[193] Yet, in *Oberg v. City of Billings*,[194] a police officer challenged the department's requirement that he take a polygraph test for employment as violating the dignity clause.[195] The court

184. Glensy, *supra* note 157, at 90.

185. 539 U.S. 558 (2003).

186. *Id.* at 558.

187. *Id.* at 574.

188. 133 S. Ct. 2675, 2692 (2013) (framing the question as whether the "resulting injury and indignity" stemming from the restrictions imposed by the Defense of Marriage Act "is a deprivation of an essential part of the liberty protected by the Fifth Amendment").

189. 135 S. Ct. 2584, 2608 (2015) ("[Petitioners] ask for equal dignity in the eyes of the law. The Constitution grants them that right.").

190. McKaskle v. Wiggins, 465 U.S. 168, 178 (1984).

191. Glensy, *supra* note 157, at 93 (describing this as "dignity as autonomy").

192. 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 n.21 (2004).

193. Jackson, *supra* note 192, at 32.

194. 674 P.2d 494 (Mont. 1983).

195. *Id.* at 494.

sided with the officer, striking down the lie detector test on other grounds,[196] 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."[197] 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 what information he withholds and extracting his own thoughts from him violates self-determination.[198]

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 the so-called "Death with Dignity" laws, which, generally speaking, allow a person to permit physicians to prescribe him lethal medications, such that the person controls the decision to end his own life.[199] Dignity also pervades the legal concept of informed consent, wherein a person is entitled to all relevant information that could influence his decision to agree to something.[200]

c. Privacy and Dignity: Important Distinctions

The above Subparts have sought to explain how liberty, privacy, and dignity are conceptualized, and how each takes form 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 people's rationality (mandating a threshold level of respect due each person) and (b) a status achieved through the

196. *Id.*

197. *Id.* at 498.

198. *See* OFFICE OF TECH. ASSESSMENT, PB88-213921, CRIMINAL JUSTICE, NEW TECHNOLOGIES, AND THE CONSTITUTION 9 (1988), https://www.princeton.edu/~ota/disk2/1988/8809/8809.PDF ("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.").

199. *See, e.g.*, Oregon Death with Dignity Act, OR. REV. STAT. §§ 127.800–.897 (2013). 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.

200. DWORKIN, *supra* note 46, 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.").

exercise of rationality to make autonomous choices (mandating noninterference with people's decision-making processes).

In concluding this Subpart, two further points are necessary, which are important to the later analysis of data breach harms. First, compared to liberty and privacy, harms to one's dignity are more difficult to identify. Second, privacy is typically not affected if one's personal information is exposed but not viewed, whereas one's dignity is said to be harmed regardless of whether viewership occurs. Each of these points causes privacy harms to be more easily recognized than harms to dignity.

d. Harms to Dignity Are the Least Observable

Liberty and privacy violations are easily observable. The freedom to do something or act in a certain way, when restricted, is apparent. To take a well-known example, the freedom to "bear arms" when circumscribed, or denied outright, is fairly obvious: the person is no longer (legally) allowed to carry a certain firearm in a certain location[201] or to carry one at all.[202] 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.[203] When a person discloses some information about another the latter desired to keep secret,[204] the information in the public domain can be identified as the byproduct of the legal transgression.[205] These characteristics of liberty (a physical act) and privacy (spatial seclusion, anonymity, or secrecy) make them easily protectable in law, because violations of each leave some sort of physical evidence.

Violations of dignity (or "indignities") are comparatively opaque. Unlike liberty, person *A* can violate person *B*'s dignity without

---

201. *See, e.g.*, MINN. STAT. ANN. § 641.165 (West 2009) (forbidding the carrying of a firearm in any jail, lockup, or correctional facility).

202. *See, e.g., id.* § 609.67 (restricting the right to own certain types of assault weapons and shotguns).

203. Time, Inc. v. Hill, 385 U.S. 374, 413 (1967) (Fortas, J., dissenting) ("[T]he 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.").

204. Thus implicating the privacy tort of publication of private fact.

205. 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." (emphasis added)).

restraining some action or conduct of *B*'s.[206] Similarly, person *A* can violate person *B*'s dignity without harming person *B*'s privacy.[207] Because indignities often involve coercion, deception, or manipulation—none of which are necessarily physical or spatial—indignities can be comparatively more difficult to identify.

e. The Importance of Viewership in Privacy and Dignity

Liberty, privacy, and dignity each derive from autonomy. When it comes to the release of information about oneself, however, an important distinction develops between privacy and dignity: the unwanted release of information about oneself typically only harms privacy if that information is actually viewed. This understanding of privacy has been codified and ingrained in privacy law. The Privacy Act of 1974,[208] 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.[209] And courts generally hold that privacy invasions require actual viewership of the information one seeks to protect.[210] Thus, saying someone's privacy has been invaded implicitly means that information one desired to keep hidden (or "secret" or "anonymous" in privacy parlance) is in fact no longer hidden, because it has been viewed by a third party.

In contrast, invasions of another's dignity also impede autonomy, but they do not necessarily require viewership of information one desires to keep hidden. The mere knowledge that a third party might view information creates uncertainty that, in certain contexts, could arguably work an injury to the victim's dignity.[211]

These distinctions matter in the data breach context. First, the trappings of privacy law that make privacy harm easy to observe—such as spatial seclusion or publication of private facts—are not

206. 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. *See* DWORKIN, *supra* note 46, at 105.

