UNC SCHOOL OF LAW

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY

Volume 23 | Issue 1 Article 2

10-1-2021

Psychological Data Breach Harms

Ido Kilovaty

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 23, ISSUE 1: OCTOBER 2021

PSYCHOLOGICAL DATA BREACH HARMS

Ido Kilovaty*

Cybersecurity law, both in statutory and case law, is primarily based on the premise that data breaches result exclusively in financial harms. Intuitively, legal scholarship has largely focused on financial harms to the exclusion of non-financial harms—emotional and mental—that also arise from data breaches. A critical mass of research in psychology, psychiatry, and internet studies shows that consumers whose information has been compromised suffer from serious emotional and mental conditions as a result. This Article seeks to evaluate cybersecurity law in light of this reality and proposes a framework to address these psychological data breach harms.

Psychological data breach harms raise significant challenges for which the law does not adequately account. Consumers suffering these harms are unlikely to pursue litigation and, even if consumers do pursue litigation, are unlikely to prevail because of both standing and cause of action reasons. In a similar vein, different cybersecurity law frameworks, such as the Computer Fraud and Abuse Act, data security laws, data breach notification laws, and Federal Trade Commission enforcement, do not generally recognize harms that are non-monetary in nature. Moreover, companies suffering data breaches are not legally required to offer any assistance to, or mitigation response for, consumers who suffer psychological harms. Contributing to these challenges is the fact that breached companies are often not even required to disclose breaches that are unlikely to cause future financial harm.

Cybersecurity law currently overlooks a conceptual framework for psychological data breach harms; this Article offers that

* Frederic Dorwart and Zedalis Family Fund Associate Professor of Law, University of Tulsa, College of Law; Visiting Faculty Fellow, Center for Global Legal Challenges, Yale Law School; Affiliated Fellow, Information Society Project, Yale Law School. The author wishes to thank the University of Tulsa College of Law for providing a summer research grant to support this project.

framework. First, this Article argues for the recognition of psychological data breach harms in the context of cybersecurity from the very outset. Second, this Article makes concrete recommendations on how psychological data breach harms ought to be addressed, both by regulators and breached entities, as well as recommends the appropriate remedies. Finally, this Article calls for a reconsideration of what "personal information" means and for the expansion of information categories that cybersecurity law should protect.

TABLE OF CONTENTS

I. INTRODUCTION

Data breaches happen more or less on a daily basis.[1] Millions,[2] and even billions,[3] of compromised sensitive consumer records have

[1] In 2019, there were 1,506 data breaches in the United States, with a total of 164 million records exposed. *See Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 1st Half 2020*, STATISTA (Aug. 2020), https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ [https://perma.cc/LA5H-SKUE].

[2] Josh Fruhlinger, *Equifax Data Breach FAQ: What Happened, Who Was Affected, What Was the Impact?*, CSO (Feb. 12, 2020), https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html [https://perma.cc/8MUJ-V38R] (narrating an overview of the Equifax breach, affecting at least 143 million consumers).

[3] Nicole Perlroth, *All 3 Billion Yahoo Accounts Were Affected by 2013 Attack*, N.Y. TIMES (Oct. 3, 2017), https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html [https://perma.cc/RKZ6-WMD5]

already affected the largest and most popular companies, as well as their consumers.[4] The impact of these breaches is often quantified in monetary terms[5] by focusing on either the damage caused to the victim company or the individual financial harm suffered by the victim company's consumers. However, too often, the law and policy on cybersecurity ignore the mental, emotional, and non-financial harms that consumers experience or may experience in the future as a direct result of a data breach.[6] This Article refers to these harms collectively as "psychological data breach harms."

While financial harms resulting from data breaches are surely important, those harms have been the sole focus of cybersecurity law to the exclusion of psychological data breach harms. The mental and emotional impact on consumers has been increasingly studied and documented in recent years.[7] However, actual misuse of

(describing the Yahoo data breach which affected three billion users' personal information).

[4] Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO (Jan. 8, 2021), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html [https://perma.cc/3Z2W-X3EF] (naming popular companies who have been breached, including eBay, LinkedIn, Marriot, Adobe, and others).

[5] *See generally Cost of a Data Breach Report 2020*, IBM (July 2020), https://www.ibm.com/security/data-breach [https://perma.cc/3RGX-7SYY] (calculating the average data breach cost at 3.86 million USD globally and 8.64 million USD in the United States).

[6] *See, e.g.*, Maria Bada & Jason R.C. Nurse, *The Social and Psychological Impact of Cyber-Attacks*, *in* EMERGING CYBER THREATS AND COGNITIVE VULNERABILITIES 73, 82 (Benson, McAlaney eds., 2020) ("Research indicates that current forms of cyberattacks can cause psychological impact . . . Depending on who the attackers and the victims are, the psychological effects of cyber threats may even rival those of traditional terrorism . . . Victims of online attacks and crime can suffer emotional trauma which can lead to depression. There is also some evidence of limited symptoms of acute stress disorder (ASD) in victims of crime in online virtual worlds, such as some anecdotal accounts of intrusive memories, emotional numbing and upset from victims of virtual sexual assault . . . .").

[7] *Id.*; *see also* Michael L. Gross et al., *The Psychological Effects of Cyber Terrorism*, 72 BULLETIN ATOMIC SCIENTISTS 284, 284 (2016) (arguing that psychological effects of cyber threats can rival those of traditional terrorism); Jessica Guynn, *Anxiety, Depression and PTSD: The Hidden Epidemic of Data Breaches and Cyber Crimes*, USA TODAY (Feb. 24, 2020), https://www.usatoday.com/story/tech/conferences/2020/02/21/data-breach-tips-mental-health-toll-depression-anxiety/4763823002/ [https://perma.cc/69F2-

compromised information is not always required in order for consumers to experience psychological harm. Such misuse may include doxing,[8] cyberstalking,[9] medical identity theft,[10] disclosure of sensitive information, and manipulation and microtargeting.[11] These forms of misuse are not all recognized by existing law, and cybersecurity law currently does not fully address psychological data breach harms that victimized consumers undoubtedly experience as a result of such misuse.

Cybersecurity law includes several smaller components that seek to achieve different goals.[12] Some of these goals include

---

LQSJ] (listing the many emotional and psychological consequences of data breaches); Ioannis Agrafiotis et al., *A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate,* 4 J. CYBERSECURITY 1, 7 (2018) (recognizing that, in the context of data breaches, "Psychological harm (i.e. harm which focuses on an individual and their mental well-being and psyche)," among other forms of harm, in the context of data breaches); Eleanor Dallaway, *#ISC2Congress: Cybercrime Victims Left Depressed and Traumatized*, INFO. SEC. (Sep. 12, 2016), https://www.infosecurity-magazine.com/news/isc2congress-cybercrime-victims/ [https://perma.cc/ES64-8JWH] (observing that victims of data breaches are experiencing trauma).

[8] *See* Josh Fruhlinger, *What Is Doxing? Weaponizing Personal Information*, CSO (Aug. 31, 2020), https://www.csoonline.com/article/3572910/what-is-doxing-weaponizing-personal-information.html [https://perma.cc/L896-S2UH] ("The quickest route to finding and weaponizing personal information about a target may be to simply buy it, whether from legal, if shady, data brokers or from databases passed around on the dark web derived from the innumerable data breaches that afflict companies large and small.").

[9] *See* Jim Reed, *EE Data Breach 'Led to Stalking'*, BBC (Feb. 8, 2019), https://www.bbc.com/news/technology-46896329 [https://perma.cc/NX9C-MMEE] (telling the story of a woman who was stalked by her ex-partner after he accessed her personal data without permission).

[10] *See, e.g.*, Pam Dixon & John Emerson, *The Geography of Medical Identity Theft*, WORLD PRIV. F. (Dec. 12, 2017), https://www.ftc.gov/system/files/documents/public_comments/2018/01/00037-142815.pdf. [https://perma.cc/58Y2-25HP] (explaining the crime of medical identity theft and impacts on the victims of the crime).

[11] *See, e.g.*, Ido Kilovaty, *Legally Cognizable Manipulation*, 34 BERKELEY TECH. L.J. 449, 453 (2019) (explaining phenomenon of online manipulation through psychographic profiling).

[12] *See generally* Orin Kerr, *What is 'Cybersecurity Law'?*, WASH. POST (May 13, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015

preventing data breaches,[13] compensating victims,[14] penalizing perpetrators,[15] and increasing transparency.[16] Throughout cybersecurity law, psychological data breach harms have little to no role to play. For example, computer crime law makes a computer-related act a criminal offense only when the information involved, or the damage done to a system, results in quantifiable financial or physical harm but does not, however, include emotional or mental harms in the definitions of "loss,"[17] "damage,"[18] or "value."[19]

Similarly, the Federal Trade Commission ("FTC"), the primary federal enforcement authority in data security,[20] does not consider consumers' mental and emotional harms resulting from data breaches to be an "injury."[21] Thus, the FTC's enforcement has focused primarily on cases where the injury—actual or potential—is financial or physical. The same logic extends to federal and state

/05/14/what-is-cybersecurity-law/ [https://perma.cc/XXR5-27X6] (explaining four basic topics of cybersecurity and components within each basic topic).

[13] *See, e.g.*, CAL. CIV. CODE § 1798.81.5 (requiring that businesses "[i]mplement and maintain reasonable security procedures and practices appropriate to the nature of the information").

[14] *See, e.g.*, 18 U.S.C. § 1030(g) (creating a private cause of action for data breach victims).

[15] *See, e.g.*, *id.* § 1030(a) (creating computer-related offenses).

[16] *See, e.g.*, N.Y. GEN. BUS. LAW § 899-AA (example of data breach notification laws).

[17] *See* 18 U.S.C. § 1030(e)(11) (defining loss as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service").

[18] *See id.* § 1030(e)(8) (defining damage as "any impairment to the integrity or availability of data, a program, a system, or information").

[19] The CFAA does not define value, though throughout the statute, the value to enhance an offense to a felony offense often includes loss of information valued at $5,000 or more. *See, e.g.*, *id.* § 1030(c)(2)(B)(iii).

[20] *See* FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 613 (D.N.J. 2014) ("[T]he FTC's . . . authority over data security can coexist with the existing data-security regulatory scheme.").

[21] FTC, FTC POLICY STATEMENT ON UNFAIRNESS (Dec. 17, 1980), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness [https://perma.cc/856U-ZLDF] [hereinafter FTC POLICY STATEMENT ON UNFAIRNESS] ("Emotional impact and other more subjective types of harm, on the other hand, will not ordinarily make a practice unfair.").

data security statutes, which require "reasonable" cybersecurity measures to protect sensitive information of a financial[22] or medical[23] nature.[24]

Finally, under data breach notification law, a company that has fallen victim to a data breach may not even be required to disclose the data breach if the company determines that the accessed information does not qualify as "personal information" or if there is no risk of financial harm to affected consumers.[25] Moreover, even when breached entities acknowledge a data breach and offer assistance to their consumers, the tools offered to mitigate any potential harm are often designed to address future financial harm.[26] Credit monitoring, for example, is often provided at no cost to consumers whose compromised information may put them at risk for identity theft or financial fraud.[27] This Article challenges this approach to mitigating potential harm because the approach offers

---

[22] *See* 16 C.F.R. § 313.3(n) (defining nonpublic personal information as part of the Safeguards Rule as "(i) Personally identifiable financial information; and (ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available").

[23] *See* 45 C.F.R. § 160.103 (defining protected health information for the purposes of the Health Insurance Portability and Accountability Act).

[24] *See, e.g.*, CAL. CIV. CODE § 1798.81.5 (requiring that California businesses implement and maintain reasonable security procedures and practices to protect California residents' "personal information").

[25] *See, e.g.*, FLA. STAT. § 501.171(4)(c) (providing, as part of the Florida data breach notification statutes, that "notice to the affected individuals is not required if, after an appropriate investigation and consultation with relevant federal, state, or local law enforcement agencies, the covered entity reasonably determines that the breach has not and will not likely result in identity theft or any other financial harm to the individuals whose personal information has been accessed.").

[26] *See* Robert Schoshinski, *Equifax Data Breach: Pick Free Credit Monitoring*, FED. TRADE COMM'N (Jul. 31, 2019), https://www.consumer.ftc.gov/blog/2019/07/equifax-data-breach-pick-free-credit-monitoring [https://perma.cc/5MDA-9SDJ] (explaining that consumers may ask for Equifax to provide them with complimentary credit monitoring as a result of a data breach).

[27] *See, e.g.*, MASS. GEN. LAWS ch. 93H § 3A (2019) (requiring that breached entities provide affected residents with "credit monitoring services at no cost to said resident for a period of not less than 18 months" under the Massachusetts data breach notification statute).

remedies that are insufficient for the needs and experiences of those consumers suffering from emotional and mental conditions as a result of a data breach. This approach currently pervades the entirety of cybersecurity law.

The absence of psychological data breach harms within the scope of cybersecurity law is not necessarily intentional. Cybersecurity law largely evolved in an era where data breach harms were believed to have involved only financial damage or damage to computers.[28] Only recently have the psychological harms of data breaches surfaced and gained more attention from researchers.[29] Law and policy have lagged behind this revelation, offering frameworks and solutions that have little to do with the true extent of data breach harms.[30] Undoubtedly, data breaches cause harm to the entity suffering the breach.[31] These harms include the costs of responding to a data breach and mitigating its effect, such as patching the vulnerability, training employees, disclosing the breach, hiring forensic experts, and more.[32] These mitigation measures are all significant costs that the victim entity needs to

---

[28] *See The Morris Worm: 30 Years Since First Major Attack on the Internet*, FBI (Nov. 2, 2018), https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218 [https://perma.cc/VPA9-FAYW] (telling the story of the first known malware, the Morris Worm, which caused damage to 6,000 out of the 60,000 computers that were then connected to the internet and subsequently led to Morris Worm facing charges in 1989 under the 1986 Computer Fraud and Abuse Act).

[29] *See, e.g.*, Bada & Nurse, *supra* note 6, at 82 (surveying recent research indicating that "cyberattacks can cause psychological impact.").

[30] *See generally* Jeff Kosseff, *Hacking Cybersecurity Law*, 2020 U. ILL. L. REV. 811, 813 (2020) (arguing for a complete overhaul and rethinking of cybersecurity law).

[31] DEREK BAMBAUER ET AL., CYBERSECURITY: AN INTERDISCIPLINARY PROBLEM 73, 73 (2021) (breaking up "technology risk" into four categories: financial risk, operational risk, reputational risk, and legal risk).

[32] *See* FED. TRADE COMM'N, DATA BREACH RESPONSE: A GUIDE FOR BUSINESS 1–4 (2019) https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business-042519-508.pdf [https://perma.cc/7CGK-LWLW] (providing businesses with a roadmap for breach response, the steps of which include: "secure your operations," "fix vulnerabilities," and "notify appropriate parties").

account for during the breach, as well as in the post-breach phase.[33] The fallout of data breaches also affects consumers, who experience direct and indirect costs, such as financial theft, legal costs, credit card monitoring costs, and more.[34]

However, these significant costs represent only part of the societal problem regarding the fallout associated with a data breach. Data breach harms can manifest in depression, anxiety, post-traumatic stress disorder ("PTSD"), and other related conditions. Additionally, those harms can be delayed, or can seem small,[35] which could lead to consumers' reluctance to make use of any remedial tools offered to them. But most importantly, the current unrecognition of psychological data breach harms means that consumers have few tools to turn to once consumers experience these harms. For example, counseling and social services aimed at reducing and managing emotional and mental conditions resulting from a data breach are currently not mandated by the law, and breached entities generally do not offer counseling or social services on their own initiative.[36] Ultimately, these psychological harms, in the aggregate, represent a major societal problem for which the law does not offer any solutions.

