Richmond Journal of Law & Technology Volume XXIX, Issue 1

WHEN THE CONSUMER BECOMES THE PRODUCT: UTILIZING PRODUCTS LIABILITY PRINCIPLES TO PROTECT CONSUMERS FROM DATA BREACHES

Mason Storm*

Cite as: Mason Storm, *When the Consumer Becomes the Product: Utilizing Products Liability Principles to Protect Consumers from Data Breaches*, 29 RICH. J.L. & TECH. 1 (2022).

* J.D. Candidate, 2023, University of Richmond School of Law; B.A., 2019, University of North Carolina at Wilmington. I am thankful for the University of Richmond Journal of Law and Technology's editors and staff who helped edit and improve this article. I would also like to thank Professor Anne Toomey McKenna and Professor Rebecca Crootof for introducing me to technology law concepts and Professor Carl W. Tobias for doing the same for products liability and helping me publish this article.

I. INTRODUCTION

[1] Current products liability law is not equipped to handle products in the age of data. The potential for harm was traditionally coupled with the product: wherever the product went, the potential for harm followed. As the product proceeded down the supply chain—from the manufacturer to the wholesaler, to the retailer, and then to the consumer—the risk of harm went with it. Data collected from consumers[1] carries a different risk. Data products originate with a person[2] who is often the consumer of a physical product in the traditional supply chain[3]. That data product is then transmitted to another entity,[4] which is often the manufacturer of the physical product that the consumer purchased. The potential for harm, however, stays with the consumer because she is the one that suffers from her data being stolen or made public. Thus, in a data breach, the collector does not suffer harm—the original consumer does.

[2] This decoupling of the harm from the product prevents a straightforward application of products liability law to data breaches. However, many of the rationales for products liability still apply.[5] For example, the collector is in the best position to prevent harm to the consumer through its data security system, consumers lack the knowledge required to effectively prevent or mitigate the harm and holding collectors liable for failing to safeguard consumer data would incentivize collectors to

[1] Hereinafter referred to as "data products."

[2] This person will be referred to as the "consumer" or the "original consumer."

[3] The product in the traditional supply chain will be referred to as the "traditional product."

[4] This entity will be referred to as the "collector," since it is collecting the data product.

[5] *See* Michael Ruttinger, *Lessons for Data Breach Lawyers From Product Liability*, LAW360 (Jan. 28, 2018, 11:09 AM), https://www.law360.com/articles/1005884/lessons-for-data-breach-lawyers-from-product-liability [https://perma.cc/VA9E-UBH8].

take all steps possible to safeguard the data. Given the content and quantity of data amassed by collectors and the precipitous rise in data breaches, consumers need a way to seek recourse in the event their data is exposed in a data breach.

[3] Congress or state legislatures—not the courts—should be the ones to act for three reasons. First, the application of products liability to data breaches does not currently fit within the common law products liability framework, even though the rationale for applying products liability to data products is the same as applying products liability to traditional products. Second, courts are increasingly hesitant to expand common law products liability protections. Third, common law changes often take place over the course of decades, but the problems posed by data breaches are urgent. While I encourage state legislatures to take action, Congress would be the ideal actor to tackle these issues because a rule of nationwide applicability would provide consumers and manufacturers certainty as to their rights and obligations regarding data security.[6]

[4] Congress or state legislatures should adopt and adapt the Restatement (Third) of Torts: Products Liability (1998)[7] as the standard for data breaches. The Restatement Third provides for a strict liability standard for manufacturing defects and a negligence standard for both design and warning defects.[8] Adopting the Restatement Third for data breaches would strike the appropriate balance by protecting consumers while still encouraging both industry innovation and safer data collection practices.

[6] *See* Alan Butler, *Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices?*, 50 U. MICH. J. L. REFORM 913, 930 (2017).

[7] RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY (AM. L. INST. 1998).

[8] *Id.* § 2.

[5] This article will begin by explaining the importance of data protection for consumers in Section II. Section III will provide a history of products liability law and explain how privacy law may supply the basis for standing in federal courts. Finally, Section IV will explain how this proposal differs from existing data breach laws, why the Restatement Third is the best template for drafting a data breach law, and how the Restatement Third will need to be adapted to encompass data breaches.

II. THE IMPORTANCE OF DATA PROTECTION

[6] When Mark Zuckerberg was in the early stages of creating Facebook, a friend of his asked how Zuckerberg was able to accumulate information on his fellow classmates at Harvard.[9] Zuckerberg responded: "[p]eople just submitted it. I don't know why. They 'trust me.' Dumb [f***s]."[10] Twenty some years later, Zuckerberg's statement continues to ring true.