207. 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. *See id.* at 104.

208. 5 U.S.C. § 552(a) (2012).

209. *See* 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)).

210. *See 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.").

211. *See infra* Part II.

necessary for one's dignity to be violated. Second, privacy is not harmed unless information about oneself has been viewed, whereas viewership is not required for dignity to be harmed.

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 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 Article 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 would otherwise do. A person's liberty has not 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 that they harm a person's dignity which, as explained below, occurs in being placed in a vulnerable, weakened state.

II. ANALYSIS: DATA BREACH HARM

This Article now seeks to apply this understanding of autonomy to the data breach context, returning to the questions posed at the outset: Have individuals been harmed when their data has been made vulnerable because of a breach but they have not become victims of identity theft? What is the nature of that harm? Additionally, 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) its storage (i.e., the security or insecurity of the PII); and (3) its release (i.e., the breach itself).

A. The Disclosure of PII

A data breach cannot happen without data, and cyber thieves would not 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 Subpart argues that consent to the release of PII is dubious where it is coerced by practical necessity. However, while

consent is important, nonconsent is normally not grounds for legal redress in and of itself; instead, non-consent is dependent on some later harm to occur.

1. 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.[212] The Information Age is, after all, fueled 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,[213] while also allowing for better services to the customer, creating consumer preference and loyalty.[214]

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,[215] and refusal to release PII today, while technically possible, would leave individuals in an untenable

---

212. *See* 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* Cohen, *supra* note 127, at 1916 (noting that increased personalization may lead to "price discounts, enhanced products and services, more convenient access to resources, and heightened social status"). 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." WESTIN, *supra* note 1, at 313 (quoting Donald N. Michael, *Speculations on the Relation of the Computer to Individual Freedom and the Right to Privacy*, 33 GEO. WASH. L. REV. 270, 275 (1964)).

213. *See* 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).

214. *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, 9–10 ("Having some information about yourself 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 trustworthy third parties. Such storage of information can dramatically simplify the purchasing experience . . . .").

215. *See* Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1248–49, 1249 n.113 (2002).

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, and others constantly collect personal information, also limits the quality of choice.[216] Professor Paul Schwartz presciently explained, more than a decade ago, how the Information Age architecture can impede meaningful consent to the release of PII.[217] Schwartz noted how the "liberal ideal" perspective assumed that individuals could protect their privacy (and thus autonomy) by controlling access to their personal information.[218] The reality, Schwartz was beginning to see, was that a power imbalance between the individual and the entities that collected the information produced an environment in which individuals had little choice but to reveal certain information to private actors.[219] The ability to keep data secure to oneself, Schwartz noted, "quickly proves illusory because of the demands of the Information Age."[220]

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."[221] Second, the "consent fallacy," which consists of "weaknesses in the nature of agreement to data use."[222] And third, the "autonomy trap."[223] Schwartz's 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."[224] The problem with privacy control in the Information Age, though, "is that individual self-determination is itself shaped by the processing of personal data."[225]

As an example, Schwartz discussed the online "click wrap" agreement.[226] As Schwartz explained, clicking through a consent page "may be considered by some observers to be an exercise of self-reliant choice" online.[227] But the screen could (and often does)

---

216. Cohen, *supra* note 79, 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.").

217. *See* Schwartz, *supra* note 87, at 1684.

218. *See id.* at 1662.

219. *See id.* at 1662–63.

220. *Id.* at 1663.

221. *Id.* at 1660.

222. *Id.*

223. *Id.*

224. *Id.*

225. *Id.* at 1661.

226. *See id.*

227. *Id.*

contain boilerplate language permitting "all further processing and transmission of one's personal data."[228] 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's example, this produces a "legal fiction that all who visit [a] Web site have expressed informed consent to its data processing practices."[229] Thus, Schwartz's 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 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 how well it is protected. Some federal statutes—notably, the Health Insurance Portability and Accountability Act ("HIPAA"), the Gramm-Leach-Bliley Act, and the Federal Information Security Management Act ("FISMA")—*do* require certain security standards.[230] 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.[231] Perhaps not surprisingly, Americans seem to be losing faith in the degree to which their information 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."[232]

2. *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 individuals must make the choice to enjoy fundamental benefits and that the

---

228. *Id.*

229. *Id.* at 1662.

230. *See* 44 U.S.C. § 3541 (2012) (requiring federal agencies to develop and implement security programs for the protection of data); 16 C.F.R § 314 (2015) ("Safeguards Rule" applying to Gramm-Leach-Bliley Act); 45 C.F.R. § 164 (2014) (security rule relating to HIPPA).

231. Although some federal laws do mandate "reasonable" levels of security, enforceable by the FCC (see Communications Act, 47 U.S.C. §§ 201, 222 (2012)) and the FTC (see Federal Trade Commission Act, 15 U.S.C. § 45 (2012)). The FTC's action in this realm is discussed below.