Surely, consumers whose sensitive information was compromised in a data breach may pursue litigation against the breached entity, often in the form of a class action lawsuit that

---

[33] Ping Wang et al., *Economic Costs and Impacts and Business Data Breaches*, 20 ISSUES INFO. SYS. 162, 165–66 (2019).

[34] *Id.* at 166–67.

[35] *See* Danielle Citron & Daniel Solove, *Privacy Harms* 3 (Geo. Wash. L. Sch. Pub. L. & Legal Theory, Paper No. 2021-11) [hereinafter Citron & Solove, *Privacy Harms*] (observing that privacy harms are small on the individual level but are significant when considered in the aggregate).

[36] Hugh Koch et al., *Psychological Injury, Cyber Crime and Data Breach Damages*, THE EXPERT WITNESS (Apr. 18, 2019), https://www.expertwitness journal.co.uk/medico-legal/1098-psychological-injury-cyber-crime-and-data-breach-damages [https://perma.cc/9VM7-PQEV] ("The immediate future for these types of [psychological injury] claim should allow greater recognition and support for individuals who have been placed in such invidious positions by data breaches."); *see also* Guynn, *supra* note 7 ("Employees were referred to short-term counseling to help them cope, whether they were just rattled by the breach or were overwhelmed unwinding the damage.").

consolidates the smaller harms.[37] This course of action is not without challenges. One such challenge is that plaintiffs must show actual harm to satisfy both standing[38] and cause of action requirements.[39] In some jurisdictions, a certain likelihood of future financial harm may suffice.[40] However, courts have been reluctant to recognize harms that are non-financial in nature, despite ample research showing that consumers whose personal information was compromised may suffer serious psychological harm.[41] Courts are deeply divided on the question of data breach harm in general. For example, the landmark Supreme Court case *Spokeo v. Robins* did little to clarify the standing elements in data breach cases.[42] In *Spokeo*, the plaintiff sued a website that offered information about individuals, such as their contact details, marital status, and financial details. The plaintiff argued that the website willfully violated the Fair Credit Reporting Act. The Court held that, to satisfy the constitutional Article III standing requirement, a "plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by favorable judicial decision."[43] The Court added that such injury in fact must be "concrete and particularized" and "actual or imminent, not conjectural or hypothetical."[44] In other words, without an actual injury, a plaintiff would be unable to recover any damages.

---

[37] *See* Jeff Stone, *Facebook Fails to Kill Class-Action Lawsuit Over Data Breach*, CYBERSCOOP (Jun. 24, 2019), https://www.cyberscoop.com/facebook-class-action-lawsuit-moves-forward/ [https://perma.cc/V9B5-QZXM].

[38] *See* U.S. CONST. art. III, § 2, cl. 1.

[39] *See* JEFF KOSSEFF, CYBERSECURITY LAW 73–97 (2d Ed., 2020) (listing the common causes of action in data breach cases, including negligence, negligent misrepresentation, breach of contract, breach of implied warranty, invasion of privacy, unjust enrichment, and state consumer protection laws).

[40] *See, e.g.*, Krottner v. Starbucks, 628 F.3d 1139, 1142 (9th Cir. 2010).

[41] *See, e.g.*, Gross, *supra* note 7, at 284 ("[T]he psychological effects of cyber terrorism can be just as powerful as the real thing.").

[42] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1546–48 (2016).

[43] *Id.* at 1547.

[44] *Id.* at 1548 (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992)).

The *Spokeo* decision has not been particularly illuminating in the context of data breach litigation; there is currently a split among appellate courts on whether future harm or an increased risk of harm can satisfy the standing requirement arising from Article III of the U.S. Constitution.[45] This split leads to an incoherence of the prevailing standard with wide-ranging differences among circuit courts.[46] The problem is further exacerbated by the Supreme Court's denial of certiorari in a Ninth Circuit data breach case, *Zappos.com v. Stevens*.[47] The split reflects the worrisome state of cybersecurity law when it comes to both future harms (either monetary or non-monetary) and actual, psychological data breach harms.[48]

Litigation raises a plethora of challenges in this circuit-split context and has been covered by some scholars.[49] Moreover, cybersecurity law scholarship is currently oversaturated with research on data breach litigation.[50] This Article, however, contributes to legal scholarship by looking at other areas of

---

[45] The DC, Third, Sixth, Seventh, Ninth, and Eleventh Circuits held that Article III standing is satisfied when there is a risk of future cyber harm. *See* Attias v. Carefirst, Inc., 865 F.3d 620 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018); In re: Horizon Healthcare Servs. Inc. Data Breach Litigation, 846 F.3d 625 (3rd Cir. 2017); Galaria v. Nationwide Mut. Ins. Co., 2016 WL 4728027 (6th Cir. 2016); Remijas v. Neiman Marcus Grp., 794 F.3d 688, 693 (7th Cir. 2015); Spokeo v. Robins, 867 F.3d 1108 (9th Cir. 2017); Resnick v. AvMed, Inc., 693 F.3d 1317 (11th Cir. 2012). Compare with the Second, Fourth, and Eighth Circuits holding that mere risk of harm does not satisfy Article III standing, in: Whalen v. Michaels Stores, Inc., 689 Fed. Appx. 89, 2017 WL 1556116 (2d Cir. 2017); Beck v. McDonald, 848 F.3d 262, 268 (4th Cir. 2017), *cert. denied sub nom.* 137 S. Ct. 2307 (2017); In re SuperValu, Inc., 870 F.3d 763 (8th Cir. 2017).

[46] *See e.g.*, *supra* note 45.

[47] *Zappos.com, Inc. v. Stevens*, 139 S. Ct. 1373 (2019).

[48] *See generally* Daniel Solove & Danielle Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 737 (2018) [hereinafter, Solove & Citron, *Risk and Anxiety*] (discussing courts' reluctance to consider psychological and future harms as too speculative).

[49] *Id.*

[50] *See, e.g.*, David Opderbeck, *Current Developments in Data Breach Litigation: Article III Standing after Clapper*, 67 S.C. L. REV. 599 (2016); Caroline Cease, *Giving Out Your Number: A Look at the Current State of Data Breach Litigation*, 66 ALA. L. REV. 395 (2014); Max Meglio, *Embracing Insecurity: Harm Reduction through a No-Fault Approach to Consumer Data Breach Litigation*, 61 B.C. L. REV. 1223 (2020).

cybersecurity law, though occasional references to courts and litigation will inevitably be made. Specifically, this Article focuses on psychological data breach harms that have been ignored by the rest of cybersecurity law, in both the pre-breach and pre-litigation contexts.

Cybersecurity law, in its different frameworks, does not do enough to address psychological data breach harms. A framework for cybersecurity law should exist where psychological data breach harms are recognized from the very outset—at the stage where organizations are designing and implementing their cybersecurity structures. As this Article shows, legislators, policymakers, and courts currently approach data breach harms as purely financial in nature and therefore misconstrue the emerging nature of the harm. As many recent data breaches illustrate, the nature of data breach harms is changing, and the focus on financial harms alone addresses only part of the problem. Hackers that compromise sensitive consumer information seek not only to monetize the data through fraud but also to capitalize on the compromised data through other means, some less documented than others. Some examples include doxing, algorithm training, subjugation of users to experiments, and more. Therefore, data breach harm should be understood as more than mere financial harm. Taking this perspective would, in turn, recalibrate the ways in which cybersecurity law applies before, during, and after the breach.

This Article's framework for psychological data breach harms is based on three key assumptions. First, data breaches expose consumers to emotional and mental harm. Second, data breaches lead to loss of control over personal data. Third, data breaches subjugate consumers to unknown harmful uses by wrongdoers. These assumptions, which are well-founded in literature and practice, challenge cybersecurity law's approach, as cybersecurity law fails to recognize psychological data breach harms within any of its existing frameworks. The proposed framework also responds to specific inadequacies in law and policy on the question of data breach harm by looking at both statutory law and regulatory approaches to data breaches. To be clear, this framework does not argue for the inclusion of all harms in the category of cognizable, litigable, enforceable injuries, but rather, argues that lawmakers,

regulators, and courts should modify their approach to harm in the context of data breaches. To achieve this goal, this Article's proposed framework offers a conceptual reform that, (1) embeds the risk of psychological harm in the risk assessment stage, (2) considers the scarcity of compromised information in addition to its sensitivity, (3) expands the meaning of "personal information," (4) detaches psychological harm from data misuse, and (5) distinguishes psychological harm from physical harm.

This Article offers a contribution to legal scholarship that has not been fully addressed up to this point. So far, cybersecurity law scholarship has focused primarily on the existence or likelihood of financial harm and the ways to mitigate such harm. Some scholarship has been published on mental harms, such as anxiety in the litigation context,[51] though a broader survey of cybersecurity law as a whole has not yet been conducted. To a large extent, this lack of scholarship is intuitive, since many harmful uses of compromised data are just now becoming better understood and studied. This Article dispels some of the dated misconceptions that have confounded lawmakers, courts, and regulators in the context of psychological data breach harms.

This Article proceeds in three parts. Part II introduces psychological data breach harms. Part III defines cybersecurity law, an area of law that is often misunderstood or conflated with privacy law. Additionally, this definitional primer highlights the concept of "harm" within these areas of cybersecurity law, which lacks the proper robustness to deal with psychological data breach harms. This Part fleshes out some of cybersecurity law's current inadequacies, to which the proposed framework responds. Part IV offers a framework for cybersecurity law to address psychological data breach harms, proposing a modification of existing concepts. Accordingly, the proposed framework offers ways to rethink psychological data breach harms.

II. PSYCHOLOGICAL DATA BREACH HARMS

"Harm" is among the central concepts in law, broadly understood as "[i]njury, loss, damage; material or tangible

[51] Solove & Citron, *Risk and Anxiety*, *supra* note 48, at 753.

detriment."[52] In law, harms can be either tangible or intangible in nature, though their recognition as recoverable or litigable harms may vary depending on different factors, such as jurisdiction and the harm's nature and concreteness.[53]

Here, "psychological data breach harms" means those harms that occur as a result of a cybersecurity incident involving personal data. While breaches are most commonly understood as events that involve the compromise of sensitive information, other types of incidents qualify as data breaches even when no sensitive information was accessed. Examples include a distributed denial-of-service attack[54] ("DDoS") that overwhelms the target with bogus requests or a ransomware attack that locks sensitive data out of the owner's or fiduciary's reach.[55] As Jeff Kosseff aptly observed, a ransomware attack would not obligate the company "to warn consumers or assist them with alternative arrangements, since consumers did not suffer a breach of sensitive information."[56] In other words, a data breach occurs whenever users lose control over their personal information, whether due to theft or unavailability, caused by DDoS, ransomware, and similar incidents.

Psychological data breach harms may arise as a result of a sensitive information compromise, leading consumers to experience mental and emotional conditions in relation to the unauthorized or

---

[52] *Harm*, BLACK'S LAW DICTIONARY (11th ed. 2019).

[53] *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016) ("'Concrete' is not, however, necessarily synonymous with 'tangible.' Although tangible injuries are perhaps easier to recognize, we have confirmed in many of our previous cases that intangible injuries can nevertheless be concrete.").

[54] Josh Fruhlinger, *DDoS Explained: How Distributed Denial of Service Attacks Are Evolving*, CSO (Feb. 12, 2021), https://www.csoonline.com/article/3222095/ddos-explained-how-denial-of-service-attacks-are-evolving.html [https://perma.cc/NYG8-QKW2] ("A distributed denial of service (DDoS) attack is when an attacker, or attackers, attempt to make it impossible for a service to be delivered . . . Generally, these attacks work by drowning a system with requests for data.").

[55] Sean Lyngaas, *Ransomware Attacks Grow More Menacing During the Pandemic, Creating Headaches in Health Sector*, CYBERSCOOP (Nov. 4, 2020), https://www.cyberscoop.com/health-care-ransomware-coronavirus-ryuk/ [https://perma.cc/HSP2-UMW3].

[56] Kosseff, *Hacking Cybersecurity Law*, *supra* note 30, at 834.

unknown future use of their personal information.[57] In Danielle Citron and Daniel Solove's words, "the range of possible future injuries is much more varied and could be anything in the typology of privacy harms."[58] Moreover, psychological data breach harms may also arise in cases where, for example, the cybersecurity incident did not affect any personal information and instead solely affected the availability of a critical service on which consumers rely.[59] In all of these events, the parties involved may experience data breach harms, whether of a monetary nature (e.g., losses, physical damage to infrastructure, repair expenses) or a non-monetary nature (e.g., anxiety, fear, risk, confusion, depression, humiliation, anger).[60]

As early as 1890, Samuel Warren and Louis Brandeis recognized the capability of technology to cause mental and emotional harm in their article, "The Right to Privacy."[61] As Warren and Brandeis framed the issue, "modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury."[62] In other words, harms of a psychological nature are on par with physical bodily injuries. This observation should keep guiding cybersecurity law in the era of psychological data breach harms.

Despite this recognition dating over a century ago, scholarship to date has not fully addressed the concept or the scope of psychological data breach harms. Understanding the full range of harms surrounding a data breach and other cybersecurity incidents is theoretically important and is of significant practical use for lawmakers, regulators, and courts constantly seeking to not only improve nationwide cybersecurity, but also remedy victims suffering from the externalities of cybersecurity incidents. As a

---

[57] *See* Bada & Nurse, *supra* note 6, at 82–83.

[58] Citron & Solove, *Privacy Harms*, *supra* note 35, at 45.

[59] *See id.* at 43 (noting that even loss of phone battery life and phone storage resulting from unwanted calls and data transmission can have "consequential" effects).

[60] *See, e.g.*, Bada & Nurse, *supra* note 6, at 74, 82, 89.

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

[62] *Id.* at 196.

result, any institution seeking to either legislate, regulate, or adjudicate a data breach matter would benefit from a broader understanding of what harms are associated with such incidents, particularly where such harms deviate from the traditional financial harms recognized by the law presently, like identity theft and fraud.

The following subparts set the stage for the conceptualization of psychological data breach harms. Commentators may disagree on the precise contours of psychological data breach harms, as the notion lends itself to competing interpretations. This Article does not attempt to come up with an exhaustive definition of the concept or develop a taxonomy.[63] This Article does, however, examine the nature of psychological data breach harms using existing research in sociology, psychiatry, internet studies, and the law. By exploring the nature of psychological data breach harms, this Article unveils common themes surrounding the concept, which will prove helpful for future legislative and regulatory endeavors.

A. Monetary Harm

To understand psychological data breach harms, one must first acknowledge the role of monetary harms within the body of cybersecurity law. Data breach harms can be either monetary or non-monetary in nature, though cybersecurity law is predominantly concerned with monetary cybersecurity harms. Cybersecurity law does not generally recognize harms of a non-monetary nature, evidenced primarily by the thresholds and metrics recognized by cybersecurity law as authoritative in cybersecurity incidents.

But what constitutes a monetary data breach harm? At present, the law is largely concerned with identity theft and financial fraud resulting from the misuse of compromised personal information by hackers or other wrongdoers.[64] This focus is perhaps best exemplified by the recent FTC settlement with Equifax, whose data

---

[63] *See generally* Agrafiotis et al., *supra* note 7, at 1 (proposing a taxonomy for data breach harms).