[7] In contrast to the basic data collected by Zuckerberg in the early days of Facebook (consisting of email addresses, photos, and physical addresses),[11] modern consumers willingly hand over sensitive information—including social security numbers, bank account information, medical information, and even biometric information[12]—to unknown third

[9] Nicholas Carlson, *Well, These New Zuckerberg IMs Won't Help Facebook's Privacy Problems*, BUSINESS INSIDER (May 13, 2010, 11:19 AM), https://www.businessinsider.com/well-these-new-zuckerberg-ims-wont-help-facebooks-privacy-problems-2010-5 [https://perma.cc/42EX-X6BX].

[10] *Id.*

[11] *Id.*

[12] *See* Kimberly Steele, *A Guide to Types of Sensitive Information*, BIGID (Nov. 3, 2021), https://bigid.com/blog/sensitive-information-guide/ [https://perma.cc/VVZ9-BES9] (listing types of sensitive information collected by organizations); *Biometrics*, U.S. DEP'T OF HOMELAND SEC. (Dec. 14, 2021), https://www.dhs.gov/biometrics [https://perma.cc/

parties via the internet.[13] One danger of such prolific data sharing is identity theft. In 2018, about 23 million people—almost 10% of adults in the United States—became victims of identity theft.[14] Almost all of these instances of identity theft involved the misuse of an existing account, including financial accounts.[15] Biometric information is even more sensitive and carries more drastic consequences for victims of identity theft; unlike social security numbers and account information, biometric identifiers cannot be changed.[16] Thus, "once [biometric information has been] compromised, the individual has no recourse, is at heightened risk of identity theft, and is likely to withdraw from biometric-facilitated transactions."[17]

[8] Although theft of sensitive information can be inherently dangerous for victims, the theft of more mundane information like email account

WMM4-A84H] ("Biometrics are unique physical characteristics, such as fingerprints, that can be used for automated recognition."); *Types of Biometrics*, BIOMETRICS INST., https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/ [https://perma.cc/LP6R-P9UL] (showing that biometric information goes well beyond fingerprints).

[13] Simon Chandler, *We're giving away more personal data than ever, despite growing risks*, VENTUREBEAT (Feb. 24, 2019, 8:35 AM), https://venturebeat.com/big-data/were-giving-away-more-personal-data-than-ever-despite-growing-risks/ [https://perma.cc/PSU9-SVMP].

[14] *Victims of Identity Theft, 2018*, BUREAU OF JUST. STAT. (Apr. 2021), https://bjs.ojp.gov/content/pub/pdf/vit18_sum.pdf [https://perma.cc/7CCE-4USF].

[15] *Id*.

[16] *See* 740 ILL. COMP. STAT. 14/5(c) (2022).

[17] *Id*. see generally ANNE TOOMEY MCKENNA AND CLIFFORD S. FISHMAN, WIRETAPPING AND EAVESDROPPING (3rd ed. 2007) (providing and in-depth discussion on biometrics and privacy issues.

information can be devastating as well. Take the 2014 Yahoo data breach for instance.[18] Yahoo's hacking was facilitated by Russian FSB agents in coordination with others.[19] The DOJ alleged that the hackers stole information from at least 500 million Yahoo accounts.[20] The Yahoo hack was just the tip of the iceberg: the stolen information was also used to access Google accounts and those of other providers.[21] The stolen information included that of FSB targets, Russian journalists, and Russian and United States government officials.[22] The Yahoo hack also targeted financial institutions.[23] Individual users of seemingly anonymous email accounts were identified when the hackers gained access to backup recovery accounts and answers to challenge questions.[24] The hack was carried out through a simple phishing email.[25]

[9] This is to say nothing of hacks targeting institutions holding the more sensitive information discussed above. The 2017 hack of Equifax—

[18] *See U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts*, DEP'T OF JUST. (Mar. 15, 2017), https://www.justice.gov/ opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions [https://perma.cc/3XF4-HZEH] [hereinafter *Russian Conspirators*].

[19] *Id*.

[20] *Id*.

[21] *Id*.

[22] *Id*.

[23] *Russian Conspirators*, *supra* note 18.

[24] *Id*.