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

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."[233] At one end, extreme and physical coercion, such as torture or rape, is widely condemned.[234] The law also acts to prevent subtler psychological forms of coercion —for instance, through laws criminalizing blackmail and extortion.[235] With torture, the act itself constitutes battery, a physical harm illegal in and of itself.[236] 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 coerces the victim into a position in which he is likely to do something independently illegal (for instance, steal from a third party), and thus harm society.[237]

The transfer of PII does not share these traits. Mere 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 with—disclosure of 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.[238]

Instead, what we associate negatively with this particular type of coercion is the attendant reality that the PII recipient then does not protect people's information 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)

---

233. M. Ryan Calo, Essay, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1150 (2011).

234. Ivana Radačići, *Does International Human Rights Law Adequately Protect the Dignity of Women?*, *in* HUMILIATION, DEGRADATION, DEHUMANIZATION: HUMAN DIGNITY VIOLATED 119, 119 (Paulus Kaufmann et al. eds., 2011) ("[R]ape has long been thought of as a prime example of a violation of human dignity."); David Sussman, *What's Wrong with Torture?*, 33 PHIL. & PUB. AFF. 1, 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.").

235. *See, e.g.*, 18 U.S.C. § 873 (2012) (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.").

236. *Battery*, BLACK'S LAW DICTIONARY (10th ed. 2014).

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

238. Madden, *supra* note 235 ("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.").

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 Storage 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 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 PII?

1. Harm Requires Awareness

Insecurity, or "carelessness in protecting stored information," as Solove notes, *can* constitute an injury: "being placed in a weakened state, of being made more vulnerable to a range of future harms."[239] Yet, if and until a person is *aware* of the insecurity of their PII, no harm has occurred.[240] Data insecurity may lay the groundwork for future harm in the form of the breach itself, but until an individual is conscious of his vulnerability, he has not been harmed.[241]

---

239. Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 490, 519 (2006).

240. To argue that the individual is not harmed in this situation is not to argue that no "wrong" has occurred. Society often criminalizes behavior deemed *malum in se* ("wrong in itself") even if the victim of the wrongful act is unaware he has been wronged. *See* Richard L. Gray, Note, *Eliminating the (Absurd) Distinction Between* Malum in Se *and* Malum Prohibitum *Crimes*, 73 WASH. U. L. Q. 1369, 1373–74 (1995) (quoting *Malum in se*, BLACK'S LAW DICTIONARY (6th ed. 1990)) ("[*Malum in se* is a] wrong in itself; an act or case involving illegality from the very nature of the transaction, upon principles of natural, moral, and public law . . . . An act is said to be *malum in se* when it is inherently and essentially evil, that is, immoral in its nature and injurious in its consequences, *without any regard to the fact of its being noticed* or punished by the law of the state." (emphasis added)). The production and distribution of child pornography, for example, is illegal regardless of whether the child is aware of his victimization; the abuse is regarded as being "repugnant to the moral instincts of a decent people" and is thereby illegal regardless of the victim's awareness. Ashcroft v. Free Speech Coal., 535 U.S. 234, 244 (2002). For a discussion of the ethics in data security, see generally Philip Brey, *Ethical Aspects of Information Security and Privacy*, *in* SECURITY, PRIVACY, AND TRUST IN MODERN DATA MANAGEMENT 21 (Milan Petković & Willem Jonker eds., 2007). It is worth noting here that this Article is concerned with whether an individual is harmed—which requires the victim's awareness—and not with whether the offending act is morally wrong from a societal standpoint, which does not.

241. Another way the individual could be harmed is if he is deceived into believing that his PII is secure, and becomes aware of that deception. As noted deception interferes with a person's autonomy. *See supra* Part I, Relation to

The classic case *De May v. Roberts*[242] serves as an example. There, a man falsely presented himself as a physician while a woman was giving birth.[243] The plaintiff sued, claiming an invasion of privacy, but only after she discovered his actual identity.[244] Had she never learned of his identity, the plaintiff's sense of being violated—her harm—would have never transpired.[245] Similarly, the tort of assault also provides a common example of the link between harm and awareness, 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.[246] So too is the situation in the data breach context. Lax security standards present a problem insofar as they make a future harm—disclosure of confidential information—possible, but the data insecurity is not harmful unless the potential victims are aware of the insecurity.

Misrepresentation or deceit regarding the degree to which data is secured, however, can also be harmful. 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 as harmful. Again, *De May v. Roberts* is illustrative.[247] The plaintiff brought an invasion of privacy claim and, because the defendant invaded her personal space and saw her giving birth—thereby violating the spatial seclusion she sought to protect—the defendant did invade her privacy, so the case was decided on those grounds.[248] As the court recognized, though, the wrongful act was the defendant's deceit in failing to disclose that he was neither medically trained nor the doctor's aide, but merely a layman.[249] While this "wrong thus done"[250] entitled the woman to damages through a privacy cause of action, a court today could

---

Autonomy. This point is discussed in the context of FTC Section 5 actions. *See infra* Part III.

242. 9 N.W. 146 (Mich. 1881).

243. *Id.* at 146.

244. *Id.* at 147.

245. M. 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. *See* Calo, *supra* note 235, at 1145.

246. *See* RESTATEMENT (SECOND) OF TORTS § 21 (AM. LAW INST. 1965) (requiring "imminent apprehension" of "harmful or offensive contact").

247. *See De May*, 9 N.W. at 149.

248. Today, the plaintiff would likely advance an intrusion upon seclusion theory. *See, e.g.*, Knight v. Penobscot Bay Med. Ctr., 420 A.2d 915, 917 (Me. 1980).

249. *See De May*, 9 N.W. at 149 ("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)).