[64] Jeff Kosseff, *Defining Cybersecurity Law*, 103 IOWA L. REV. 985, 1007–08 (2018) ("Courts and legislators often focus on the financial harm to individuals—such as the consequences of identity theft—caused by data breaches.").

breach affected as many as 147 million people.[65] In this settlement, Equifax agreed to pay $575 million, of which $300 million formed a fund to compensate consumers for credit or identity monitoring services.[66] The remaining $275 million covered penalties in forty-eight states, the District of Columbia, Puerto Rico, and the Consumer Financial Protection Bureau.[67]

In another data breach settlement, Yahoo! agreed to pay $117.5 million to provide to affected customers, among other things, credit monitoring and identity protection services for up to two years.[68] The settlement fund also covered any out-of-pocket losses, including lost time.[69]

Furthermore, data breach litigation is predominately financially-oriented.[70] This trend could be the result of a strict conceptualization of Article III standing or the reluctance of courts, in general, to remedy consumers for non-financial harm.[71] In the *Target* data breach litigation, for example, the plaintiffs argued that they "incurred unauthorized charges; lost access to their accounts; and/or were forced to pay sums such as late fees, card-replacement fees, and credit monitoring costs because the hackers misused their personal financial information."[72] The plaintiffs' argument in *Target* is reflective of typical data breach litigation, which often revolves

---

[65] *Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach*, FTC (July 22, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related [https://perma.cc/T6UJ-FJMZ]; *see also* Judge Thrash, *Order Granting Final Approval of Settlement, Certifying Settlement Class, and Awarding Attorney's Fees, Expenses, and Service Awards*, (Jan. 13, 2020) https://www.equifaxbreachsettlement.com/admin/services/connectedapps.cms.extensions/1.0.0.0/927686a8-4491-4976-bc7b-83cccaa34de0_1033_EFX_Final_Approval_Order_(1.13.2020).pdf [https://perma.cc/9RCQ-AG4Z].

[66] *Equifax to Pay $575 Million*, *supra* note 65.

[67] *Id.*

[68] YAHOO! INC. CUSTOMER DATA SEC. BREACH LITIG. SETTLEMENT, https://yahoodatabreachsettlement.com/ [https://perma.cc/ZWX6-7LNS] (last visited Aug. 18, 2021).

[69] *Id.*

[70] *See* Kosseff, *Defining Cybersecurity Law*, *supra* note 64.

[71] *Id.* at 1007–08.

[72] *In re* Target Corp. Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1158 (D. Minn. 2014).

around financial harms.[73] This reality suggests a call to examine the nature of psychological data breach harms, which are often excluded from litigation or dismissed by courts.[74]

B. The Nature of Psychological Data Breach Harms

Increasingly, researchers from different disciplines have begun to recognize the mental aspect of harm resulting from data breaches. For example, Elias Aboujaoude, a Stanford professor of psychiatry and behavioral sciences, recently published an academic paper, which highlighted that personal data exposure might cause anxiety, depression, and PTSD in people whose data had been compromised.[75]

Similarly, Dr. Ryan Louie, in his talk at the RSA Conference in 2020, recognized that cybersecurity events may cause a plethora of mental health conditions, such as "depression, anxiety, PTSD-like symptoms, paranoia, and other issues."[76] Some research has also shown that victims who experienced online fraud "consistently reported emotional impact as more severe than financial impact across all fraud types."[77] Many other examples in similar research expose the often-ignored, non-monetary harms of cybersecurity incidents.[78]

Indeed, consumers informed of a data breach that compromised their most sensitive information have reported feeling "dizzy with

---

[73] Sasha Romanosky, et al., *Empirical Analysis of Data Breach Litigation*, 11 J. of Empirical Stud. 74, 86 (2014) ("[B]reaches appear less likely to be litigated in federal court absent financial harm.").

[74] *See, e.g.*, Attias v. CareFirst, Inc., 365 F. Supp. 3d 1, 23 (D.D.C. 2019) (dismissing the plaintiff's allegation of psychological harm as insufficient "to sustain their claims for negligence or negligence per se, fraud or constructive fraud, or violation of the MCPA").

[75] Elias Aboujaoude, *Protecting Privacy to Protect Mental Health: The New Ethical Imperative*, 45 J. MED. ETHICS 604, 606 (2019), https://jme.bmj.com/content/45/9/604.full [https://perma.cc/F3DL-M78P].

[76] Ryan Louie, MD, PhD, *Quick Look: #Psybersecurity: Mental Health Impact of Cyberattacks*, YOUTUBE (Feb. 17, 2020), https://youtu.be/JxGar7_2KLA [https://perma.cc/M4RJ-UTSW].

[77] David Modic & Ross Anderson, *It's All but The Crying: The Emotional and Financial Impact of Internet Fraud*, 13 IEEE SEC. & PRIV. 99, 102 (2015).

[78] *See, e.g.*, Bada & Nurse, *supra* note 6, at 85–88.

shock."[79] Nearly 85% of affected consumers reported "disturbances in their sleep habits, 77% reported increased stress levels, and nearly 64% said they had trouble concentrating. Aches, pains, headaches, and cramps were symptoms for nearly 57%."[80] In the most extreme cases, some consumers have reported suffering from depression, anxiety, and PTSD.[81] Further psychological research has confirmed the prevalence of diagnosable mental disorders resulting from data breaches, such as Major Depressive Disorder, Panic Disorder, Agoraphobia, and more.[82] Some other studies equate these psychological consequences to those experienced by trauma survivors or victims of home invasion or assault.[83]

One question to ask is: why are psychological data breach harms rising at such an alarming rate in recent years? There are many potential answers as to why these harms are occurring more often than ever before. First, better data supports the existence of these harms, particularly their likely disconnect from physical harms. Researchers in psychology, psychiatry, sociology, cybersecurity, and the law have all been reinforcing the notion that psychological data breach harms are real and often neglected by society's current law and policy approach to cybersecurity. A critical mass of research supports this assertion.[84]

Second, data collection practices in recent years may share the blame for the statistical increase in psychological data breach harms. Data collectors have expanded the scope and nature of consumer data collected, using the maxim of "collect data first, ask questions

---

[79] Guynn, *supra* note 7.

[80] *Id.*

[81] *Id.*

[82] *See* Koch et al., *supra* note 36 (listing the diagnosable psychological injuries experienced by victims of data breaches); *see also* Karen Reilly & Gráinne Kirwan, *Online Identity Theft, An Investigation of the Differences Between Victims and Non-victims with Regard to Anxiety, Precautions and Uses of the Internet*, *in* CYBERPSYCHOLOGY AND NEW MEDIA: A THEMATIC READER ACCOUNT 112, 112 (Andrew Power & Gráinne Kirwan eds., 2014) (showing heightened levels of anxiety in victims of online identity theft).

[83] EQUIFAX, A LASTING IMPACT: THE EMOTIONAL TOLL OF IDENTITY THEFT (2015).

[84] *See supra* notes 6–7 and accompanying text.

later."[85] It is therefore not only financial data that today's online platforms and services collect, but also other details, such as verbal, biometric, and audiovisual data.[86] This practice means that data breach harms go beyond the costs of replacing one's credit card or subscribing to credit monitoring and identity protection services. Moreover, some data that is prone to causing psychological data breach harms is immutable and of an intimate nature; these data include, among others, sexual orientation,[87] HIV status,[88] nudity,[89] and private communications.[90]

Cybersecurity is a societal problem. In the words of the late Joel Reidenberg, a leading authority on information security and privacy, "[S]ociety as a whole has an important stake in the contours of the

---

[85] Andrew Burt & Dan Geer, *The End of Privacy*, N.Y. TIMES (Oct. 5, 2017), https://www.nytimes.com/2017/10/05/opinion/privacy-rights-security-breaches.html [https://perma.cc/C7HF-ML4R] (characterizing the American data protection system as "collect data first, ask questions later" where "American technology companies disclose their privacy policies in a terms-of-service statement, but these disclosures are often comically ambiguous and widely misunderstood.").

[86] Vivian Ng & Catherine Kent, *Smartphone Data Tracking Is More Than Creepy – Here's Why You Should Be Worried*, THE CONVERSATION (Feb. 7, 2018), https://theconversation.com/smartphone-data-tracking-is-more-than-creepy-heres-why-you-should-be-worried-91110 [https://perma.cc/ER6E-LEJK] (reporting that data collected by smartphones "can include our location, internet search history, communications, social media activity, finances and biometric data such as fingerprints or facial features. It can also include metadata—information about the data—such as the time and recipient of a text message.").

[87] Kelvin Chan, *Norway to Fine Dating App Grindr $11.7M Over Privacy Breach*, ASSOCIATED PRESS (Jan. 26, 2021), https://apnews.com/article/europe-data-privacy-norway-12d34063d0c20acd0e7a55fc8a6dfe1d [https://perma.cc/85ST-PWJ9].

[88] James Griffiths, *HIV Status of Over 14,000 People Leaked Online, Singapore Authorities Say*, CNN (Jan. 28, 2019), https://www.cnn.com/2019/01/28/health/hiv-status-data-leak-singapore-intl/index.html [https://perma.cc/2MDU-8PQM].

[89] Lily Newman, *Hacks, Nudes, and Breaches: It's Been a Rough Month for Dating Apps*, WIRED (Feb. 15, 2019, 4:44 PM), https://www.wired.com/story/ok-cupid-dating-apps-hacks-breaches-security/ [https://perma.cc/3NGL-95L6].

[90] Mark Jones, *Adult Streaming Website Leaks 11 Million Emails and Private Chats*, KIM KOMANDO (May 5, 2020), https://www.komando.com/security-privacy/adult-streaming-website-leaks-11-million-emails-and-private-chats/737815/ [https://perma.cc/T7FS-L2WT].

protection of personal information."[91] If one accepts that psychological data breach harms are a societal problem, the next inquiry is, what can the law do to alleviate this problem? After all, psychological data breach harms can impose significant costs on consumers in the form of suffering, counseling, medication, and treatment; if no recovery is available, affected consumers inevitably bear these costs.[92] This problem can be tackled via four potential angles. One approach is to let consumers absorb the cost under the theory that this harm is an acceptable and common risk in the digital world.[93] The second approach is to allow private enforcement to deal with the problem through private litigation initiated by affected consumers; however, such private enforcement may only succeed in limited jurisdictions. The remedy would usually be monetary damages. The other two approaches, which are not as widely explored, involve expanding the terminology of cybersecurity law to allow for more regulatory oversight, and focusing on the breached entity's role in both preventing harm and responding to harm if the harm were to materialize. The proposed framework in Part IV involves both of the latter approaches.

C. Emerging Recognition of Psychological Data Breach Harms

Recently, law and policy scholars and experts have become more vocal about the psychological risks that data breaches can

---

[91] Joel Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 882–83 (2003).

[92] *See* Thomas Cotter, *Damages for Noneconomic Harm in Intellectual Property Law*, 72 HASTINGS L.J. 1055, 1059 (2021) ("[N]oneconomic harm sometimes results in quantifiable economic losses—a person suffering from emotional distress, for example, may incur out-of-pocket expenses to treat her condition; but if her distress is not a cognizable injury for the type of claim at issue, she's out of luck, despite the relative ease of quantifying these losses in comparison with some of the economic losses for which damages routinely are awarded.").

[93] *See* Lauren Scholz, *Privacy Remedies*, 94 IND. L.J. 653, 663 (2019) ("Analysis of the harm is absent where courts seek to avoid analysis of compensatory harms based on the theory that any disclosure of information anywhere constitutes consent, obviating the potential for relief from the privacy tort.").

cause.[94] Scholars and other commentators have raised multiple arguments concerning the urgent need to address psychological data breach harms.[95]

First, regulators themselves have become somewhat more transparent as to psychological data breach harms, though this transparency has not translated into actual enforcement or regulation yet.[96] The FTC—the primary cybersecurity enforcement authority in the United States—recently held an "Informational Injury Workshop,"[97] where panelists provided a variety of examples including individuals who suffered serious mental or otherwise non-physical harm as a result of a data breach that exposed their personal information.[98] The Workshop participants recognized that doxing attacks can result in violence, physical threats, emotional harm, and social isolation,[99] and that disclosure of private information may negatively affect consumers' relationships with family, friends, and coworkers.[100] Nevertheless, very little has been done at the FTC or elsewhere to address non-monetary harms regulatorily.

Second, many legal scholars have been increasingly cognizant of the exclusion of psychological data breach harms from the ambit of extant law and have therefore proposed a broadening of the concept of harm in data breach lawsuits.[101] Professors Daniel Solove and Danielle Citron, in their article titled "Risk and Anxiety," make a compelling argument that courts ought to recognize these psychological harms, such as the harm of anxiety—either in the

---

[94] *See* Fed. Trade Comm'n, *In the Matter of: Informational Injury Workshop*, FTC, (Dec. 12, 2017), https://www.ftc.gov/system/files/documents/public_events/1256463/informational_injury_workshop_transcript_with_index_12-2017.pdf [https://perma.cc/G34E-Z6P2].

[95] *See id.*

[96] *See id.*

[97] *Id.*

[98] Fed. Trade Comm'n, *supra* note 94, at 32:3–7 ("[T]here are cyber harms that are hard to kind of boil down to dollars. They are, you know, physical threats and things like this, emotional harm, social isolation, that are very hard to kind of boil down into dollars . . . ." (quoting David McCoy, assistant professor of computer science at NYU Tandon School of Engineering)).

[99] *Id.* at 31:15–32:17.

[100] Lynn Langton, *supra* note 94, at 243:14–21.

[101] *See* Solove & Citron, *Risk and Anxiety*, *supra* note 48, at 737.

future or at present—as a cognizable harm for both Article III standing and cause of action purposes.[102] Solove and Citron laid an important foundation for the evolving definition of "harm" in cybersecurity law literature: rejecting the approach that most courts take to cognizable harm in data breach litigation.[103]

Solove and Citron's work specifically focuses on data breach litigation, which is one of the many subareas of cybersecurity law. This Article builds on Solove and Citron's work by expanding their proposal to other areas within the law of cybersecurity beyond litigation—for example, computer crime law, data security law, data breach notification law, and FTC regulation and enforcement. Moreover, this Article also distinguishes itself from the work of Solove and Citron by recognizing a broader subset of harms that may occur as a result of a data breach—not solely the harm of anxiety or increased risk but also harms of depression, PTSD, and other conditions. This Article takes the view that psychological data breach harms require a legal framework that both prevents psychological data breach harms and responds to psychological data breach harms when the harms occur.

In addition, George Ashenmacher in "Indignity: Redefining the Harm Caused by Data Breaches," has argued that data breach victims suffer a violation of their dignity, even when no financial harm or actual misuse of the breached information occurs.[104] Ashenmacher, in the same vein as Solove and Citron, argues for a broader understanding of data breach harms to include non-monetary harms, such as harms against the autonomy, dignity, and privacy of consumers.[105]

Following the same logic of expanding cybersecurity law's concepts, Jeff Kosseff in "Hacking Cybersecurity Law," proposed the adoption of seven principles for a more robust and effective cybersecurity law doctrine.[106] One of these principles is

---

[102] *Id.* at 767.

[103] *Id.* at 756.

[104] George Ashenmacher, *Indignity: Redefining the Harm Caused by Data Breaches*, 51 WAKE FOREST L. REV. 1, 7 (2016).

[105] *Id.*

[106] Kosseff, *Hacking Cybersecurity Law*, *supra* note 30, at 814.

"comprehensive," which recommends that cybersecurity law "focus not just on financial harms, but [on] any threats to national security or individual privacy or safety."[107] Kosseff suggested that "personal information," used in many cybersecurity statutes, should be expanded to accommodate emerging harms and abuses that have only recently surfaced, such as harms and abuses of autonomy, privacy, well-being, and more.[108] This Article makes a similar proposal in the context of psychological data breach harms.

Part III explores cybersecurity law and the particular frameworks that this Article will draw upon for its proposed framework. For the purposes of this Article, the cybersecurity law covered will include computer crime law, FTC enforcement, data security law, and data breach notification law. These subareas form the bulk of cybersecurity law, though additional categories could be classified as cybersecurity law.