[25] Martyn Williams, *Inside the Russian hack of Yahoo: How they did it*, CSO (Oct. 4, 2017, 5:16 AM), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html [https://perma.cc/XM32-DE5A].

which, like the Yahoo hack, was carried out by a foreign intelligence agency[26]—exposed the personal information, including "social security numbers, names, addresses, and drivers licenses (sic)," of at least 143 million Americans.[27] Unfortunately, incidents like these are not uncommon.[28] In fact, data breaches are so prevalent that they are now ranked at the end of the year like popular songs.[29] Because so many large companies that store personal information have been hacked, it is almost impossible to track a case of stolen identity to a single data breach.[30] Frighteningly, the risk associated with biometric information is especially great because biometric information cannot be changed.[31]

[10] Since Zuckerberg's candid comments about Facebook's early users trusting him with their data, the landscape of data collection has changed

[26] Brian Barrett, *How 4 Chinese Hackers Allegedly Took Down Equifax*, WIRED (Feb. 10, 2020, 12:52 PM), https://www.wired.com/story/equifax-hack-china/ [https://perma.cc/PZG5-VHCN].

[27] Adam Shell, *Equifax data breach: Number of victims may never be known*, USA TODAY (Sep. 17, 2017, 7:00 AM), https://www.usatoday.com/story/money/2017/09/17/equifax-data-breach-number-victims-may-never-known/670618001/ [https://perma.cc/9NKG-XMBV].

[28] *See* Maria Henriquez, *The top data breaches of 2021*, SECURITY (Dec. 9, 2021), https://www.securitymagazine.com/articles/96667-the-top-data-breaches-of-2021 [https://perma.cc/WC4E-ZXPH].

[29] *See id.*

[30] *Id.*

[31] *Biometric Data Breach Security Threats*, IDENTITY MGMT. INST. (last visited Sept. 1, 2022), https://identitymanagementinstitute.org/biometric-data-breach-security-threats [https://perma.cc/9AKL-GN79].

significantly.[32] Implicit in Zuckerberg's statement is that those users *actually knew* that Facebook had this data.[33] Today, the information that people hand over to companies takes on a life of its own once it is disclosed.[34] Those photos you uploaded to Facebook? Facebook may have used them to create a geometric template of your face and to train its facial recognition algorithm via Facebook's "Tag Suggestions" feature.[35] The Amazon Alexa you forgot you have? It may be collecting and storing voiceprints of anyone who talks in its vicinity—whether they have agreed to Amazon's terms of service or not.[36] Did you accept a website's cookies just to remove that annoying banner from the bottom of the screen? You just allowed the site to access information about you which may include your "browsing habits and history, personal preferences and interests,"

[32] Michael Ngadaonye, *Facebook And Data Privacy Issues*, THE CIRCULAR (Mar. 26, 2021), https://thecircular.org/facebook-and-data-privacy-issues/ [https://perma.cc/LJ7P-B7ER].

[33] *See* Julia Carrie Wong, *I was one of Facebook's first users. I shouldn't have trusted Mark Zuckerberg*, THE GUARDIAN (Apr. 17, 2018, 3:01 PM), https://www.theguardian.com/technology/2018/apr/17/facebook-people-first-ever-mark-zuckerberg-harvard [https://perma.cc/LYR7-RP4P].

[34] *See* Max Freedman, *How Businesses Are Collecting Data (And What They're Doing With It)*, BUSINESS NEWS DAILY, https://www.businessnewsdaily.com/10625-businesses-collecting-data.html [https://perma.cc/Z44D-PNPK] (Aug. 25, 2022).

[35] *Facebook brings face recognition to all users, discontinues 'Tag Suggestions*,' REUTERS (Sep. 3, 2019, 2:06 PM), https://www.reuters.com/article/us-facebook-face-recognition/facebook-brings-face-recognition-to-all-users-discontinues-tag-suggestions-idUSKCN1VO2C7 [https://perma.cc/WQ89-EPKX].