250. *Id.*

recognize the harm the woman suffered—the loss of autonomy or, put another way, the indignity—by awarding damages for a breach of confidentiality action.[251]

2. Should Law Respond?

Though inadequate security does not, standing alone, harm individuals, both law and private-sector standards and regulations recognize the harm 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.[252] 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 their reputation (and bottom line), certain industry groups impose security standards upon their members.[253] When a company does decide to publish its data security or privacy policy, the FTC holds those companies to their word through the use of its Section 5 authority to police "deceptive" practices.[254]

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

C. The Release of PII

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 pierces a security system, this surely violates the law in that the third party was not

---

251. *See* Sheldon F. Kurtz, *The Law of Informed Consent: From "Doctor Is Right" to "Patient Has Rights,"* 50 SYRACUSE L. REV. 1243, 1245 (2000) (discussing how autonomy and dignity values pervade the doctrine of informed consent in the medical context, including consent to treatment).

252. *See* Schwartz, *supra* note 87, at 1673–74 (discussing how the Cable Communications Policy Act of 1984 and the Telecommunications Act of 1996 have created safeguards to protect customers' PII).

253. For instance, the Payment Card Industry Security Standards Council imposes "Data Security Standards" on vendors who use credit and debit cards. *See* Press Release, Sec. Standards Council, PCI Security Standards Council Releases Version 1.2 of PCI Data Security (Oct. 1, 2008), http://www.pcisecuritystandards.org/pdfs/pr_080930_PCIDSSv1-2.pdf.

254. The FTC's "deceptive" and more recent "unfairness" actions in this area are discussed *infra* Part III.

granted access to the information.[255] 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 his PII has not actually been used to commit fraud? This subpart argues that such a harm manifests in an individual's loss of autonomy, specifically through the loss of knowledge regarding the choices available to individual. This loss of negative freedom inhibits the individual's actions to the extent that a concrete harm has occurred.

1. 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.[256] 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 otherwise would be able to. Not surprisingly, this harm, in the form of a loss of liberty, is easily recognizable and redressable through the legal system.[257]

But another harm exists regardless of whether the overt harm of identity theft ever occurs[258]: a lack of knowledge about freedom. As soon as the victim is aware of the data breach, the victim knows his information could be used without his consent to commit fraud or another crime. This knowledge arrests the victim's rational decision making because he cannot be sure what the criminal may or may not do with his information. Professor Boudewijn de Bruin offers an example of this process in the information security context:

> [D]isclosure 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

255. For a well-known example, see Kim Zetter, *TJX Hacker Gets 20 Years in Prison*, WIRED (Mar. 25, 2010, 2:02 PM), http://www.wired.com/2010/03/tjx-sentencing/.

256. *See* Krottner v. Starbucks Corp., 628 F.3d 1139, 1141–43 (9th Cir. 2010); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007); Miles L. Galbraith, *Identity Crisis: Seeking a Unified Approach to Plaintiff Standing for Data Security Breaches of Sensitive Personal Information*, 62 AM. U. L. REV. 1365, 1369–71, 1385–87 (2013); Vincent R. Johnson, *Credit-Monitoring Damages in Cybersecurity Tort Litigation*, 19 GEO. MASON L. REV. 113, 139–41 (2011).

257. *See supra* Part II.

258. Often, breaches expose information without any resulting identity theft. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-07-737, DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN 5 (June 2007), http://www.gao.gov/new.items/d07737.pdf ("[A]vailable data and interviews with researchers, law enforcement officials, and industry representatives indicated that most breaches have not resulted in detected incidents of identity theft.").

> 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.[259]

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."[260]

This feeling of powerlessness and vulnerability constitutes harm in itself: the victims' dignity, in terms of being free from manipulation and coercion, is impaired. 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 process of identity reclamation with the government.[261] Such physical acts incur financial costs, and the law currently recognizes this financial burden as a cognizable harm.[262] The question is then: Should the law wait to act until a financial injury accrues?

---

259. Boudewijn de Bruin, *The Liberal Value of Privacy*, 29 LAW & 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.

260. Solove, *supra* note 242, at 522.

261. De Bruin, *supra* note 262, at 509–10 (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.").

262. *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693–94 (7th Cir. 2015); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007); *In re* Adobe Sys., Inc., 66 F. Supp. 3d 1197, 1211, 1216–17 (N.D. Cal. 2014).

2. Should Law Respond?

A person's autonomy is violated in everyday life by seemingly innocuous events.[263] A white lie, for instance, can be considered a violation of the listener's autonomy, yet the law does not respond. Why should the law respond to the loss of autonomy that results from a data breach?[264] 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.[265] 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." In the Information Age, this maxim can translate to a mandate that consumers not be "used" for their PII[266] 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 the consumer may feel, such as vulnerability, anxiety, and nervousness, discussed above, if his 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 idiosyncratic infringements of autonomy that occur in day-to-day interactions with fellow citizens, data breaches cause similar harms that affect literally millions of people.[267] Not surprisingly—given the increased prevalence of data breaches—more Americans are reporting themselves as victims of breaches.[268] Thus, unlike losses of

---

263. 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. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633, 655 (Cal. 1994) (citing RESTATEMENT (SECOND) OF TORTS, § 652D, cmt. c. (AM. LAW INST. 1977)).