III. CYBERSECURITY LAW: A PRIMER

While "cybersecurity law" is used in various contexts, the precise definition of this legal field is far from settled.[109] Different definitions of cybersecurity law have been offered,[110] but there is not yet a settled, authoritative definition. In the abstract, cybersecurity law is a somewhat nascent field of law that seeks to address a variety of issues related to information security for computers, networks, systems, data, and other technologies.[111]

Information security, as a technical field, seeks to protect a wide variety of valuable "assets" pertaining to computer systems.[112] These assets can take the form of "hardware, software, data, people,

---

[107] *Id.*

[108] *See* Jeff Kosseff, *Cybersecurity of the Person*, 17 FIRST AMEND. L. REV. 343, 364–65 (2018).

[109] *See* Kerr, *supra* note 12; Kosseff, *Defining Cybersecurity Law*, *supra* note 64, at 994–1010; Ido Kilovaty, *Availability's Law*, 88 TENN. L. REV. 69, 78–79 (2021).

[110] *See* Kerr, *supra* note 12; Kosseff, *Defining Cybersecurity Law*, *supra* note 64, at 1010; Kilovaty, *supra* note 109, at 78–79.

[111] Kosseff, *Defining Cybersecurity Law*, *supra* note 64, at 1010–11.

[112] CHARLES P. PFLEEGER, SHARI LAWRENCE PFLEEGER & JONATHAN MARGULIES, SECURITY IN COMPUTING 2 (5th ed. 2015).

processes, or combinations of these."[113] In order to do so, information security focuses on three distinct properties: (1) confidentiality, (2) integrity, and (3) availability.[114] This "CIA triad"[115] is seen purely as an embodiment of the "engineering properties of a system."[116]

Confidentiality seeks to ensure that assets are only viewed by authorized parties.[117] For example, a student's grades may only be viewed by the student and other predetermined authorized users.[118] A breach of confidentiality occurs when a third party, say the student's friend, gains unauthorized access to the system that stores the grades and, by doing so, views the grades.[119]

Integrity refers to the "ability of a system to ensure that an asset is modified only by authorized parties."[120] For instance, using the previous example, only an authorized educator should be able to modify a student's grade if such modification is warranted. A breach of integrity occurs when a third party, say the same friend of that

---

[113] *Id.*

[114] Debbie Walkowski, *What Is the CIA Triad?*, F5 LABS (July 9, 2019), https://www.f5.com/labs/articles/education/what-is-the-cia-triad [https://perma.cc/45J2-ADH7].

[115] Ashish Agarwal & Aparna Agarwal, *The Security Risks Associated with Cloud Computing*, 1 INT'L J. COMPUT. APPLICATIONS ENG'G SCIS. (SPECIAL ISSUE) 257, 257–58 (2011).

[116] *See* Andrea M. Matwyshyn, *Cyber!*, 2017 BYU L. REV. 1109, 1138 ("Security, in the technical community, historically refers to questions of data confidentiality, integrity, and availability as engineering properties of a system—questions likely to be disconnected from the identity of any individual human person.").

[117] C. PFLEEGER, S. PFLEEGER & MARGULIES, *supra* note 112, at 6.

[118] *Id.* at 8 ("A proud student may run out of a classroom screaming 'I got an A!' but the student should be the one to choose whether to reveal that grade to others.").

[119] In U.S. computer crime law, the main statutory provision that seeks to protect information technology systems from confidentiality attacks is 18 U.S.C. § 1030(a)(2)(C), which punishes whoever "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer." 18 U.S.C. § 1030(a)(2)(C) (2018).

[120] C. PFLEEGER, S. PFLEEGER & MARGULIES, *supra* note 112, at 6.

student, decides to add (or subtract) points from the student's grades in an unauthorized manner.[121]

And finally, availability pertains to the system's ability to ensure uninterrupted access to assets by authorized users.[122] For example, a student who wants to view a grade should be able to do so by accessing the grading system. An availability incident occurs when the notorious friend of that student decides once again to mess with the system, such as by flooding it with bogus traffic that overwhelms the system, which can only handle a limited amount of traffic at a single point in time.

The CIA triad illustrates that "cyber security" is "not a single problem, but rather a group of very different problems involving various sets of threats, targets, and costs."[123] Cybersecurity law, therefore, is a body of law that seeks to address some of these problems, though with mixed aptitude and success.

While information security and cybersecurity are generally synonymous, the latter is used more often in legal and policy circles.[124] Recently, scholars, policymakers, and practitioners have started referring to the law and policy of information security as "cybersecurity law."[125] The Congressional Research Service has identified more than fifty statutes related to information security that could be considered part of cybersecurity law.[126] However,

---

[121] *See, e.g.*, United States v. Barrington, 648 F.3d 1178, 1191 n.11 (11th Cir. 2011) (upholding defendant's conviction under the Wire Fraud Statute, reasoning that by changing his own and his friends' grades, the defendant committed a federal crime because "the University certainly has an intangible property interest in the integrity of its grading system.").

[122] C. PFLEEGER, S. PFLEEGER & MARGULIES, *supra* note 112, at 6.

[123] Jennifer A. Chandler, *Security in Cyberspace: Combatting Distributed Denial of Service Attacks*, 1 U. OTTAWA L. & TECH. J. 231, 233 (2004).

[124] *See* Matwyshyn, *supra* note 116, at 1158 ("In essence, the term 'cybersecurity' is the consequence of a cultural divide between the two coasts: 'cybersecurity' is the Washington, D.C. legal rebranding for what Silicon Valley veterans have historically usually called 'infosec' or simply 'security.'").

[125] *See, e.g.*, Kosseff, *Defining Cybersecurity Law*, *supra* note 64, at 987 (discussing lawmakers' use of the term "cybersecurity law").

[126] ERIC A. FISCHER, CONG. RSCH. SERV., R42114, FEDERAL LAWS RELATING TO CYBERSECURITY: OVERVIEW OF MAJOR ISSUES, CURRENT LAWS, AND PROPOSED LEGISLATION 28 (2014).

cybersecurity law may lend itself to multiple definitions[127] and, as noted above, does not have an authoritative definition.[128] This Article takes the view that, in general, cybersecurity law is comprised of a patchwork of statutes and regulations that promote, or ought to promote, "the confidentiality, integrity, and availability of public and private information, systems, and networks."[129]

While this definition may seem desirable and complete, cybersecurity law currently lacks a robust approach to psychological data breach harm. The fact of cybersecurity law being a patchwork—rather than a body of law representing a cohesive set of policy priorities and values—may be a contributing factor to this gap. This gap is also evidenced in the limited scope of the definition of "personal information" adopted by cybersecurity law, which "does little to address the very real integrity and availability threats."[130]

Despite the absence of a comprehensive approach to cybersecurity harm, harm is nonetheless a critical concept in cybersecurity law. Many issues of cybersecurity law are resolved through either the existence or absence of harm, usually of monetary nature.[131] The following subparts provide an overview of areas in cybersecurity law where the question of "harm" is consequential. These areas include the Computer Fraud and Abuse Act ("CFAA"), FTC enforcement, and various data breach notification statutes.

---

[127] *See, e.g.*, Kerr, *supra* note 12 ("If you look closely, though, there isn't much clarity about what 'cybersecurity law' actually means.").

[128] *See* FISCHER, *supra* note 126, at 1 n.1 ("Thus cybersecurity, a broad and arguably somewhat fuzzy concept for which there is no consensus definition, might best be described as measures intended to protect information systems—including technology (such as devices, networks, and software), information, and associated personnel—from diverse forms of attack.") (emphasis omitted).

[129] *See* Kosseff, *Defining Cybersecurity Law*, *supra* note 64, at 1010 (providing a definition that goes further: "[T]hrough the use of forward-looking regulations and incentives, with the goal of protecting individual rights and privacy, economic interests, and national security.").

[130] Kosseff, *Hacking Cybersecurity Law*, *supra* note 30, at 834; *see also* Kilovaty, *supra* note 109, at 91–92.

[131] *See* Kosseff, *Hacking Cybersecurity Law*, *supra* note 30, at 836.

A. Computer Fraud and Abuse Act

The CFAA is the primary federal criminal statute that both criminalizes certain computer-related activities and also creates a private cause of action for victims of computer-related offenses.[132] The CFAA prohibits seven computer-related acts: hacking to commit espionage,[133] hacking to obtain information,[134] hacking a federal government computer,[135] hacking to commit fraud,[136] hacking to commit damage,[137] trafficking in passwords,[138] and threats of hacking.[139] While the term "harm" is only used once in the statute, other terms appear in the statute that focus on the existence of a certain level of harm: information, value, damage, and loss.

1. Information and Value as Harm

One of the main CFAA offenses is the act of unauthorized access to obtain information.[140] Whether a CFAA offense has been committed revolves around the question of information access. While courts have defined "information" in a variety of ways, the statute itself offers little guidance on what counts as information. Does the definition purely focus on financial information, information related to national security, and other sensitive information? Or is there room for information that is potentially intimate and embarrassing?

Despite the lack of a clear understanding of what "information" means, a person commits a CFAA offense whenever the person "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains" information from either a U.S. government computer or a protected computer.[141] The felony

---

[132] *See* 18 U.S.C. § 1030.
[133] *See id.* § 1030(a)(1).
[134] *See id.* § 1030(a)(2).
[135] *See id.* § 1030(a)(3).
[136] *See id.* § 1030(a)(4).
[137] *See id.* § 1030(a)(5).
[138] *See id.* § 1030(a)(6).
[139] *See id.* § 1030(a)(7).
[140] *Id.* § 1030(a)(2).
[141] *Id. See also id.* § 1030(e)(2)(B) (defining protected computer, among other things, as "a computer . . . which is used in or affecting interstate or foreign commerce or communication.").

enhancement portion of the statute provides metrics to assess unauthorized access to information and thus provides some guidance on what constitutes information. Specifically, the statute indicates that a § 1030(a)(2) offense would become a felony if "the value of the information obtained exceeds $5,000."[142]

But how should we determine the value of information when the information is of a non-financial nature? What if the information accessed is of an intimate nature, such as the sexual orientation or gender identities of consumers—the kind of information that does not have a readily-available "value"? The answer is not particularly clear. In *United States v. Batti,* the Sixth Circuit held that market value is the primary metric used to determine the "value of the information," and where such market value is unascertainable, "any reasonable method" is an appropriate alternative.[143] In *Batti,* the Court said, the "cost of production as a means to determine the value of the information obtained" would be a reasonable method to ascertain the market value of the information accessed.[144] This holding could open the door for juries to determine the value of consumers' harm on the basis of the psychological harm that may have resulted from the consumers' compromised information.

2. Damage and Loss

The CFAA also makes it a criminal offense to cause damage and loss to a protected computer.[145] For example, the CFAA makes it an offense to transmit malware or otherwise harmful code, which intentionally causes damage.[146] In addition, the CFAA criminalizes unauthorized access to protected computers that "as a result of such conduct . . . [causes] *damage* and *loss*."[147]

The CFAA raises a "damage and loss to a protected computer" misdemeanor offense to a felony offense in several cases: where the loss (1) exceeds $5,000 in a one-year period, (2) involves the modification or impairment of medical information, (3) causes

---

[142] *Id.* § 1030(c)(2)(B)(iii).
[143] *See* United States v. Batti, 631 F.3d 371, 374–78 (6th Cir. 2011).
[144] *Id.* at 378.
[145] *See* 18 U.S.C. § 1030(a)(5).
[146] *See id.* § 1030(a)(5)(A).
[147] *Id.* § 1030(a)(5)(C) (emphasis added).

physical injury, (4) threatens public health or safety, (5) damages a U.S. government computer used in the administration of criminal justice, or (6) damages at least ten protected computers in a given year.[148] The increase in the level of these offenses focuses on the physical and monetary consequences resulting from the offense.

The CFAA defines both damage and loss, though those definitions do not support an inclusion of non-monetary harms, such as mental harms. The term "damage" is defined by purely technical elements as "any impairment to the integrity or availability of data, a program, a system, or information."[149] The term "loss" is defined via a combination of technical and monetary elements as

> [A]ny reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.[150]

Again, non-monetary losses and damage are not expressly included in either of these two definitions.

3. Private Cause of Action

The CFAA's approach to computer misuse—not expressly including non-monetary and non-physical harms from its unauthorized access to information, and failing to address damage or loss to protected computers offenses—is not limited to the criminal portion of the statute. The CFAA recognizes a private cause of action that victims of computer crime may take against perpetrators, contingent on one of the felony increase factors listed above.[151] The CFAA recognizes a civil cause of action for "[a]ny person who suffers damage or loss,"[152] which could entitle that person to "compensatory damages and injunctive relief or other equitable relief," depending on the damage or loss suffered.[153]

---

[148] *Id.* § 1030(c)(4)(A)(i).
[149] *Id.* § 1030(e)(8).
[150] *Id.* § 1030(e)(11).
[151] *Id.* § 1030(g).
[152] *Id.*
[153] *Id.*

Yet, following the CFAA's logic on limiting the terms of art of "damage" and "loss" to monetary and physical harms only, it is unlikely that any psychological harm would be sufficient for a private cause of action under the CFAA. In other words, a victim of a computer offense may be unable to pursue the perpetrators of a data breach and recover any remedy for psychological harm under the CFAA due to the statute's direct focus on solely the physical and monetary elements of information, damage, and loss.

B. Federal Data Security Enforcement

The FTC is the primary enforcement authority on data security under Section 5 of the Federal Trade Commission Act ("FTC Act"). Section 5 of the FTC Act makes unlawful any "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce."[154] The FTC Act labels a method of competition as unfair if it satisfies the three-part unfairness test.[155] The three-part unfairness test makes unfair an "act or practice [that] causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[156]

The term "injury" in the unfairness test has not been clearly defined by the FTC and therefore lends itself to multiple interpretations.[157] In a 1982 letter, FTC Chairman J.C. Miller iterated the FTC's interpretation that, "[a]s a general proposition, substantial injury involves economic or monetary harm and does not cover subjective examples of harm such as emotional distress or offenses

---

[154] 15 U.S.C. § 45(a)(1).

[155] *See id.* § 45(n).

[156] *Id.*

[157] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 639 (2014) ("Monetary, health, and safety risks are common injuries considered 'substantial,' but trivial, speculative, emotional, and 'other more subjective types of harm' are usually not considered substantial for unfairness purposes." (quoting Letter from FTC Comm'rs to Wendell H. Ford & John C. Danforth, Senators (Dec. 17, 1980), *reprinted in In re* Int'l Harvester Co., 104 F.T.C. 949, 1070–76 (1984))).

to taste or social belief."[158] Another FTC statement from 1980 supported a similar approach, that "[e]motional impact and other more subjective types of harm . . . will not ordinarily make a practice unfair."[159]

These statements, however, should be taken with some caution. The FTC opined on the place of emotional harm in its enforcement actions decades before cybersecurity became a major societal problem.[160] The FTC recognized that "[i]n an extreme case, . . . where tangible injury could be clearly demonstrated, emotional effects might possibly be considered as the basis for a finding of unfairness."[161] But, at present, the FTC has not indicated how it might approach emotional and mental harms resulting from data breaches in its enforcement actions. These harms have never formed the basis for an enforcement action on their own. Additionally, regardless of the FTC's approach, courts and administrative law judges are reluctant to recognize emotional harms as recoverable damages.[162]

In enforcement, the FTC's focus is on either those companies whose data security practices are inadequate where some monetary injury to consumers occurs or those instances when sensitive medical information is compromised due to unreasonable data security practices.[163] For example, in the landmark Third Circuit case of *FTC v. Wyndham*, the FTC alleged that consumers had suffered and would suffer substantial injury as a result of a data security compromise affecting 619,000 consumers with $10.6 million in

---

[158] Letter from FTC Chairman J.C. Miller, III to Senator Packwood and Senator Kasten (March 5, 1982), *reprinted in* H.R. Rep. No. 98-156, pt. 1, at 32 (1983).