[36] Wendy Davis, *Amazon Must Face Children's Privacy Claims Over Voiceprint Collection*, MEDIAPOST: DIGITALNEWSDAILY (Apr. 24, 2021), https://www.mediapost.com/publications/article/362675/amazon-must-face-childrens-privacy-claims-over-vo.html [https://perma.cc/Z2PX-LAHD].

personal information, and more.[37] People constantly shed data, often without the slightest clue of where it is going or how it is used.[38]

[11] Although this article seeks to address the implications of data breaches as it pertains to individuals, it is critical to appreciate how data collection and data breaches can also have broader societal consequences as well. Take Strava, for example. Strava, coined as the social network for athletes, allows its fitness trackers to link with a user's social media account, enabling easy data sharing for its users.[39] The military has used the app to promote physical training amongst its members.[40] One of Strava's features is GPS tracking. As a marketing ploy, Strava shared a heatmap it created by combining the running routes of its users to show how popular its app has become.[41] This practice inadvertently revealed the location of secret military bases in foreign countries.[42] Although willingly shared by Strava, the data could have been uncovered if a hacker wanted to infiltrate its system. [43]

---

[37] Alison Grace Johansen, *Should you accept cookies? 5 times you definitely shouldn't*, NORTON (Aug. 15, 2022), https://us.norton.com/internetsecurity-privacy-should-i-accept-cookies.html [https://perma.cc/6TRU-PYNB].

[38] *See* Bhaskar Chakravorti, *Why It's So Hard for Users to Control Their Data*, HARV. BUS. REV. (Jan. 30, 2020), https://hbr.org/2020/01/why-companies-make-it-so-hard-for-users-to-control-their-data [https://perma.cc/NT8R-EN26].

[39] *Strava Features*, STRAVA, https://www.strava.com/features [https://perma.cc/AH9M-PUSZ].

[40] *See* Jeremy Hsu, *The Strava Heat Map and the End of Secrets*, WIRED (Jan. 29, 2018, 7:14 PM), https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/ [https://perma.cc/5RD7-W26L].

[41] *See id.*

[42] *Id.*

[43] *See id.* Some companies—including companies storing medical records for research—anonymize data by removing personal identifiers, but this process is highly suspect and can be defeated in a process known as re-identification. *See* Gina Kolata, *Your Data Were*

[12] Finally, I want to address phone location tracking. In 2019, the New York Times published an opinion piece trumpeting research on a file from a location data company that collects location data from code hidden in mobile phone apps.[44] The file contained "50 billion location pings from the phones of more than 12 million Americans" collected in 2016 and 2017.[45] Each ping represented the exact location of a single smartphone.[46] Although this information was purportedly anonymized, "it's child's play to connect real names to the dots that appear on the maps."[47] The researchers connected the dots by isolating a certain phone's identifier, which made it simple to connect the pings to the person's home and place of work.[48]

[13] With this dataset—which, while incredibly large, includes only a sliver of the location data stored by such companies—the researchers "followed military officials with security clearances as they drove home at night," "tracked local law enforcement officers as they took their kids to school," and "watched high-powered lawyers (and their guests) as they

'Anonymized'? These Scientists Can Still Identify You, N. Y. Times (July 23, 2019), https://www.nytimes.com/2019/07/23/health/data-privacy-protection.html [https://perma.cc/9FDT-FHQD], *See* Anne Toomey McKenna et al., *The Role of Satellites and Smart Devices: Data Surprises and Security, Privacy, and Regulatory Challenges*, 123 Penn St. L. Rev. 591 (2019) (discussing Strava and other satellite-based privacy concerns in more detail).

[44] Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. TIMES: THE PRIVACY PROJECT (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html [https://perma.cc/G3VA-KJ6G].

[45] *Id.*

[46] *Id.*

[47] *Id.*

[48] *Id.*

traveled from private jets to vacation properties."[49] The researchers were able to easily track individuals around the country as they went to work at sensitive government facilities, went to church, and went to protests.[50] All of this, the researchers said, was uncovered with *far less* information than these companies possess.[51] If this data fell into the wrong hands, there could be a catastrophic privacy infiltration of a magnitude never before seen. As the researchers noted, "[t]he data set is large enough that it surely points to scandal and crime [,] but our purpose wasn't to dig up dirt."[52] For hackers, it certainly would be.

III. A PRIMER ON PRODUCTS LIABILITY, PRIVACY LAW, AND STANDING

[14] In order to understand how the Restatement Third should be adapted to encompass data breaches, it is important to provide a primer on the development of products liability law and the relationship between privacy and standing.

a. Products Liability

[15] There are three main theories of recovery in products liability: warranty, negligence, and strict liability.[53] Although all three are still valid theories of recovery for plaintiffs, warranty has largely fallen out of favor

[49] Thompson & Warzel, *supra* note 44.