264. Solove, *supra* note 242, at 485 ("[D]eclaring 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.").

265. *See supra* Part I.

266. 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, 556–57 (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").

267. *See supra* Introduction.

268. Mary Madden, *More Online Americans Say They've Experienced a Personal Data Breach*, PEW RES. CTR. (Apr. 14, 2014), http://pewresearch.org/fact-tank/2014/04/14/more-online-americans-say-theyve-experienced-a

autonomy occurring in everyday private interactions, data breaches cause uniform, widely felt harms ripe for widespread legal 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.[269] As the White House recently noted in support of cybersecurity legislation: "As cybersecurity threats 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."[270] 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.[271]

D. Liberty and Privacy

Companies that face data breaches withhold knowledge of who is in possession of an individual's 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.

-personal-data-breach/ (reporting on a survey that suggested a "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").

269. *See* Solove, *supra* note 242, at 487, 521–22.

270. Michael Shear & Natasha Singer, *Obama to Call for Laws Covering Data Hacking and Student Privacy*, N.Y. TIMES, Jan. 11, 2015, at A10. 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 "nearly one-quarter of patients (21 percent) withhold personal health information from their doctors due to data security concerns." Gaby Loria, *HIPAA Breaches: Minimizing Risks and Patient Fears*, SOFTWARE ADVICE (Mar. 12, 2015), http://www.softwareadvice.com/medical/industryview/hipaa-breaches-report-2015/.

271. *See, e.g.*, *The Threat of Data Theft to American Consumers: Hearing Before the Subcomm. on Commerce, Mfg., and Trade of the H. Comm. on Energy and Commerce*, 112th Cong. 14 (2011) (statement of David C. Vladeck, Director of the Bureau of Consumer Protection at the Federal Trade Commission) ("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.").

Victims' privacy and liberty, in contrast, remain intact. First, where victims' PII have 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 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 otherwise available. But until their PII are used, the main harm that Mike and Hallie suffer is an intangible 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 have been made vulnerable, but not misused, commonly invoke state common law Invasion of Privacy claims when suing in court.[272] 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 unprovable). Many data breaches do not result in identity theft.[273] 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.

This reality was recently on display in *Storm v. Paytime, Inc.*[274] In that case, a consolidation of two class actions, the defendant computer company suffered a data breach at the hands of unknown hackers, who gained access to over 230,000 people's PII.[275] The plaintiffs alleged, inter alia, that they had suffered a "harm to their privacy interest."[276] 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."[277] Because the plaintiffs could not

272. *See* Paul Karlsgodt, *Key Issues in Consumer Data Breach Litigation*, PRAC. L.J., Oct.–Nov. 2014, at 48, 51; Sasha Romanosky, David Hoffman & Alessandro Acquisti, *Empirical Analysis of Data Breach Litigation*, 11 J. EMPIRICAL LEGAL STUD. 74, 100–01 (finding that only state unfair business practice claims, Fair Credit Reporting Act claims, breach of contract claims, and negligence claims are brought more than Privacy Act and Privacy Tort claims); *see also* Cease, *supra* note 38, 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.").

273. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 261, at 21.

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

275. *Id.* at *8–9.

276. *Id.* at *23.

277. *Id.* (citing *In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 28 (D.D.C. 2014)).

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.[278] Despite some courts' feeling that a PII recipient has wronged the individual, courts simply cannot let a suit succeed on an invasion of privacy claim.[279]

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.

III. 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 ("FTC Act") in 1914.[280] As conceived, the FTC was intended to recapture legislative control of antitrust regulation from the judiciary,[281] but in 1938, Congress passed the Wheeler-Lea Amendment, which

---

278. *Id.* at *23–24.

279. *See, e.g*, Randolph v. ING Life Ins. & Annuity, 973 A.2d 702, 710–11 (D.C. Cir. 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.").

280. The Federal Trade Commission Act, ch. 311, 38 Stat. 717 (codified as amended as 15 U.S.C. §§ 41–58 (2012)).

281. *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.").

broadened the FTC's authority to police companies' "unfair or deceptive acts or practices," on behalf of consumers.[282] Today, the Bureau of Consumer Protection brings actions against private entities it has reason to believe violate Section 5.

A deceptive practice is defined as "a representation, omission, or practice that . . . is likely to mislead consumers acting reasonably under the circumstances, and . . . the representation, omission, or practice is material."[283] Actions in which the FTC challenges a company's practice as deceptive are relatively straightforward in the data-security 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.[284] 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 when they diverge from that promised path.[285]

The term unfair, however, is notoriously broad.[286] At the time of Wheeler-Lea's passage, Congress declined to narrow its scope, purposefully maintaining vagueness so the FTC could respond to future unanticipated acts.[287] 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

---

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

283. Cliffdale Assocs., 103 F.T.C. 11 (1984); *see also* 15 U.S.C. § 45(a)(1); FTC v. Pantron 1 Corp., 33 F.3d 1088, 1095 (9th Cir. 1994).

284. *See* Scott, *supra* note 42, 132–33.

285. *See, e.g.*, Complaint at 8–9, Snapchat, Inc., No. C-4501, 2014 WL 7495798 (F.T.C. Dec. 23, 2014), 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) . . . .").

286. 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) (citing Davidson v. New Orleans, 96 U.S. 97, 104 (1877)).