[159] FTC POLICY STATEMENT ON UNFAIRNESS, *supra* note 21.

[160] *See id.* at n.16.

[161] *Id.*

[162] *See e.g.*, LabMD Inc., No. 9357 (Initial Decision) (Nov. 13, 2015), https://ftc.gov/system/files/documents/cases/151113labmd_decision.pdf [https://perma.cc/YA7K-VQVN]) ("[T]he evidence fails to prove Complaint Counsel's contention that embarrassment or similar emotional harm is likely to be suffered from the exposure of the 1718 File alone. Even if there were proof of such harm, 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).").

[163] *See* Solove & Hartzog, *supra* note 157, at 639.

fraud loss.[164] Notably, the district court in the *Wyndham* case asserted that "the Court is not convinced that non-monetary harm is, as a matter of law, unsustainable under Section 5 of the FTC Act,"[165] potentially leaving the door open for psychological harms to be adjudicated in the future and remedied when proven. In *LabMD v. FTC*, the FTC pursued enforcement against a medical laboratory where an employee negligently shared sensitive health-related consumer information on a peer-to-peer network.[166] However, the enforcement action in *LabMD* was more focused on the lack of reasonable cybersecurity measures and potential harm to consumers than on any embarrassment or loss of privacy.[167]

The FTC enforcement mechanism is a welcomed remedy but suffers from a serious gap in relation to psychological harms. While FTC enforcement may coincide with the existence of both monetary and psychological harms to consumers, psychological harm alone is usually insufficient for the FTC to get involved and pursue enforcement.[168] Some argue that this gap is the flaw of the "do no harm" approach, which disregards the wrongfulness of a data collection practice as long as no financial harm occurs.[169] As was observed by many commentators, the FTC's approach "fails to properly deal with opportunism."[170] In short, corporate data opportunism allows companies to use consumer information in ways

---

[164] FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 242 (3d Cir. 2015).

[165] FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 623 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015).

[166] LabMD, Inc. v. FTC, 894 F.3d 1221, 1223–24 (11th Cir. 2018).

[167] *See id.*

[168] *See* Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, at 44 (drft., 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3642217 [https://perma.cc/UF-47-GLTN].

[169] FED. TRADE COMM'N, FEDERAL TRADE COMMISSION 2020 PRIVACY AND DATA SECURITY UPDATE 1, 7 (2020), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-2020-privacy-data-security-update/20210524_privacy_and_data_security_annual_update.pdf [https://perma.cc/EPX8-VSPK] ("[T]he FTC is focused on protecting consumers from the financial harm that occurs when bad actors mishandle personal information.").

[170] *Id.*

that disadvantage consumers.[171] Therefore, the FTC enforcement focus leaves a lot to be desired.

C. Data Security Regulation

The FTC Act serves as a general data security regulation, requiring that organizations adopt reasonable data security measures.[172] Additionally, other data security regulations exist, both on the federal[173] and state levels.[174] These data security statutes set the minimum cybersecurity standards for organizations, either in general or for a specific sector. Federally, for example, the Health Insurance Portability and Accountability Act ("HIPAA") contains a security rule, which applies to the healthcare sector, requiring that every covered entity ensure the confidentiality, integrity, and availability of "electronic protected health information."[175] Similarly, the financial sector is regulated by the Gramm-Leach-Bliley Act, which sets the data security standards for regulated financial institutions.[176]

State data security statutes likewise set minimum cybersecurity standards for organizations processing data of their state's residents. Generally, these statutes mandate "reasonable security procedures" to protect "personal information." Examples of states that take such an approach are California,[177] Colorado,[178] Florida,[179] Texas,[180] and

---

[171] *See id.* at 19.

[172] FTC, START WITH SECURITY: A GUIDE FOR BUSINESS (2015) ("Once you've decided you have a legitimate business need to hold on to sensitive data, take reasonable steps to keep it secure.").

[173] For a list of federal data security statutes, *see* ERIC FISCHER, CONG. RSCH. SERV., R42114, FEDERAL LAWS RELATING TO CYBERSECURITY: OVERVIEW OF MAJOR ISSUES, CURRENT LAWS, AND PROPOSED LEGISLATION 62–71 (2014), https://fas.org/sgp/crs/natsec/R42114.pdf [https://perma.cc/LY2B-VEPK].

[174] For a list of state data security statutes, *see* NAT'L CONF. OF ST. LEGS., DATA SECURITY LAWS – PRIVATE SECTOR (May 29, 2019), https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx [https://perma.cc/VH9D-S6Z3].

[175] 45 C.F.R. § 164.302.

[176] *See* 15 U.S.C. § 6801.

[177] CAL. CIV. CODE § 1798.81.5.

[178] COLO. REV. STAT. §§ 6-1-713 to 713.5.

[179] FLA. STAT. § 501.171(2).

[180] TEX. BUS. & COM. CODE § 521.052.

several others.[181] The definitions in these statutes are similar in their focus on demographics and individuals' plainly identifiable information covered under the statutes' mandates. There is little to suggest that these statutes also focus on information that has the potential of causing psychological harm to consumers affected by a breach. For example, if the online chats on a dating site are compromised, unless the chats contain personally identifiable information, such as a social security number, a bank account number, or a driver's license number, it is hard to qualify such information as "personal information," despite the undisputed psychological impact if this information is seen by others.

Just like data breach notification laws,[182] data security statutes have been designed to address threats to specific pieces of information that qualify as "personal information." Their mandate is usually unnuanced, involving only broad concepts of reasonableness and protection of personal information.[183] State data security statutes do not go beyond this mandate to address more emerging cybersecurity threats with respect to consumer data.[184] The definitional flaw of "personal information" discussed in the next subpart is equally applicable to both data security statutes and data breach notification statutes.

D. Data Breach Notification Law

Data breach notification statutes mandate public disclosure whenever an entity experiences a data breach.[185] The specifics vary from state to state, and every statute has its own definition of a data breach that qualifies for disclosure.[186]

---

[181] *See* NAT'L CONF. OF ST. LEGS., *supra* note 174.

[182] *See* discussion *infra* Part II.D.

[183] *See* CAL CIV. CODE § 1798.81.5; COLO. REV. STAT. §§ 6-1-713 to 713.5; FLA. STAT. § 501.171(2); TEX. BUS. & COM. CODE § 521.052.

[184] *See* CAL CIV. CODE § 1798.81.5; COLO. REV. STAT. §§ 6-1-713 to 713.5; FLA. STAT. § 501.171(2); TEX. BUS. & COM. CODE § 521.052.

[185] *See* Mark Verstraete & Tal Zarsky, *Optimizing Breach Notification*, 2021 U. ILL. L. REV. 803, 805 (2021).

[186] For a list of state data security statutes, *see* NAT'L CONF. OF ST. LEGS., SECURITY BREACH NOTIFICATION LAWS (July 17, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/5E6L-S8Q5].

In the context of psychological data breach harms, data breach notification law suffers from two major flaws. The first flaw is *definitional*—that is, the definitions of data breach and personal information are often limited to financial information that will likely be misused and cause financial harm.[187] The second is *risk-related*, where most state statutes mandate a risk of harm assessment, which could absolve the breached entity from the reporting obligations in cases where there is no risk of economic or financial harm, either present or future.[188] Both the definitional and risk-related flaws are reflective of the omission of any information that may cause emotional or mental harm. This includes any present or future emotional or mental harm from the risk assessment methodology.

1. The Definitional Flaw

State statutes define "data breach" and "personal information" differently. In California, a breach notification is required whenever a data breach involves information like social security numbers, financial account numbers, medical information, health insurance information, unique biometric data, and license plate numbers.[189] In addition, usernames and passwords allowing access to online accounts similarly require a notification if compromised.[190] In general, this notification approach focuses on the sensitivity of the compromised information and the potential that the information will be abused for the financial benefit of the perpetrators.

As one commentator notes, data breach notification statutes do not cover breaches that involve "information that could be used to stalk, harass, or dox" consumers.[191] Following the same logic, a disclosure is not required when the compromised information is of such nature that psychological harm to consumers is likely.[192] While personal information of a financial nature is very likely to also cause

---

[187] *See* Verstraete & Zarsky, *supra* note 185, at 810 ("[I]n defining personal information, most states merely address information linking names to social security numbers, drivers' license number, or financial account information (such as bank account or credit card numbers).").

[188] *See, e.g.*, N.Y. GEN. BUS. LAW § 899-aa.

[189] CAL. CIV. CODE §§ 1798.29, 1798.82.

[190] *Id.*

[191] Kosseff, *Cybersecurity of the Person*, *supra* note 108, at 358.

[192] *See* CAL. CIV. CODE §§ 1798.29, 1798.82.

psychological harm, the latter is not exclusive to data breaches involving personal financial information.

2. The Risk-Related Flaw

Most data breach notification statutes have a risk of harm exception, under which the breached entities are not required to disclose a breach if the entity determines that there is no risk of harm to consumers as a result of the breach.[193] The risk of harm assessment varies among states but often focuses on the likelihood of financial and economic harms to consumers.[194] The Florida statute, for example, reads as follows: "Notice . . . is not required if . . . the covered entity reasonably determines that the breach has not and will not likely result in identity theft or any other financial harm to the individuals whose personal information has been accessed."[195] Many other statutes have a similar approach.[196]

However, New York's statute was recently amended to include an explicit mention of emotional harm as part of the risk of harm assessment.[197] To date, this is the only statute acknowledging the important role of emotional harm in these risk of harm assessments. The New York statute reads: "Notice to affected persons . . . is not required if the exposure . . . will not likely result in . . . financial harm to the affected persons or emotional harm."[198]

While only a partial solution, this statute certainly offers a more robust approach to these harms. As discussed in Part IV below, such inclusion of emotional harms in the risk of harm assessment is desperately needed to tackle the emerging recognition of data breach harms.

---

[193] *See* FOLEY & LARDNER LLP, STATE DATA BREACH NOTIFICATION LAWS (Apr. 17, 2020), https://www.foley.com/en/insights/publications/2019/01/-/media/files/insights/publications/2020/04/20mc28174-data-breach-chart-041720.pdf [https://perma.cc/2M9W-CX3X] (comparing the different statutes and their respective risk of harm analyses).

[194] *See id.*

[195] FLA. STAT. § 501.171(4)(c).

[196] *See* FOLEY & LARDNER LLP, *supra* note 193 (comparing the different statutes and their approaches to risk of harm).

[197] N.Y. GEN. BUS. LAW § 899-aa(2)(a).

[198] *Id.*

E. The Shortcomings of Data Breach Litigation in the Context of Psychological Harm

The body of data breach litigation forms an additional part of cybersecurity law. Litigation may offer an important remedy to consumers who suffer from a significant psychological data breach harm, but litigation is only one tool in the cybersecurity law toolbox. Therefore, for the reasons discussed below, data breach litigation is not in and of itself a solution to the emergence of psychological harms in data breaches. The following subparts briefly summarize the shortcomings of data breach litigation in the context of psychological harms.

1. Litigation is Backward-Looking

This Article proposes solutions to address psychological data breach harms largely from an *ex-ante* viewpoint; whereas, litigation is, first and foremost, a legal process that comes after the fact, where plaintiffs seek to recover damages in connection with a data breach. Litigation, at least directly, does not prevent data breaches from happening but can, of course, serve as a deterrent in the sense that entities might be more cautious with personal consumer information in order to avoid costly and publicized litigation resulting from a data breach.

Addressing psychological data breach harms in litigation requires their recognition within the process of cybersecurity organizations. Forgoing the collection of information that could cause psychological harm or protecting against those harms in the same manner as financial harms is a critical change that needs to take place. In addition, litigation does not usually affect the baseline obligations that breached organizations need to have, such as providing consumers with the proper resources, offering counseling services, and, in general, informing consumers of their options.

2. Litigation is Unlikely to Succeed

Courts are reluctant to remedy harms of a non-monetary nature[199] and are also less likely to remedy future harms.[200] This reluctance goes both to the Article III standing question, where plaintiffs must show an injury in fact, and also to the merits, where courts are simply more cautious when it comes to considering emotional and mental harms.

The logic that informs courts to dismiss data breach lawsuits for solely showing a hypothetical future harm is that there are too many unknowns. As the Eleventh Circuit in *Amburgy v. Express Scripts* stated, for the plaintiff to succeed in showing actual harm, "many 'ifs' would have to come to pass . . . 'if' his personal information was compromised, and 'if' such information was obtained by an unauthorized third party, and 'if' his identity was stolen as a result, and 'if' the use of his stolen identity caused him harm."[201]

Given this unfortunate reality, litigation is simply unlikely to succeed in the context of psychological data breach harms. Such harms may not be recoverable in most circuits, thereby making litigation a suboptimal avenue for recovery. Data breach victims aware of these difficulties generally avoid litigation since their claims of psychological harm would likely not prevail under current case law. Moreover, even where the harms litigated are of a financial nature, class action lawsuits often result in a settlement that does little to make the data breach victims better off.[202]

3. Proposals to Address Risk and Anxiety as Cognizable Data Breach Harms

Professors Solove and Citron have already proposed recommendations for courts in adjudicating cases regarding data breach harms,[203] making the compelling argument that risk and anxiety are no different than financial harms, and, therefore, courts

---

[199] Solove & Citron, *Risk and Anxiety*, *supra* note 48, at 753.

[200] *See, e.g.*, Tsao v. Captiva MVP Rest. Partners, LLC, 986 F.3d 1332, 1344 (11th Cir. 2021) (dismissing the lawsuit on the ground that the plaintiff's future harms were too speculative).

[201] Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046, 1053 (E.D. Mo. 2009).

[202] Citron & Solove, *Privacy Harms*, *supra* note 35, at 44.

[203] Solove & Citron, *Risk and Anxiety, supra* note 48, at 773–78.

ought to recognize these psychological harms as legitimate and redressable harms.[204] Their proposal is an important contribution to the legal scholarship on psychological data breach harms yet is largely confined to the area of data breach litigation. Solove and Citron are aware of the imperfections of data breach litigation and the likelihood that new legal tools would "work better."[205] Following this logic, this Article shows the efficacy of additional legal tools other than litigation. These legal tools include the other bodies of cybersecurity law: computer crime law, FTC enforcement, data security law, and data breach notification law, which all need to be reimagined in order to cover psychological data breaches in the realm of cybersecurity harms.

This Article will not reiterate the robust and comprehensive proposals made by Solove and Citron, as well as others, on how data breach litigation could realign itself with the reality of emotional and mental harms. To fill the gap in the existing scholarship, this Article addresses cybersecurity law outside of litigation.

IV. A FRAMEWORK FOR PSYCHOLOGICAL DATA BREACH HARMS

Cybersecurity law is overdue for reform to address the evolving nature of data breach harms. Such reform must grapple with, among other things, the inclusion of emotional and mental data breach harms. This Article proposes a framework for the inclusion of the psychological impact of data breaches in the process of organizations' cybersecurity structures, as well as within existing statutory frameworks.

Privacy law scholarship has already begun addressing privacy harms, which result from privacy violations rather than from data breaches.[206] The subparts that follow specify the contours of

---

[204] *Id.*

[205] *Id.* at 783 ("It is true that litigation is a flawed legal tool, but the other legal tools to deal with data breaches have limitations. New legal tools might work better.").

[206] *See, e.g.*, Ignacio N. Cofone & Adriana Z. Robertson, *Privacy Harms*, 69 HASTINGS L.J. 1039, 1041–47 (2018); Ryan M. Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131 (2011); Matthew S. DeLuca, *The Hunt for Privacy Harms After* Spokeo, 86 FORDHAM L. REV. 2439, 2440–52 (2018).

psychological data breach harms by looking to the scholarship on privacy harms, but first, a few words of caution.