[50] *Id.*

[51] *Id.*

[52] *Id.*

[53] *See* RESTATEMENT (SECOND) OF TORTS § 402A cmt. b (AM. L. INST. 1965).

for personal injury and is mostly used as a replacement in those states that have not adopted strict liability.[54]

[16] Justice Cardozo's opinion in *MacPherson v. Buick*[55] was the beginning of modern products liability. Prior to *MacPherson*, a plaintiff could not recover from a manufacturer for injuries sustained as a result of a defective product without privity of contract between the two parties.[56] The court in *MacPherson* determined that manufacturers owe a duty to all when the nature of the thing they manufacture is "reasonably certain to place life and limb in peril when negligently made…."[57] *MacPherson* signaled the beginning of the end of the privity requirement, with American courts now overwhelmingly rejecting the necessity for a contractual link between the seller and purchaser in products liability cases.[58] *Macpherson* firmly established negligence as a theory of recovery in products liability, thereby extending the reach of products liability to any product that could injure a person if negligently made.[59] Although *Macpherson* signaled the end of the privity requirement for negligence claims, it was not until 1960 when the same happened for warranty claims.[60]

---

[54] Kyle Graham, *Strict Products Liability at 50: Four Histories*, 98 MARQ. L. REV. 555, 576–79 (2014).

[55] *MacPherson v. Buick Motor Co.*, 111 N.E. 1050 (N.Y. 1916).

[56] *See id.* at 1053; *see also Winterbottom v. Wright* (1842) 152 Eng. Rep. 402; 10 M. & W. 109 (holding that the plaintiff, a stagecoach driver, could not recover against the defendant, a contractor, who had agreed with the postmaster to keep the coach in repair, for injuries sustained as a result of a defective wheel on the coach, because there was no privity of contract between the driver and the contractor).

[57] *MacPherson*, 111 N.E. at 1053.

[58] *See* Anita Bernstein, *How Can a Product Be Liable?*, 45 DUKE L. REV. 1, 58 (1995).

[59] *See MacPherson*, 111 N.E. at 1053.

[60] *Henningsen v. Bloomfield Motors, Inc.*, 161 A.2d 69, 99–102 (N.J. 1960). *But cf.* Graham, *supra* note 54, at 576 (stating that the impact of the *Henningsen* decision on

[17] The development of negligence as a theory of recovery in products liability was a victory for potential plaintiffs, but the changes were not as effective as they appeared. Plaintiffs discovered that proving negligence was increasingly difficult as supply chains lengthened and products became more complex.[61] While some form of strict liability in the products liability realm had existed for some time, it was not until Justice Traynor's concurrence in *Escola v. Coca-Cola Bottling Co.*[62] that strict liability was seriously promoted across the spectrum of products liability cases.[63] While the majority relied on *res ipsa loquitur* to hold Coca-Cola liable for injuries sustained by a server as a result of a defective bottle,[64] Justice Traynor argued that a host of public policy concerns promoted the application of strict liability when a defectively manufactured product harms a user.[65] Almost twenty years later, in *Greenman v. Yuba Power Products*,[66] Justice Traynor's concurrence became law. In *Greenman*, the plaintiff was injured while using a defective shop smith manufactured by Yuba Power Products.[67] The court held that Greenman did not need to prove negligence; rather, Greenman only needed to prove that (1) he was injured while using the product as it was intended to be used, (2) he was injured as a result of the product defect, (3) the defect rendered the product unsafe for its intended

products liability is far less pronounced because of the adoption of strict liability in tort law that soon swept the nation).

[61] Graham, *supra* note 54, at 565–69.

[62] *Escola v. Coca Cola Bottling Co.*, 150 P.2d 436 (Cal. 1944).

[63] Graham, *supra* note 54, at 559–60.

[64] *Escola*, 150 P.2d at 459.

[65] *Id*. at 461.

[66] *Greenman v. Yuba Power Prods.*, 377 P.2d 897 (Cal. 1963).

[67] *Id.* at 898.

purpose, and (4) that he was not aware of the defect.[68] The court clearly stated warranty, which required a potential plaintiff to give prompt notice to the manufacturer or seller of the defect, was inadequate to protect consumers.[69] To date, only five states use warranty in lieu of strict liability.[70]

[18] Although *Greenman* formally started the push towards strict liability in tort for injuries caused by defective products, it was the promulgation of the Restatement (Second) of Torts § 402A that led to the widespread adoption of the idea.[71] Section 402A provides that:

> (1) One who sells any product in a defective condition unreasonably dangerous to the user or consumer or to his property is subject to liability for physical harm thereby caused to the ultimate user or consumer, or to his property, if
>
> > (a) the seller is engaged in the business of selling such a product, and
> >
> > (b) it is expected to and does reach the user or consumer without substantial change in the condition in which it is sold.
>
> (2) The rule stated in Subsection (1) applies although
>
> > (a) the seller has exercised all possible care in the preparation and sale of his product, and

[68] *Id.*

[69] *Id.* at 900.