287. *See* U.S. FED. TRADE COMM'N, FTC POLICY STATEMENT ON UNFAIRNESS, (Dec. 17, 1980), 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.").

authority."[288] The statement began by noting that "[u]njustified consumer injury is the primary focus of the FTC Act."[289] The Commission decided that any harm must be "substantial" and not "trivial or merely speculative."[290] 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."[291] "In most cases," the FTC explained, "a substantial injury involves monetary harm."[292] "Emotional impact and other more subjective types of harm, on the other hand, will not ordinarily make a practice unfair."[293]

The FTC acknowledged that "[m]ost business practices entail a mixture of economic and other costs and benefits for purchasers."[294] Such tradeoffs, the FTC reasoned, justified that only those practices which are "injurious in [their] net effects" warranted action.[295] 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."[296]

Lastly, the FTC explained, "the injury must be one which consumers could not reasonably have avoided."[297] Consumers could be expected in most circumstances "to make their own private purchasing decisions without regulatory intervention."[298] 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."[299] 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

---

288. *Id.*
289. *Id.*
290. *Id.*
291. *Id.* The FTC is required to show only that a company's practices "cause or are likely to cause" injury to any class of consumers. 15 U.S.C. § 45(a)(4)(a) (2012).
292. 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." U.S. FED. TRADE COMM'N, *supra* note 287. However, the FTC does not always require monetary harm. *See* FTC v. Neovi, Inc., 598 F. Supp. 2d 1104, 1115 (S.D. Cal. 2008) (citing FTC v. Accusearch, No. 06-CV-105–D, 2007 WL 4356786, at *6–7 (D. Wyo. Sept. 28, 2007) ("harm need not be monetary to qualify as an injury")).
293. U.S. FED. TRADE COMM'N, *supra* note 287.
294. *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.*
295. *Id.*
296. *Id.*
297. *Id.*
298. *Id.*
299. *Id.*

advantage of an obstacle to the free exercise of consumer decision making."[300]

Congress codified the policy statement in 1994[301] 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."[302] That three-part cost-benefit test "is the most precise definition of unfairness articulated by either the Commission or Congress."[303]

B. The FTC's Unique Position to Respond

As this Article 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 when the PII has not been used to commit identity theft.[304] This Subpart argues that the FTC is better able to respond to data breach harm than are individual plaintiffs for two reasons: it is not hindered by the standing requirement, and it can redress a small harm widely felt.

1. The FTC Does Not Have to Show Standing

Data breaches cause dignity harms to the victims whose information is made vulnerable, and these harms manifest in feelings of anxiety, vulnerability, and distress. Yet, federal courts have thus far not recognized a private remedy for a consumer when the PII recipient's failure to adequately protect the PII results in a breach, but the PII has not yet been misused, at least to the consumer's knowledge.[305] This is because the federal courts' standing doctrine requires plaintiffs to show that an injury is concrete, particularized, and actual or imminent.[306] In *Clapper v. Amnesty International*,[307] the Supreme Court considered plaintiffs' claims that the government's surveillance program constituted an unconstitutional search and seizure—but plaintiffs could not show that their particular communications had been viewed, only that such surveillance was likely because of their particular actions.[308]

---

300. *Id.*

301. *See* H.R. REP. NO. 103-617, at 12 (1994) (Conf. Rep.).

302. 15 U.S.C. § 45(n) (2012).

303. Brief for the FTC, FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014) (No. 14-3514), 2014 WL 6629142, at *5 (citing Am. Fin. Servs. Ass'n v. FTC, 767 F.2d 957, 972 (D.C. Cir. 1985)).

304. *See* Reilly v. Ceridian Corp., 664 F.3d 38, 45 (3d Cir. 2011).

305. Brief of Amici Curiae Pub. Citizen, Inc., Cent. for Dig. Democracy et al. in Support of Plaintiff-Appellee Fed. Trade Comm'n Urging Affirmance at *4–5, FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602 (D.N.J. 2014), 2014 WL 6629143.

306. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147 (2013).

307. *Id.*

308. *Id.*

The Court held that fear of some future harm was not sufficient, in itself, to achieve standing.[309] In the wake of *Clapper*, most federal courts have held that an increased *risk* of future harm—the future harm being identity theft—is not enough to confer standing.[310]

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. Additionally, 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.[311] But courts simply cite to *Clapper* for the proposition that the plaintiffs cannot "manufacture" their injury in fear of a speculative future harm.[312]

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.[313] The FTC can bring adjudicative claims against companies it suspects of violating Section 5's prohibition of "unfair or deceptive" trade practices, or it may file in federal court.[314] If the party receiving the complaint disputes the FTC's authority or the complaint against it, the party may appeal to an adjudicatory board and, if it disputes that court's finding, may appeal to federal court.[315]

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 in selectively targeting companies that store large amounts of PII or those whose errors in data security were

309. *Id.*

310. *See Reilly*, 664 F.3d at 43.

311. *See, e.g.*, *id.* at 40.

312. *See, e.g.*, Peters v. St. Joseph Servs. Corp., 74 F. Supp. 3d 847, 855 (S.D. Tex. 2015) (citing *Clapper*, 133 S. Ct. at 1151).

313. 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'N (July 2008), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.