A. Privacy ≠ Cybersecurity: Avoiding Privacy Conflation

Privacy law scholarship is years ahead of the scholarship of cybersecurity. Privacy law scholarship offers certain lessons that are valuable and applicable to cybersecurity law, depending on the context. Strictly speaking, privacy law and cybersecurity law are distinct areas of law, dealing with separate issues, actors, motivations, and effects. However, there are certain conceptual overlaps that may justify learning from the work of prominent privacy law scholars.

The framework proposed by this Article is mindful of cybersecurity law scholars' inclination to conflate their area of expertise with privacy law. This phenomenon is known as "privacy conflation."[207] Privacy conflation refers to the tendency to put cybersecurity in the same legal category as privacy.[208] While privacy is focused on protecting communications and de-identifying personal information, cybersecurity relates to the confidentiality, integrity, and availability (the "CIA triad" described above) of computer systems and networks.[209] Privacy law, for example, addresses the mismatch between one's expectation of privacy and the actual use of one's personal information by the data collector, say, a social media platform.[210] Cybersecurity law, on the other hand, regulates the information security of computers, networks, data, and systems against outside and inside threats and creates a legal framework surrounding the consequences of a data breach.[211]

From a consumer point of view, there is a "substantial gap between privacy- and security-related concerns . . . Internet users recognize a difference between the two types of harms . . . [and] are

---

[207] Matwyshyn, *supra* note 116, at 1135.
[208] *Id.*
[209] *Id.* at 1138.
[210] *Id.* at 1135.
[211] *Id.*

far more concerned about security-related concerns than privacy-related concerns."[212]

Regardless of the distinct nature of the two areas of law, privacy law scholarship on privacy harms has a lot to offer on the topic of non-monetary data breach harms. Privacy law addresses the subjective and objective nature of such harm experienced by users whose data has been compromised and its subsequent misuse. The following two subparts apply the subjective and objective nature of privacy harms to data breach harms.

B. Subjective Data Breach Harms

In "The Boundaries of Privacy Harm," Ryan Calo categorizes privacy harms into two groups: subjective and objective.[213] Subjective privacy harm is the "perception of unwanted observation, broadly defined."[214] To constitute harm, the observation must be unwanted.[215] In the realm of data breaches, an unwanted observation by an unknown entity (an intruder) is a given.[216] After all, a data breach is by definition an unauthorized access to protected information.[217] Consumers have an implicit, and often explicit, expectation that the personal information consumers share with a trusted third party will not end up in the hands of outside hackers.[218]

In this context, subjective data breach harm is indeed a very central part of psychological data breach harms. Consumers whose information has been compromised in the past may feel a variety of emotions and experience many mental conditions in situations where their sensitive information is obtained by an unidentified

---

[212] Gus Hurwitz, *Privacy and Cybersecurity Are Not the Same, and Americans Care Far More About Cybersecurity*, AM. ENTER. INST. (July 2016), https://www.aei.org/wp-content/uploads/2016/07/Privacy-and-Security.pdf?x91208 [https://perma.cc/E64L-HPLG].

[213] Calo, *supra* note 206, at 1144–52.

[214] *Id.* at 1144.

[215] *Id.*

[216] *See* Solove & Citron, *Risk and Anxiety*, *supra* note 48, at 752 ("The motives of those who obtained the data are unknown . . . It will not be clear who has the data or what they will do with it.").

[217] *See id.*

[218] *See* Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 467 (2016).

entity. This harm may be individualized, that is, stemming from a given data breach, or systematic, where consumers experience these effects given the prevalence and scope of intrusions taking place in recent years.

Labeling psychological data breach harms as subjective is critical. This categorization reflects the important notion that psychological data breach harms can be experienced by affected consumers without there having to be any subsequent action or misuse beyond the initial data breach. Unfortunately, regulators and courts have consistently declined to recognize the subjective nature of these harms.[219] Nonetheless, the subjective nature of these harms does not make them any less real. Cybersecurity law should find appropriate methods to address this subjective nature, some of which are described in more detail in this Article's proposed framework below.

C. Objective Data Breach Harms

Many of the subjective data breach harms described above are also objective, that is, having some "adverse, real-world consequence."[220] Objective data breach harms are "external to the victim,"[221] in the sense that the harms involve an outside action with regards to the information compromised in a data breach. Wrongdoers may decide to use the compromised personal information to engage in identity theft or financial fraud.[222] In less publicized cases, unauthorized actors may decide to purchase the compromised data in bulk to perform doxing, microtargeting, stalking, or other data processing with the view of monetary gain.[223]

The relationship between subjective and objective data breach harms may not be self-evident. Yet, the objective data breach harm

---

[219] *See* Scholz, *supra* note 93, at 656 (arguing in the context of privacy law, Scholz asserts that "Courts' concerns with privacy cases, though, run deeper than the standing question. Courts worry that recognizing the privacy right in the absence of a clearly defined concrete harm may lead to unpredictable, excessive damages based on plaintiffs' subjective perceptions.").

[220] Calo, *supra* note 206, at 1148.

[221] *Id.*

[222] *See id.*

[223] *See id.* at 1148–49.

is the factor that reinforces the subjective data breach harm that consumers may experience—increased anxiety, depression, fear, PTSD, and other conditions.[224] In other words, there is an objective psychological and emotional harm, but the objective emotional harm is also a subjective harm experienced by the consumers affected. Understanding this relationship may also explain the overreliance of cybersecurity law on objective data breach harm, which presumptively is easier to prove, as it is external to the victim and involves more concrete evidence and quantifiable metrics. Both subjective and objective aspects of psychological data breach harms will be considered throughout the proposed framework that follows.

D. A Legal and Conceptual Framework for Psychological Data Breach Harms

Psychological data breach harms are predominately subjective in nature. They are experienced by the consumers affected individually.[225] Often, these consumers may be diagnosed with a recognized mental condition, making the harm objective as well.[226] Nonetheless, this subjective nature does not make psychological data breach harms any less worthy of recognition. In this context, the law is severely lagging. Cybersecurity law's shortcoming is that it is overly focused on objective data breach harms that can be demonstrated with external evidence. The CFAA, FTC's regulations, data breach notification laws, and other statutes are designed to respond to financial harms and unauthorized access to valuable data.[227]

Private litigation and FTC enforcement play an important role in potentially offering victims a remedy to psychological data breach harms. However, as previously discussed, both private litigation and FTC enforcement come after the fact and fail to address the underlying data collection practices that are not sensitive to the emotional and mental impact of the data collected if compromised. In addition, private litigation and FTC enforcement presume a

---

[224] *See id.* at 1143.
[225] Calo, *supra* note 206, at 1144.
[226] *Id.* at 1147–48.
[227] *See supra* Part III.

certain action, whereas there should be a substantial role for the breached company itself in minimizing the non-monetary impact of the breach experienced. Finally, both litigation and enforcement have already been proposed by scholars as solutions to future harms.

This Article adds to existing scholarship by considering subjective psychological data breach harms as mental health implications that require a proper response, which is not litigation per se. Cybersecurity law is designed to prevent, respond to, and mitigate financial harms, but it ought to be redesigned to also include the nuance of psychological data breach harms. There are tools and methods to address harms of a psychological nature and assist victims in dealing with and overcoming anxiety, depression, fear, and PTSD associated with data breaches. The law already recognizes the viability of some of these tools in the financial context, but little has been said on their capacity to also address psychological harms. This Article, therefore, proposes additional methods of responding to these emerging data breach harms.

1. Information Security Programs and Psychological Harms as Risks

The FTC requires companies that collect personal information to adopt an information security program.[228] An information security program involves procedures, methods, tools, and rules to protect the computers, network, data, and systems of the company.[229] For example, any company collecting sensitive consumer information is expected to encrypt the sensitive part of the information,[230] employ an information security officer,[231] train their employees on best

---

[228] *See* FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS 2 (2015), https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business [https://perma.cc/TB83-Svv8].

[229] *See id.*

[230] *See* Thomas Pahl, *Stick With Security: Store Sensitive Personal Information Securely and Protect it During Transmission*, FTC (Aug. 18, 2017), https://www.ftc.gov/news-events/blogs/business-blog/2017/08/stick-security-store-sensitive-personal-information-securely [https://perma.cc/Q8WT-MU5B].

[231] *See* William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1140 (2019) ("Developing a data security program requires considerable judgment and expertise in both management and information technology (IT), which is part of the reason so many responsible data custodians hire specialized chief information security officers (CISOs) and similar leaders.").

practices,[232] and audit policies periodically.[233] There are differences among different information security programs since companies often have varying degrees of risk, sizes, data collection practices, and sensitivity, as they "weigh costs and benefits, assess risk, and invest accordingly."[234] In other words, every information security program and cybersecurity policy is the result of a risk assessment. Designing an organization's cybersecurity approach is a result of a risk assessment that looks to potential threats, as well as the value of an organization's assets.[235] If the psychological impact of a data compromise is unknown, the organization will likely not implement the appropriate cybersecurity approach.

Turning to risk assessment: currently, risk assessment and cybersecurity policies primarily focus on financial losses and damage if a data compromise were to occur.[236] Under this approach, companies that assess their cybersecurity risk and develop policies for data protection are neither required nor expected to quantify the psychological risk of harm to consumers in the event of a breach. As some commentators put it, a cybersecurity policy "often includes a data classification regime or standard that categorizes data for purposes of specifying which cybersecurity requirements apply to particular data or system types."[237] At present, a robust system of classifying consumer data, where such data is not of a financial or medical nature, does not exist. Thus, is metadata protected? Should only financial information be encrypted? Or should other categories of information be encrypted as well?

---

[232] *Id.* at 1187 ("Most of the frameworks expect data custodians to train employees throughout the organization to ensure that they adhere to policy.").

[233] *Id.* at 1187–88 ("Numerous frameworks call for continual risk assessment. This effectively becomes a duty of ongoing monitoring. Some frameworks have begun specifying that data custodians have a duty to test their security systems, sometimes by particular means.").

[234] *Id.* at 1137.

[235] DEREK E. BAMBAUER ET AL., CYBERSECURITY: AN INTERDISCIPLINARY PROBLEM 15 (2021).

[236] *Id.*

[237] *Id.* ("[F]or example, sensitive personal information like biometric data might be required to be encrypted, while internal plans for marketing campaigns may not require encryption.").

Either not assessing the risk of psychological harm or ignoring consumer data that could cause such harm within the internal cybersecurity policy regime contributes to data breaches exposing sensitive pieces of information about consumers, which enables the loss of privacy and loss of control over consumers' information, as well as anxiety, depression, and other conditions. The same approach is illustrative of how the psychological harm resulting from data breaches can be traced back to the breached company designing and reevaluating its information security program that never accounted for such harm. The process of creating an information security structure internally is simply devoid of an assessment of risk of psychological harm, which puts consumers at risk.

Changing a company's understanding of what qualifies as an informational risk could contribute to decreasing the risk of psychological harm resulting from a data breach. Likewise, changing what qualifies as an informational risk could also decrease the likelihood of the company becoming a victim of a data breach, though the implication of a better designed information security program leads to a broader effect. For example, including the risk of psychological harm as part of the risk assessment process could better inform a company's policies on data collection, retention, protection, and use. It would affect the types of data collected by the company and the data's storage duration. If a company knows the likely psychological impact of a certain category of information getting compromised, the company is more likely to take the security of such data more seriously from an information security point of view. Thus, even if a breach were to occur, hackers would not be able to easily access consumer information that is embarrassing, private, or sensitive—albeit non-financial.

The FTC, in its *Start with Security: A Guide for Business*, generally recommends that businesses avoid collecting personal information that is not needed and that businesses hold on to information only for as long as necessary.[238] However, these recommendations are tied to businesses creating an "unreasonable

[238] FED. TRADE COMM'N, *supra* note 228, at 2.

risk,"[239] which is understood as involving consumers' monetary and financial risks. Involving psychological harm within the ambit of an "unreasonable risk" would likely improve the overall data security practices of the company in question. Additionally, including psychological harm in "reasonable risk" would likely legitimize regulatory enforcement, which is not as constrained by the same harm requirements as courts.[240]

All in all, cybersecurity is the process by which organizations try to protect their assets. This process mainly requires "regularly auditing data assets and risk, minimizing data, implementing technical, physical, and administrative safeguards, and creating and following a data breach response plan."[241] Awareness of the psychological impact of data breaches can better inform organizations on the appropriate degree of security and the tools necessary to protect consumer information even where such information has no apparent financial or medical nature.

2. Amending Cybersecurity Law: Recognizing Psychological Harm

As discussed earlier,[242] data breach notification and data security statutes suffer a major shortcoming in the context of psychological harm. Most federal and state statutes regarding breach notification and data security have a particularly narrow definition of "personal information," which typically serves as a threshold matter for whether the statute applies.[243] The concept of "personal information" is unlikely to include all or most pieces of information that can cause psychological harm, such as intimate details about consumers, the compromise of which would result in mental distress.[244]

---

[239] *See id.* ("[B]y holding on to the information without a legitimate business need, the FTC said BJ's Wholesale Club created an unreasonable risk.").

[240] *See* Citron & Solove, *Privacy Harms*, *supra* note 35, at 16.

[241] Richards & Hartzog, *supra* note 218, at 465–66.

[242] *See* discussion *supra* Parts III.C, III.D.

[243] *See, e.g.*, CAL. CIV. CODE § 1798.81.5; COLO. REV. STAT. §§ 6-1-713 to 713.5; FLA. STAT. § 501.171(2); TEX. BUS. & COM. CODE § 521.052.

[244] *See, e.g.*, Kosseff, *Hacking Cybersecurity Law*, *supra* note 30, at 836 (giving the example of the 2015 Ashley Madison breach, where a "website that matched people who were searching for extramarital affairs" was an incident that could "upend an individual's personal life.").

In addition, in the context of data breach notification law, when breached companies are evaluating whether a breach notification is required, their "risk of harm" assessment does not include the risk of psychological harm.[245] Thus, even where personal information is compromised, the breached company may still find a safe harbor if the company reasonably determines that the compromised information would not cause any financial harm to the consumers affected. This outcome is true for all states that have a "risk of harm" assessment in their statutes.[246] New York's statute is an important exception, as its "risk of harm" assessment requires the consideration of possible psychological harms.[247]

i. Expanding "Personal Information"

Incorporating the risk of psychological harm requires a reassessment of what constitutes "personal information." Different federal and state statutes on data breach notification and data security contain their own definitions of personal information.[248] All fifty states' data breach notification laws have their respective definitions of "personal information,"[249] as well as the Children's

---

[245] *See, e.g.*, CAL. CIV. CODE § 1798.81.5; COLO. REV. STAT. §§ 6-1-713 to 713.5; FLA. STAT. § 501.171(2); TEX. BUS. & COM. CODE ANN. § 521.052.

[246] *See, e.g.*, CAL. CIV. CODE § 1798.81.5; COLO. REV. STAT. §§ 6-1-713 to 713.5; FLA. STAT. § 501.171(2); TEX. BUS. & COM. CODE ANN. § 521.052.

[247] *See* discussion *infra* Part IV.D.2.(iii).

[248] *See e.g.*, CAL. CIV. CODE § 1798.29.

[249] *See* STEPTOE & JOHNSON LLP, COMPARISON OF US STATE AND FEDERAL SECURITY BREACH NOTIFICATION LAWS (Sept. 1, 2017), https://www.steptoe.com/images/content/1/7/v2/172961/SteptoeDataBreachNotificationChart.pdf [https://perma.cc/23B7-JZEU] (comparing all state breach notification laws including, for example, California's security breach notification law defining personally identifiable information as:

> [An] individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
>
> (1) Social security number.
>
> (2) Driver's license number or California Identification Card number.
>
> (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
>
> (4) Medical information.
>
> (5) Health insurance information.).