[70] Graham, *supra* note 54, at 579.

[71] *Id.* at 613–14.

> (b) the user or consumer has not bought the product from or entered into any contractual relation with the seller.[72]

[19] "By 1976, forty-two states and the District of Columbia had" adopted § 402A.[73] While the adoption of § 402A was swift, so was the pushback. Products liability cases became divided into three types: manufacturing defects, design defects, and failures to warn.[74] In each group, nuances, clarifications, and exceptions developed over the years.[75] Design defects and failure to warn claims shifted toward a negligence standard (with a focus on the product rather than the actions of the manufacturer).[76] These changes ultimately led to the promulgation of the Restatement Third.[77]

[20] Section 1 of the Restatement Third states that distributors are liable for harm caused by defective products.[78] Section 2 states:

> A product is defective when, at the time of sale or distribution, it contains a manufacturing defect, is defective in design, or is defective because of inadequate instructions or warnings. A product:

[72] RESTATEMENT (SECOND) OF TORTS § 402A (AM. L. INST. 1965).

[73] Graham, *supra* note 54, at 578.

[74] *Id.* at 579.

[75] *See generally id.* at 579–80, 598, 600–01 (detailing the progression of classifications of products liability cases).

[76] *Id.* at 579.

[77] *See* RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 1 cmt. a (AM. L. INST. 1998).

[78] *Id.* § 1.

> (a) contains a manufacturing defect when the product departs from its intended design even though all possible care was exercised in the preparation and marketing of the product;
>
> (b) is defective in design when the foreseeable risks of harm posed by the product could have been reduced or avoided by the adoption of a reasonable alternative design by the seller or other distributor, or a predecessor in the commercial chain of distribution, and the omission of the alternative design renders the product not reasonably safe;
>
> (c) is defective because of inadequate instructions or warnings when the foreseeable risks of harm posed by the product could have been reduced or avoided by the provision of reasonable instructions or warnings by the seller or other distributor, or a predecessor in the commercial chain of distribution, and the omission of the instructions or warnings renders the product not reasonably safe."[79]

[21] Thus, the Restatement Third adopted negligence as the standard for design and warning defects.[80] Interestingly (and controversially), the Restatement Third usually requires the plaintiff to show a "reasonable alternative design" ("RAD") even though many courts had not required a plaintiff to make such a showing, favoring instead a broader form of the risk-utility balancing test that allowed a court to weigh the utility of the challenged design against the risk of harm posed by the design.[81] The

[79] *Id.* § 2.

[80] *Id.*

[81] *See* Matthew R. Sorenson, Comment, *A Reasonable Alternative? Should Wyoming Adopt the Restatement (Third) of Torts: Products Liability?*, 3 WYO. L. REV. 257, 280

Restatement Third remains less popular than § 402A almost 25 years after its publication.[82]

b. Standing and Privacy Law

[22] Standing to sue under privacy laws in federal court has been fraught with inconsistency and confusion.[83] Numerous theories could potentially support standing in federal court, although the Supreme Court's persistently inadequate standing decisions have failed to provide any clear guidance on how a plaintiff can establish standing to sue for injuries to privacy.[84] A full discussion on standing in privacy cases is beyond the scope of this paper, but I will briefly identify potential standing theories to show that my proposal is not dead on arrival.

[23] In federal court, a plaintiff needs to satisfy the standing requirements of Article III of the constitution.[85] The leading case on Article III standing is *Spokeo v. Robins*.[86] In *Spokeo*, the Supreme Court outlined the elements for standing: the plaintiff must have suffered an injury in fact that is fairly traceable to the challenged conduct of the defendant and that is likely to be redressed by a favorable judicial decision.[87] In privacy cases, the main issue

(2003) (discussing the use of the risk utility test versus the use of the consumer expectations test).

[82] *Id.* at 264.

[83] *See* Parker Hudson, Comment, *Risky Business: The Risk of Identity Theft and Standing to Sue*, 125 PENN ST. L. REV. 533, 535 (2021).

[84] *See id*. at 543 (discussing how circuit courts have split in interpreting standing in cases asserting an increased risk of identity theft).