314. *Id.*

315. 15 U.S.C. § 45(b), (c) (2012).

especially egregious.[316] These actions are valuable insofar as they induce other companies to react accordingly out of fear of receiving their own FTC complaint.[317]

2. Small Harms, Widely Felt

The FTC is also uniquely situated to respond to data breaches because it is designed 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."[318] This is especially appropriate in the data breach context when, 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.[319] 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.[320]

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.[321] This Subpart argues that the FTC should frame the harm in the data breach context—at least where there is no identity theft—as harm to victims' dignity, as opposed to their privacy, for two reasons. 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.

---

316. Daniel Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 605 (2014).

317. *Id.* at 606.

318. U.S. FED. TRADE COMM'N, *supra* note 287. The FTC is required to show only that a company's practices "cause or are likely to cause" injury to any class of consumers. 15 U.S.C. § 45(a) (2012).

319. *See* Thomas B. Leary, *The FTC and Class Actions* (June 26, 2003), 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).

320. *See* Solove & Hartzog, *supra* note 318, at 613–19 (discussing the usual requirements of consent decrees).

321. FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 607 (D.N.J. 2014).

1. 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.[322] 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 BJ's Company when BJ's failed to encrypt its customers' information and use other "readily available security measures."[323] Hackers were able to pierce BJ's security system and use its customers' PII to rack up $13 million in fraudulent charges.[324] Instead of challenging the FTC that "unreasonable" security standards were not "unfair," as defined by Section 5, BJ's settled, entering into a consent decree.[325] In the decade since, twenty companies that had received FTC complaints for "unfair" data-security practices ended up doing the same.[326]

However, each of these breaches resulted in identity theft and consequent financial loss.[327] The FTC seemed to be limiting its authority to only those instances where financial harm occurred—thus, indirectly defining "unfairness" and consumer injury as requiring 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 Article has sought to show, the FTC would therefore be failing to respond to the harm that occurs even where there is no alleged identity theft or financial loss.

More recently, the FTC seems to have changed its approach. In 2013, the FTC filed an administrative complaint against LabMD, a health care 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.[328] The information was later

322. See Schwartz & Solove, *supra* note 13, at 1856–57.

323. Complaint at 2, BJ's Wholesale Club, Inc., No. C-4148, WL 1541551 (F.T.C. Sept. 20, 2005), http://www.ftc.gov/os/caselist/0423160/092305comp0423160.pdf.

324. Press Release, FTC, BJ's Wholesale Club Settles FTC Charges (June 16, 2005), https://www.ftc.gov/news-events/press-releases/2005/06/bjs-wholesale-club-settles-ftc-charges.

325. Agreement Containing Consent Order at 1, BJ's Wholesale Club, Inc., No. 0423160 (F.T.C. May 17, 2005), https://www.ftc.gov/enforcement/cases-proceedings/042-3160/bjs-wholesale-club-inc-matter.

326. *See* Complaint Counsel's Response in Opposition to Respondent's Motion to Dismiss Complaint with Prejudice and to Stay Administrative Proceedings, at v–vi, LabMD, Inc., No. 9357 (F.T.C. Nov. 22, 2013), https://www.ftc.gov/sites/default/files/documents/cases/131122ccoppositiontormotiontodismiss.pdf (listing the FTC's unfairness cases).

327. *Id.*

328. Complaint at 4, LabMD, Inc., No. 9357 (F.T.C. Aug. 19, 2013), https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter.

found in the possession of individuals who pleaded no contest to identity theft charges.[329] Importantly, the FTC did not base its action on the occurrence of identity theft; instead, the FTC's allegation seemed to imply that the allegedly "unreasonable" security program which made the patients' information vulnerable, in and of itself, constituted an unfair practice.[330] 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 not reasonably avoidable by consumers. This practice was, and is, an unfair act or practice."[331]

In November 2015, the presiding administrative law judge dismissed the FTC's complaint.[332] The judge held that "the evidence fails to prove that the limited exposure of the [P2P files] has resulted, or is likely to result, in any identity theft-related harm . . ." and that it failed to prove the FTC's "contention that embarrassment or similar emotional harm is likely to be suffered from the exposure of the [files] alone."[333] "Even if there were proof of such harm," the judge noted, "this would constitute only subjective or emotional harm that, under the facts of this case, where there is no proof of other tangible injury, is not a 'substantial injury' within the meaning of Section 5(n)."[334] The judge seized on the fact that no identify theft had occurred and that the FTC had not shown that it was likely—thus, the judge challenged the FTC to show how vulnerability, without more, constitutes a harm.

The decision has been regarded as a big setback for the FTC, because it relegates the FTC's enforcement power to that of ordinary

---

> 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.

329. *Id.* at 5.

330. 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.* (emphasis added).

331. *Id.*

332. *See* Initial Decision at 51, LabMD, Inc. No. 9357 (F.T.C. Nov. 13, 2015), https://www.ftc.gov/system/files/documents/cases/151113labmd_decision.pdf.

333. *Id.*

334. *Id.* at 13.

plaintiffs who often struggle to show concrete financial harm before being granted standing to sue in federal court.[335] The judge's narrow view of harm has, for the moment, posed an obstacle to the FTC's cyber-security agenda.[336]

But the FTC has appealed the decision. In its December 2015 brief, the FTC argued that the judge had erred by failing to recognize that "significant risk of concrete harm itself causes substantial consumer injury within the meaning of Section 5(n)" and that the Judge had failed to evaluate how LabMD's "multiple, systemic, and serious data security failures created a significant risk of concrete harm."[337] Notably, the FTC has tried a different approach, arguing that one of the harms was to a consumer's privacy interests.[338] It has also argued forcefully that "significant risk of concrete harm is substantial injury in itself."[339] The oral arguments for the FTC's appeal were being scheduled as this Article went to press.