Online Privacy Protection Act,[250] Financial Modernization Act,[251] Fair Credit Reporting Act,[252] Health Insurance Portability and Accountability Act,[253] and the Privacy Act.[254]

This focus on financial harm is understandable, as these statutes were enacted long before the existence of the critical mass of research on psychological data breach harms present today. Some other statutes, while enacted more recently, likewise do not bridge the gap in failing to account for psychological data breach harm, as the statutory language is largely duplicative.

However, in light of all the evidence surrounding psychological data breach harms, the current approach—asking whether personal information was accessed—can be problematic when simply applied. Primarily, this approach might not include pieces of information that could nonetheless be exploited and misused against the data subjects and thus ignores the "many vectors of cyberattacks that [could] harm individuals."[255] Such information can vary and includes sexual orientation, nudity, metadata, contacts, private communications, location, and more. This shortcoming is not to say that the protection of personal information is not important for society as a whole, but rather that data points that do not qualify as "personal information" could nonetheless cause significant psychological harm to consumers if compromised. Expanding what constitutes "personal information," or, at the very least, creating a contextual and more flexible standard, is a desirable solution. As one

---

[250] *See* 15 U.S.C. § 6501(8); 16 C.F.R. § 312.2 (defining "personal information" as "individually identifiable information about an individual collected online" which, among other things, includes first and last name, home address, contact information, Social Security Number, and more).

[251] *See id.* § 6809(4)(A) (defining "nonpublic personal information" as "personally identifiable financial information").

[252] *See id.* § 1681.

[253] *See* 45 C.F.R. § 160.103 (2014) (defining "protected health information" broadly as "individually identifiable health information").

[254] *See* 5 U.S.C. § 552a(a)(4) (1974) (defining "record" as a combination of "education, financial transactions, medical history, and criminal or employment history" and the employee's "name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph").

[255] Kosseff, *Hacking Cybersecurity Law*, *supra* note 30, at 836.

commentator aptly stated in the context of the "personal information" approach's inadequacy, "a thousand words are . . . worth a picture."[256] Jeff Kosseff made a similar observation, noting that such non-personal information "still may be quite sensitive and valuable to identity thieves or other criminals, but the notification rule does not apply."[257] Essentially, the "personal information" approach represents a considerable gap.

An example where the law does accept a slightly more nuanced approach to personal information can be found, surprisingly, in the United States Sentencing Guidelines, where the Guidelines define "personal information" as:

> sensitive or private information involving an identifiable person (including such information in the possession of a third party), including (i) medical records; (ii) wills; (iii) diaries; (iv) private correspondence, including email; (v) financial records; (vi) photographs of a sensitive or private nature; or (vii) similar information.[258]

Furthermore, the United States Department of Justice Computer Crime and Intellectual Property Section in the Criminal Division has directed courts adjudicating CFAA cases that involve either "an intent to obtain personal information, or . . . the unauthorized public dissemination of information" to interpret "personal information" in the same manner as the U.S. Sentencing Guidelines.[259]

However, expanding the categories of personal information may not be sufficient per se, as computer science has demonstrated the capability to "reidentify" and "deanonymize" databases of anonymized personal information.[260] Essentially, society's

---

[256] Andrew McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. L. REV. 63, 70 (2003).

[257] KOSSEFF, CYBERSECURITY LAW, *supra* note 39, at 44.

[258] U.S. SENTENCING GUIDELINES MANUAL, § 2B1 (U.S. SENT'G COMM'N 2018).

[259] Comput. Crime and Intell. Prop. Section Crim. Div., *Prosecuting Computer Crimes* 139–40 (2nd ed. 2010) https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf [https://perma.cc/T8BD-TPCJ] (quoting U.S. SENTENCING GUIDELINES MANUAL, § 2B1.1(b)(15)).

[260] *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1704 (2010) ("Yet reidentification science exposes the underlying promise made by these laws—that anonymization protects privacy—as an empty one, as broken as the technologists' promises. At the very least, lawmakers must reexamine every privacy law, asking

understanding of what constitutes personal and non-personal, encrypted and decrypted, anonymized and deanonymized is immensely outdated. The peril in such anachronism is that a considerable portion of current information privacy law is outdated and dangerously ineffective, requiring a reexamination by lawmakers;[261] information that may seem unvaluable or unintelligible may nonetheless be misused.

Some other scholars raised a similar concern, which is called the "PII (Personal Identifiable Information) problem."[262] These scholars have examined whether the "unstable category" of PII—adopted by information privacy law—is flawed in the sense that information privacy law limits the scope of what information is worthy of legal protection.[263] PII is not a category limited to just one statute; rather, it is an overarching theme in all of information privacy and security law, both on the federal and state levels.[264] These scholars conclude that the delineations of PII and non-PII should not be abandoned. To achieve this end, they offer certain modifications to the PII approach, which would consider PII on a continuum of identifiability risk rather than a simple dichotomy, which the law in its "personal information" approach currently favors.[265]

Indeed, expanding "personal information" is not solely aimed at reforming data security and data breach notification statutes. Rather, expanding the scope of "personal information" is a reconceptualization of our thinking about assets worth protecting and the efficacy of our current statutory frameworks. As an additional example, while the CFAA does not use "personal information" where it criminalizes computer-related offenses, the CFAA's use of "information," "damage," "loss," and "value" should nonetheless be scrutinized as too narrow or lacking in

---

whether the power of reidentification and fragility of anonymization have thwarted their original designs.").

[261] *Id.*

[262] Paul Schwartz & Daniel Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV 1814, 1815–28 (2011).

[263] *Id.* at 1816.

[264] *Id.*

[265] *Id.* at 1879.

imagination.[266] This suggestion is by no means a call to expand the criminalization of computer-related activities, an approach that has been criticized,[267] but rather to ensure that the CFAA protects those assets that society considers critical. Though some scholars, such as Andrea Matwyshyn and Stephanie Pell, have been calling for the narrowing of what qualifies as "harm" under the CFAA to only "demonstrable technical harms experienced by a 'protected computer.'"[268] Nonetheless, the psychological impact of data breaches must be recognized under criminal law, and the CFAA may seem an inappropriate vehicle for some due to its focus on protected computers rather than the impact of hacking on individuals. Subject to more research, it may be desirable to focus on expanding cyberstalking and cyber harassment penalties to cover some psychological data breach harms so that the intentional infliction of significant emotional and psychological harm would be penalized and deterred.

Society's understanding of personal information, or information worthy of protection, cannot be reliant on a fixed list of information categories of a financial nature alone. A broader approach would mean more flexibility in how companies and regulators understand personal information at a given point in time. This would require closely observing the trends of data misuse by unauthorized individuals and organizations and a periodic readjustment of the meaning of what information needs protection.

ii. Scarcity Versus Sensitivity of Information Compromised

One way to approach the question of what qualifies as "personal information" is to supplement the definition of information's sensitivity with information's scarcity. Value, broadly speaking, is derived, not only from the sensitivity (e.g., credit card number), but also from the scarcity (e.g., sexual practices) of the information in

---

[266] For the criticisms and list of reform proposals, *see* EFF, COMPUTER FRAUD AND ABUSE ACT REFORM, https://www.eff.org/issues/cfaa [https://perma.cc/L743-6QHX].

[267] *See id.* (criticizing the call to expand the criminalization of computer-related activities).

[268] Andrea Matwyshyn & Stephanie Pell, *Broken*, 32 HARV. J. L. & TECH. 479, 515 (2019).

question.[269] Given the current motives of hackers, billions of sensitive records are available for purchase on the dark web, while scarce information is not often seen as valuable or readily exploitable.[270] Andrea Matwyshyn argues that the value of information in this day and age is derived primarily from its scarcity rather than its sensitivity.[271] This approach would transform the definition of personal information from a demographic and financial focus into a scarcity focus—how rare or secretive the compromised information is.

The introduction of the "Internet of Things" into the legal framework of cybersecurity could increase the importance of scarcity in the evaluation of the information's value. The "Internet of Things" refers to the plethora of "smart" devices with embedded sensors that collect information about their users and surroundings.[272] The growing number of "Internet of Things" devices suggests that there are categories of information that the law has not had the opportunity to fully consider and protect. Examples of such categories include video recordings, sensor data, user activity, temperature preference, physical activity data, driving habits, and many more.[273] As one legal scholar observes, the compromising of "Internet of Things" sensor data does not at

---

[269] *See* Andrea Matwyshyn, *Privacy, The Hacker Way*, 87 S. CAL. L. REV. 1, 15 (2013) ("Value in information is driven by scarcity, not sensitivity.").

[270] *See, e.g.*, Dan Goodin, *Data For a Whopping 26 Million Stolen Payment Cards Leaked in Hack of Fraud Bazaar*, ARS TECHNICA (Oct. 15, 2019), https://arstechnica.com/information-technology/2019/10/data-for-a-whopping-26-million-stolen-payment-cards-leaked-in-hack-of-fraud-bazaar/ [https://perma.cc/RY7P-TWYK].

[271] *See* Reporting Data Breaches: Is Federal Legislation Needed to Protect Consumers?: Hearing Before the Subcomm. on Com., Mfg., and Trade of the H. Comm. on Energy and Com, 113th Cong. 45 (2013) (statement of Dr. Andrea M. Matwyshyn, Assistant Professor of Legal Stud. and Bus. Ethics, on behalf of The Wharton School, Univ. of Pa.).

[272] Bruce Schneier, *Click Here to Kill Everyone*, N.Y. MAG. (Jan. 2017), https://nymag.com/intelligencer/2017/01/the-internet-of-things-dangerous-future-bruce-schneier.html. [https://perma.cc/95CJ-N86W].

[273] Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 98–117 (2014) (providing many implementations of the "Internet of Things" in our lives).

present trigger data breach notification laws.[274] Given this shortcoming, the argument goes that "sensor data are so sensitive and revealing that consumers should be reassured that [their sensor data] will not leak into the public sphere."[275] As legislators and regulators reassess sensitivity from an economic harm perspective, legislators and regulators should also consider scarcity, which can provide a viable alternative with the view of protecting consumers from psychological data breach harm, in particular where such information is indeed scarce (i.e., collected by individual "Internet of Things" devices).

While the data collected by the "Internet of Things" may undoubtedly cause psychological harm if compromised, "Internet of Things" data can also cause serious physical harm to consumers. For example, a hacked pacemaker may cause significant bodily injury, and in extreme cases, death.[276] To respond to these harms, one legal scholar proposes a torts regime for physical harms caused by "Internet of Things" devices.[277] The emerging challenges with the "Internet of Things" ecosystem will likely require further research on its psychological impacts and the potential liabilities that arise from those impacts. In short, the data collected by the "Internet of Things" has the potential to cause emotional and mental harm if compromised.

However, psychological harms must be part of a broader cybersecurity process. Scarcity alone can help determine the value of information due to its rarity, as well as afford information all of the equivalent protections as sensitivity, but scarcity does not tell the whole story about the psychological harm when information is compromised. Therefore, the scarcity approach must be supplemented with a "Psychological Exploitability Assessment," discussed in the next subpart.

---

[274] *Id.* at 137.

[275] *Id.* at 162.

[276] Lily Hay Newman, *A New Pacemaker Hack Puts Malware Directly on the Device*, WIRED (Sep. 8, 2018), https://www.wired.com/story/pacemaker-hack-malware-black-hat/ [https://perma.cc/89AJ-2CWK].

[277] Rebecca Crootof, *The Internet of Torts: Expanding Civil Liability Standards to Address Corporate Remote Interference*, 69 DUKE L.J. 583, 588 (2019).

iii. Psychological Exploitability Assessment and Risk of Harm

Both the definitional flaw in data security law and the risk-based flaw in data breach notification statutes require a change in approach so that the law considers the nature of the protected or compromised information. These two flaws can be remediated by assessing the *impact* of collecting data that could mentally and emotionally affect consumers if that data is accessed by hackers. "Impact" can be understood using the National Institute for Standards and Technology Guide for Conducting Risk Assessments, which defines "impact" as the "harm that can be expected to result."[278] In order to determine the impact of a potential or actual data breach on the mental health of affected consumers, breached companies should perform a Psychological Exploitability Assessment. This assessment would focus on the expected psychological harm that would result from a data breach. This assessment can apply both to the question of "what information is being protected?" and to the question of "is there a risk of harm?"

The Psychological Exploitability Assessment is a parallel concept to the "risk of harm" assessment. Instead of assessing the likelihood of financial harm to consumers affected by a data breach, the breached company would look to the nature and scope of the compromised information to determine how likely wrongdoers are to exploit the information for blackmail, coercion, shaming, exposure, and other objectionable uses of the breached information. This assessment would determine: (1) whether a piece of information that is not strictly within the ambit of "personal information" should nonetheless be protected under the current cybersecurity structure of the entity, and (2) if a breach does occur, what the obligations are of the breached entity toward its consumers (e.g., notification and remedies). The scope and nature of the Psychological Exploitability Assessment will likely change from time to time, as entities collect new categories of information, and additional misuses of breached information surface and become more widely recorded. Since cybersecurity is a process of

[278] NAT'L. INST. OF STANDARDS & TECH., SPECIAL PUBLICATION 800-30 REVISION 1: GUIDE FOR CONDUCTING RISK ASSESSMENTS 11 (Sept. 2021), http://dx.doi.org/10.6028/NIST.SP.800-30r1 [https://perma.cc/6DVS-XKNU].

responding to emerging threats, constantly reevaluating what "psychological exploitability" means makes sense.

The basis of the Psychological Exploitability Assessment is that of trust. Consumers trust data collectors to safeguard their data and keep them safe from harm, whether physical, financial, or psychological.[279] As one legal scholar argues, "if we want to be serious about safeguarding trust, more entities need to be responsible for security, while the law must recognize broader theories of harm, such as increased risk and anxiety."[280] Safeguarding trust and recognizing additional harms would involve adopting the "mentality of data stewardship,"[281] which requires that entities protect data against new threats.

As mentioned above, New York law has made some advancements on this front, though incomplete. The 2019 amendment to the New York data breach notification statute now requires that breached companies consider emotional harms as part of their risk of harm assessment. The statute reads:

> Notice to affected persons under this section is not required if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the person or business reasonably determines such exposure will not likely result in misuse of such information, or financial harm to the affected persons or emotional harm.[282]

This statute reflects the only recognition of emotional harm in a state data breach notification statute to date. As welcome as the New York approach is to the risk of psychological harm, the statute does not provide guidance on the circumstances where emotional harm could be found.[283] Accordingly, this lack of guidance serves as a prime example of where a Psychological Exploitability Assessment could assist both breached entities and regulators in determining the

---

[279] Jack Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1186 (2016) ("[I]nformation fiduciaries have special duties to act in ways that do not harm the interests of the people whose information they collect, analyze, use, sell, and distribute.").

[280] Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B. C. L. REV. 1687, 1749 (2020).

[281] Richards & Hartzog, *supra* note 218, at 466.

[282] N.Y. GEN. BUS. LAW § 899-aa (d)(2)(a).

[283] *Id.*

likelihood of emotional and mental harm in a given case. The Psychological Exploitability Assessment would differ between different organizations based on different factors. It would take into account the type of the compromised data, the scope of the data, digital forensic and other expert assessments on the likelihood and nature of harms resulting from the breach, current and future trends in data breaches, and more.