[85] *Spokeo, Inc. v. Robbins*, 578 U.S. 330, 339 (2016).

[86] *See id*.

[87] *Id*. at 338.

is whether the plaintiff suffered an injury in fact.[88] The Court in *Spokeo* stated that injury in fact requires a plaintiff to show an invasion of a legally protected interest that is concrete and particularized, and actual or imminent, not conjectural or hypothetical.[89] The Court stated that when analyzing an intangible injury, such as those caused by invasions of privacy, courts should look to tradition for a historical basis for suit in English or American courts. [90] The Court also reiterated that "Congress may elevate to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law."[91] However, the Court stated that "a bare procedural violation" would not be sufficient to convey standing, even if it violated a statute.[92] Although the Court recognized that an injury must be imminent, it did not state *how* imminent an injury must be.[93]

[24] In his concurrence, Justice Thomas differentiated situations where plaintiffs allege a violation of their private rights versus when they allege a violation of a public right.[94] Justice Thomas stated that courts have traditionally found standing for the former, but not the latter.[95] Thus, Justice Thomas would find that Robins alleged an injury in fact only "[i]f Congress

[88] *Id.*

[89] *Id.* at 339.

[90] *Id.* at 340–41.

[91] *Spokeo*, 578 U.S. at 341.

[92] *Id.*

[93] *See id.* at 339.

[94] *Id.* at 343–48 (Thomas, J., concurring).

[95] *Id.* at 347.

ha[d] created a private duty owed personally to Robins to protect *his* information."[96]

[25] One theory of standing in data breach cases rests on the increased risk of identity theft.[97] In evaluating the requirements set forth in *Spokeo*, the federal circuits have been split as to whether an increased risk of identity theft may convey standing in data breach cases.[98] Another theory is that a data breach is analogous to the common law tort of breach of confidence.[99]
[26] As with the increased risk of identity theft, there is a split regarding whether the common law tort of breach of confidence may serve as the historical analog that conveys standing under *Spokeo*'s "traditional basis" test.[100]

[27] These splits exist in a world where neither Congress nor state legislatures have attempted to elevate the harm of a data breach by statute to a level sufficient to confer standing.[101] Because federal circuits have found standing to sue for data breaches without legislation under various theories, legislative action should comfortably be able to elevate data breach

[96] *Spokeo*, 578 U.S. at 349.

[97] *Id.* at 861–62.

[98] *Id.* at 860.

[99] *See Jeffries v. Volume Servs. Am., Inc.*, 928 F.3d 1059, 1064–65 (D.C. Cir. 2019) (referencing the relationship between data breach and the tort of breach of confidence).

[100] *See id.* (finding that a breach of confidence is a traditional common law tort sufficient to serve as the historical analog to convey standing); *Kamal v. J. Crew Grp., Inc.*, 918 F.3d 102, 114 (3d Cir. 2019) (indicating that an analogy to breach of confidence can support standing); *Thomas v. Toms King (OhioII), LLC*, 997 F.3d 629, 641 (6th Cir. 2021) (expressing skepticism regarding the status of the tort of breach of confidence); *Muransky v. Godiva Chocolatier, Inc.*, 979 F.3d 917, 931 (11th Cir. 2020) (examining the dispute as to whether a breach of confidence tort is a basis for a lawsuit).

[101] *See Spokeo*, 578 U.S. 341.

protections "to the status of [a] legally cognizable injur[y]" sufficient to confer standing.[102]

[28] Common law privacy torts like publicity to private life or appropriation of another's name or likeness may also suffice to establish standing so long as Congress or state legislatures articulate the language of statutes in such a way that can sustain an analogy to these torts.[103] For instance, Illinois' Biometric Information Privacy Act ("BIPA") specifically details the legislature's findings and lists the exact harms associated with the collection, storage, and safeguarding of biometric information.[104] The findings make clear that the protections sought are analogous to common law privacy torts.[105] As a result, both the Seventh and Ninth Circuits have found that a plaintiff suing under BIPA may have Article III standing.[106] Thus, the drafters of a data breach statute would be wise to specify the precise injury that plaintiffs suffer under the statute and the specific damages for a violation of the statute, ideally based on the type of information exposed in the data breach.

[29] Finally, as this proposal is not strictly limited to federal legislation, states with a more lenient standing requirement than Article III need not be concerned about Article III standing in state court. In fact, a state may craft

[102] *Id.*

[103] Devin Urness, Note, *The Standing of Article III Standing for Data Breach Litigants: Proposing a Judicial and a Legislative Solution*, 73 VAND. L. REV. 1517, 1555–59 (2020).