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

LabMD has challenged the FTC: How are consumers harmed if their PII have not been used to commit identity theft? Some, including LabMD, believe the FTC may be exceeding the role set for it by Congress.[340] 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"—especially where the practices never led to viewership or identity theft.[341]

---

335. *Id.*

336. Allison Grande, *FTC's Data Security Authority Limited in LabMD Ruling* LAW360.COM (last accessed Nov. 18 10:38 PM), http://www.law360.com/articles/727969/ftc-s-data-security-authority-limited-in-labmd-ruling (noting a practitioner's claim that "[t]his is a very important decision because it essentially equates the FTC's enforcement requirements with the same kinds of standards that private litigants must meet in connection with data breach cases").

337. *See* Complaint Counsel's Appeal Brief at 10, Lab MD Inc., No. 9357 (F.T.C. Dec. 22, 2015).

338. *Id.* at 20, 39–41. It is unclear whether the FTC is arguing that privacy interests were harmed by the disclosure of the 1718 file—which actually was viewed by a third party (and thus could be an invasion of privacy)—or whether the mere exposure constituted a privacy harm. *See id.* at 40 ("In addition to the evidence described above, which shows that it is very likely the 1718 File was accessed by unauthorized third parties, the uncontroverted evidence in this case establishes that it was accessed and downloaded by at least one unauthorized third party.").

339. *Id.* at 12–14.

340. *See, e.g.*, David Alan 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, 9.

341. *See, e.g.*, Editorial, *Hacking Victims Become Federal Targets*, WALL STREET J., Aug. 18, 2014, at A12 ("The problem with [the FTC's] reasoning is

The FTC should respond that injuries occur in the form of a harm to dignity, putting consumers in the unfortunate position of doubting the security of their PII. Doing so stays true to the common understandings of privacy and dignity, while also positioning the FTC in a traditional role as protector of consumer dignity.

a. 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.[342] This is no doubt influenced by the reality that privacy-related claims are popular among plaintiffs suing in private actions.[343]

Privacy, however, is not the interest at stake where no identity theft has occurred. Individuals' privacy is arguably invaded when their PII are 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.[344] Although viewing the information for use to commit a further crime certainly occurs in some breaches, it does not occur in all. Thus, if harm is defined only in terms of privacy, any harm an individual experiences would be neglected if the individual (or FTC) cannot prove viewership of the PII.

In contrast, harm to dignity 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 suspended state of anxiety and fear stemming from the loss of negative freedom regarding what the unknown hacker may do with the information.

Not only is conceptual clarity necessary to both affirm common understandings of what each of privacy and dignity means, but it is also necessary to understand how best to remedy invasions of each. As Daniel Solove notes, "Using 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

---

that the companies targeted by the FTC were the *victims* of 'deceptive' hacking acts. But in FTC land they are guilty of an unfair trade practice . . . .").

342. *See, e.g.*, Order Denying Respondent LabMD's Motion to Dismiss at 7, LabMD, Inc., No. 9357, (F.T.C. Nov. 22, 2013), https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter ("[T]he Commission has been involved in addressing online privacy issues for almost as long as there has been an online marketplace.").

343. *See* Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633, 654–55 (Cal. 1994).

344. *See supra* Part I.

policymakers from addressing the issues before them."[345] 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.

b. 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 never directed it to go.[346] 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.

The FTC's 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.[347] In addition, the FTC also has a long history of protecting consumer dignity by pursuing deception through the form of false advertising.[348] And even its unfairness claims have historically

345. Solove, *supra* note 242, at 486; *see also*, Calo, *supra* note 236, at 1137 (the "overuse" of privacy "risks its diffusion into a meaningless catchall").

346. *See, e.g.*, Brief of Wyndham Worldwide Corp. at 1, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (2015) (No. 14-3514) ("The FTC's brief proposes a breathtaking expansion of agency authority.").

347. *See, e.g.*, Complaint Counsel's Response in Opposition to Respondent's Motion to Dismiss Complaint with Prejudice and to Stay Administrative Proceedings, *supra* note 328, at 3 ("Specifically, the Complaint alleges that Respondent failed to employ reasonable and appropriate measures to prevent unauthorized access to consumers' personal information.").

348. *See* Mary L. Azcuenaga, The Role of Advertising and Advertising Regulation in the Free Market at the Turkish Association of Advertising Agencies, Conference on Advertising for Economy and Democracy (Apr. 8, 1997), 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").

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) postpurchase rights and remedies."[349] 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 consumer can come to his 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 his 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."[350] 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 reconceptualize 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.[351] Vladeck noted how behavioral advertising could

---

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

350. *See* J. Howard Beales, The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection at the Marketing and Public Policy Conference (May 30, 2003), https://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection.

351. *An Interview with David Vladeck of the F.T.C.*, 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

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."[352] 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 fit more within the FTC's traditional role.

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 FTC 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 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 the FTC as fulfilling the role it always has: protecting consumer dignity.

---

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").

352. *Id.*