HIPAA is another example where non-financial harms have been incorporated into the risk of harm assessment. In 2013, the U.S. Department of Health and Human Services ("HHS") considered a rule that, under HIPAA, would have elevated an "incident" to the level of a security breach of protected health information whenever a breach posed "a significant risk of financial, reputational, or other harm to the individual."[284] Under this view of harm, psychological data breach harm to patients would support labeling an incident as a security breach, thereby triggering all legal consequences under the statute. This definition of "incident" also took the subjective approach to viewing psychological data breach harms and has thus been criticized by some scholars as overly focused on a subjective standard.[285] Eventually, the HHS reversed course and succumbed to the criticism, offering a more objective standard for security breaches.[286] This unfortunate reversal is due to a misunderstanding of the nature of psychological data breach harms in the legal and regulatory sphere. In particular, the legal and regulatory sphere is lagging behind current research indicating the unambiguous psychological and emotional harms arising from data breaches.

Other legal systems have adopted an approach to breach notification that reflects the logic underlying psychological assessment. In Australia, data breach notification is mandatory when the breach will likely cause serious harm to the affected

---

[284] Modifications to the Breach Notification Rule Under the HITECH Act, 78 Fed. Reg. 5565, 5639 (Jan. 25, 2013).

[285] *Id.* at 5641 ("[C]ommenters argued that, rather than a subjective standard measuring the risk of harm to an individual, the final rule should include a more objective standard against which entities would be required to assess risk.").

[286] *Id.* at 5641–42.

consumers.[287] Among the harms recognized is "serious psychological harm."[288] Accordingly, whenever breached entities in Australia are assessing their obligation under data breach notification law, one of the harms under the risk of harm assessment is "serious psychological harm." This approach largely mirrors New York's recent amendment to its data breach notification law.

Overall, a Psychological Exploitability Assessment would take into account not only the subjective nature of data breach harms, but also their objective nature; therefore, criticism that focuses on the general indeterminacy of subjective harms should not prevent the implementation of this assessment. The Psychological Exploitability Assessment should be informed by interdisciplinary expertise on psychological harms: from psychologists, psychiatrists, sociologists, lawyers, and information security professionals. By utilizing experts, the Psychological Exploitability Assessment would reduce the indeterminacy that many critics raise as a problem to considering the subjective nature of data breach harms.

iv. Detaching Psychological Data Breach Harm from Data Misuse

Conditioning the existence of psychological data breach harm on whether there has been any data misuse conflates two different questions and ignores the nature of psychological data breach harm. When making such a determination, courts and regulators have frequently reasoned that plaintiffs or victims cannot claim any emotional or mental harm if there is no actual proof of data misuse. For example, in *Willey v. J.P. Morgan Chase*,[289] a district court held that the plaintiff "ha[d] not alleged that his or any class member's information ha[d] actually been misused"[290] and therefore, the plaintiff's

> claims for expenses related to credit monitoring, anxiety, emotional distress, and loss of privacy all [arose] due to the probability that his data

---

[287] *See What Is a Notifiable Data Breach?* AUSTRALIAN GOVERNMENT, OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER, https://www.oaic.gov.au/privacy/data-breaches/what-is-a-notifiable-data-breach/ [https://perma.cc/4A58-V3F9] (last visited Sept. 18, 2021).

[288] *Id.*

[289] Willey v. J.P. Morgan Chase, N.A., No. 09 CIV. 1397(CM), 2009 WL 1938987 (S.D.N.Y. July 7, 2009).

[290] *Id.* at *10.

> might have been misused. Because this does not rise to the level of actual damages, the state law claims fail to allege actual damages and must be dismissed.[291]

The *Willey* court's traditional approach to harm during data breaches ignores the subjective and objective nature of psychological data breach harms, which does not require actual data misuse in order for victims to experience incredibly real and often debilitating mental and emotional consequences.[292]

While actual data misuse may serve as a basis for a finding of a plaintiff's allegation of emotional and mental harm, actual data misuse should not be a mandatory element that plaintiffs must prove by introducing such a pleading. Courts and regulators should refocus their analyses from requiring proof of data misuse to showing the nature of the breached information and the potential misuses of the compromised information, as well as providing expert testimony on the plaintiffs' psychological harms. As one commentator notes, "there is a growing sense that individuals are harmed even where their information has not been used to commit identity theft."[293] In addition, another legal scholar argues that courts should actually "permit liability at a much lower threshold of harm and fault or blameworthiness," an approach that conceptualizes cybersecurity similarly to the principles of a contractual bargain.[294]

Whether data misuse has occurred should be a separate inquiry from the preceding question of whether psychological data breach harm exists. Data misuse can surely strengthen the overall evidence that victimized consumers present, but data misuse should not be a mandatory, prima facie element, especially where psychological

---

[291] *Id.*

[292] *See* Benjamin C. West, *No Harm, Still Foul: When an Injury-in-Fact Materializes in a Consumer Data Breach*, 69 HASTINGS L.J. 701, 716 (2018) ("[T]here is actual [psychological] harm at the breach stage, regardless of whether there is evidence that the obtained data was improperly 'used.'").

[293] Ashenmacher, *supra* note 104, at 6.

[294] Derek E. Bambauer, *Privacy Versus Security*, 103 J. CRIM. L. & CRIMINOLOGY 667, 680 (2013) ("Courts do not care whether a breaching party is blameworthy, or whether the harm resulting from a breach is weighty or small. Merely showing breach is sufficient.").

harms are often caused merely by virtue of a data breach occurring, which can be determined objectively.

v. Isolating Psychological Harm from Physical Harm

Relatedly, requiring physical harm or a physical manifestation of psychological harm, as a prerequisite for damages, ignores data breach victims whose psychological harm is not accompanied by any physical manifestations.

Some state laws require proof of a physical manifestation of psychological harm in data breach cases. For example, in Nevada, such proof is required and was demonstrated in *Pruchnicki v. Envision Healthcare Corp*.[295] In *Pruchnicki,* the district court noted that Nevada law requires a plaintiff to "demonstrate that he or she has suffered some physical manifestation of emotional distress in order to support an award of emotional damages."[296] In denying the plaintiff's damages for emotional harm resulting from a data breach, the *Pruchnicki* court cited the Nevada Supreme Court in *Betsinger v. D.R. Horton*,[297] which held that an emotional distress claim arising from "a failed real estate and lending transaction" cannot survive without "some physical manifestation of emotional distress."[298] This approach—requiring proof of a physical harm—risks excluding data breach victims, who suffer harm of a solely psychological nature.

The U.S. Supreme Court followed the same logic in *Federal Aviation Administration v. Cooper*, which involved the mishandling of medical records, whereby the U.S. Supreme Court held that the plaintiff needed to show "actual damages" under the federal Privacy Act of 1974: that emotional distress alone was insufficient, even if proven.[299] The U.S. Supreme Court explained that "the Privacy Act does not unequivocally authorize an award of damages for mental or emotional distress."[300]

---

[295] Pruchnicki v. Envision Healthcare Corp., 439 F. Supp. 3d 1226, 1233–34 (D. Nev. 2020).

[296] *Id.* at 1233 (quoting Betsinger v. D.R. Horton, Inc., 232 P.3d 433, 436 (Nev. 2010)).

[297] *Pruchnicki*, 439 F. Supp. 3d at 1233–34; *Betsinger*, 232 P.3d at 436.

[298] *Betsinger*, 232 P.3d at 436.

[299] Fed. Aviation Admin. v. Cooper, 566 U.S. 284, 304 (2012).

[300] *Id.*

The U.S. Supreme Court's approach is part of what Professors Solove and Citron identified as a "cramped view of harm," which requires harm to be vested, that is, "already materialized in the here and now."[301] "Plaintiffs must experience physical, monetary, or property damage or, at least, the damage must be imminent."[302] In the context of data breach harms, approaching psychological harms through physical manifestations is problematic, as these harms rarely have physical manifestations besides the breaches themselves.[303]

A more appropriate approach for courts, regulators, and companies is to treat psychological data breach harm as a separate harm from any other physical manifestation of harm. In the 2015 United Kingdom case of *Google v. Vidal-Hall,*[304] the U.K. Court of Appeal adopted this "separated" approach. In *Vidal-Hall,* the plaintiffs filed suit under the U.K. Data Protection Act of 1998 ("DPA"), arguing that, by invading their privacy and collecting sensitive information, Google had caused them emotional distress.[305] The Court, therefore, had to inquire whether the term "damage" within the meaning of the statute included non-pecuniary damages, such as emotional distress. By looking at the purpose of European data protection legislation and interpreting the DPA, the Court concluded that the law protects "privacy rather than economic rights," and therefore, the law compensates individuals whose data privacy has been invaded by a data controller, which caused the individual emotional distress.[306] In effect, the *Vidal-Hall* decision made the process easier for plaintiffs to bring suit with compensation claims deriving solely from emotional and mental

---

[301] Solove & Citron, *Risk and Anxiety*, *supra* note 48, at 754.

[302] *Id.*

[303] *Id.* at 755.

[304] Google Inc. v. Vidal-Hall & Ors [2015] EWCA Civ 311 at ¶21 (27 March 2015).

[305] *Id.* at ¶5 ("The claimants allege in respect of their claims for misuse of private information and/or breach of confidence, that their personal dignity, autonomy and integrity were damaged, and claim damages for anxiety and distress. In respect of their claims under the DPA, they claim compensation under section 13 of the DPA for damage and distress. In neither case is there a claim for pecuniary loss.").

[306] *See id.* at ¶77.

distress. Courts and regulators should conceptualize psychological data breach harms similarly—in isolation from any physical manifestation or pecuniary damages. Such an approach might lead to an increase in case load, which is a systemic problem to be addressed by legislators. However, the existence of harm and its redressability is a separate issue that should be resolved by individual courts.[307]

vi. Rethinking Remedies for Psychological Data Breach Harms

The nature of psychological data breach harms offers an opportunity to rethink remedies in the context of cybersecurity law. Ensuring an appropriate remedy for informational harms has already been proposed in privacy law scholarship. For example, in "Privacy Harms," Professors Citron and Solove identified three goals of enforcement in privacy law: compensation, deterrence, and equity.[308] Citron and Solove have raised the concern that often, a mismatch occurs between the goal of enforcement and the remedy provided to victims. For example, the goal may be equity for a specific situation, yet the only remedy available is monetary compensation, which does little to address real and debilitating psychological harm.

This concern regarding a mismatch between goals and remedies also holds in cybersecurity law. Consumers who are psychologically harmed as a result of a data breach may wish to secure monetary compensation; however, cybersecurity law should consider broader goals, such as equity and deterrence. The logic that cybersecurity law enforcement goals should extend beyond monetary compensation suggests that the law should make available other remedies to harmed consumers.

---

[307] *See* Citron & Solove, *Risk and Anxiety*, *supra* note 47, at 782 ("Despite these concerns, which are legitimate, courts should not focus on them when evaluating whether there is a legally cognizable harm. Courts should analyze whether the law should recognize harms independently from the downstream consequences of such recognition. Often, these downstream consequences become conflated with the issue of whether there should be legally cognizable harm. Harm should not be denied merely because finding harm will involve facing challenging issues about the form and amount of redress.").

[308] Citron & Solove, *Privacy Harms*, *supra* note 35, at 46.

An example of an appropriate remedy in this context is psychological counseling. Just as breached companies must provide credit monitoring and identity protection services for a period of time after a breach, breached companies should likewise be required to compensate consumers with psychological data breach harms through counseling that responds to the conditions the consumers experienced. With some consumers, these conditions may arise much later, but remedies should nonetheless be available, within a reasonable amount of time.

Already, some companies offer "psychological first-aid" for employees whose sensitive information has been compromised.[309] In addition, a group of insurance company Chief Risk Officers has recognized "psychological support" as its own loss type, which encompasses "assistance and psychological support to the victim after a cyber [breach] event leading to the circulation of prejudicial information on the policyholder without . . . consent."[310] Thus, the cyber insurance industry may have a role to play in increasingly recognizing coverage for costs associated with psychological data breach harms.

Considering that psychological data breach harms are rampant, deterrence should be one of the goals of cybersecurity law. Accordingly, when the goal of liability is deterrence, the remedy should be designed consonantly. However, who should be deterred in this context? The answer may vary, but primarily, cybersecurity law's goal should center around the obligation of the data collector to limit collection and implement procedures that internalize the emotional and mental impact of any compromise of collected data.

Deterrence goes beyond the obligations of the data collector. For example, any potential intruder should be deterred from using compromised information to inflict psychological harm. The CFAA, discussed in Part III.A., *supra*, creates certain thresholds like "information," "damage," "loss," and "value," which ought to be

---

[309] Guynn, *supra* note 7.

[310] THE ORGANISATION FOR ECONOMIC CO-OPERATION [OECD], ENHANCING THE ROLE OF INSURANCE IN CYBER RISK MANAGEMENT 21 (2017), https://www.oecd.org/daf/fin/insurance/Enhancing-the-Role-of-Insurance-in-Cyber-Risk-Management.pdf [https://perma.cc/7KUJ-V8PU].

interpreted as being protective of non-financial information that has the potential to inflict psychological harm. An expansion of "personal information" and the key thresholds in the CFAA would likely have some deterrent power, though deterrence is not the sole goal of cybersecurity law, as corporations must—first and foremost—protect the confidentiality, integrity, and availability of their systems and data.

Overall, compensating the costs of psychological data breach harms would be a good start. Compensation may be the direct obligation of the breached organization to cover consumers' expenses related to the breach. Alternatively, as some have suggested, the creation of a "data breach compensation fund,"[311] modeled after the Comprehensive Environmental Response, Compensation, and Liability Act's Superfund, would cover the high costs associated with psychological data breach harms.[312] The data breach compensation fund would "balance the high cost of lawsuits with the aggregated psychological and economic harms to countless individuals from data insecurity."[313]

IV. CONCLUSION

Cybersecurity law is currently designed to predominately address financial harms resulting from data breaches. While there are areas of cybersecurity law that have slightly broader approaches to harm, psychological data breach harms are ignored by the majority of cybersecurity law's statutory and regulatory frameworks. Research from psychology, psychiatry, sociology, and cybersecurity on psychological data breach harms has shown how devastating data breaches can be for consumers, yet law and policy have failed to keep up with this overwhelming evidence.

This Article proposes a framework for cybersecurity law that would afford more recognition and protection for information that may inflict psychological harm on consumers, such as emotional

---

[311] Carol M. Hayes, *Comparative Analysis of Data Breach Laws: Comprehension, Interpretation, and External Sources of Legislative Tex*t, 23 LEWIS & CLARK L. REV. 1221, 1278 (2020).

[312] 42 U.S.C. §§ 9601–75.

[313] Hayes, *supra* note 311, at 1278.

and mental conditions, including anxiety, depression, and PTSD. This proposed framework approaches cybersecurity as a process and focuses on the evolving nature of harm, which requires a constant revaluation and reassessment of what assets ought to be protected. Rethinking cybersecurity law means reexamining key cybersecurity terminology, adjusting the categories of information that require protection, developing the appropriate remedies for psychological data breach harms, and thinking about psychological data breach harms in relation to data misuse and physical harms. This framework is only the beginning, as newer techniques of information abuse are likely to be introduced in the coming years. Notably, the framework proposed in this Article revolves around ensuring flexibility in the right areas of cybersecurity law and therefore will offer the nimbleness required to respond to these various new and emerging threats.

In the future, Congress and the States may need to draft new legislation, and regulatory agencies may need to update their guidelines and enforcement priorities. However, cybersecurity law and policy, as it stands today, may nonetheless prove somewhat effective to resolve the difficulties arising from data breaches that create psychological data breach harms. The first step is to acknowledge the psychological impact of data breaches and allow this fact to inform existing cybersecurity law and policy, ultimately resulting in a legal framework that holistically protects consumers' psychological and emotional wellbeing from the consequences of data breaches.