[104] 740 ILL. COMP. STAT. ANN. 14/5 (2022).

[105] *See id.*

[106] *See Patel v. Facebook, Inc.*, 932 F.3d 1264, 1270–71 (9th Cir. 2019); *Bryant v. Compass Grp. USA, Inc.*, 958 F.3d 617, 619 (7th Cir. 2020).

a statute to intentionally fail the Article III analysis to keep its data-breach cases in state court.[107]

IV. ADAPTING THE RESTATEMENT THIRD TO APPLY TO DATA BREACHES

[30] All fifty states and the District of Columbia have data breach notification laws that, in some form or another, require an entity that suffers a data breach to notify the state or consumers.[108] My proposal, however, does not concern notification, but concerns the steps an entity must take to secure collected data.

a. Why Products Liability?

[31] First, Data is a product.[109] It is important to note that the product being discussed here is the data itself—not the data security system. That being said, the data product becomes "not reasonably safe" when it is left unprotected. Such protection necessarily invokes data collection and security procedures.[110] In this sense, we can think of the data security system as the mechanism through which the collector ensures that the product is reasonably safe.

---

[107] *See Kislov v. American Airlines, Inc.*, No. 17 C 9080, 2022 U.S. Dist. LEXIS 50841, at *4 (N.D. Ill. 2022).

[108] Taryn Elliot, Comment, *Standing a Chance: Does Spokeo Preclude Claims Alleging the Violation of Certain State Data Breach Laws?*, 49 SETON HALL L. REV. 233, 242 (2018).

[109] *See Big Data & Business Analytics Market To Reach USD 684.12 Billion By 2030, Growing At A CAGR of 13.5% - Valuates Reports*, CISION PR NEWSWIRE (Oct. 29, 2021, 10:00 AM), https://www.prnewswire.com/news-releases/big-data--business-analytics-market-to-reach-usd-684-12-billion-by-2030--growing-at-a-cagr-of-13-5----valuates-reports-301411846.html [https://perma.cc/2QLZ-9ZPC] [hereinafter *Big Data*].

[110] 740 ILL COMP. STAT. ANN. 14/5 (2022).

[32] Although the Restatement Third defines a product as "tangible personal property," it also states that "[o]ther items, such as real property and electricity," may be products when they are distributed and used analogously to physical products.[111] Data products fit in with these "other items." Data products are collected, packaged, stored, used, and sold by companies at commercial scale. In fact, data is now a $200 billion per year industry.[112]

[33] The reason data products do not seem like an exact match with products liability is simply because the supply chain for data products is different than that of traditional products. The main difference between the data supply chain and the traditional supply chain is that, for data products, the potential for harm becomes decoupled from the data product, meaning that the potential for harm remains with the consumer even though the data product is in the hands of the manufacturer. However, this difference does not warrant disparate treatment because the chief concern of products liability law is the same for traditional and data products: products liability is intended to prevent harm to consumers caused by a defective product when another entity is best positioned to prevent that harm.[113]

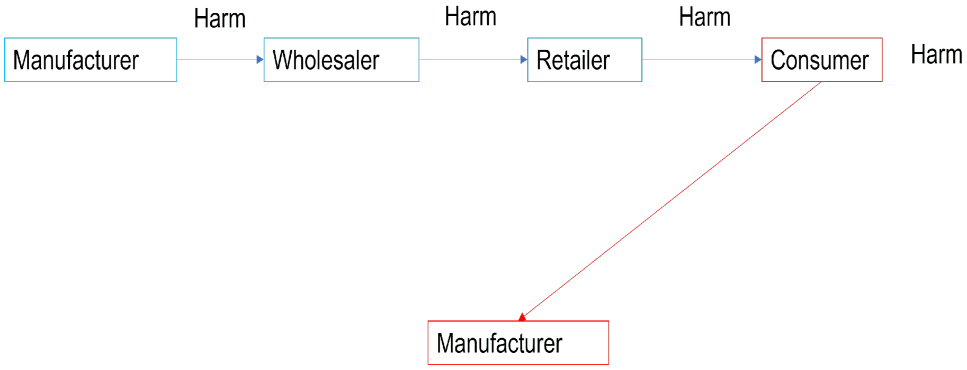
[34] Unlike the traditional supply chain contemplated by the Second and Third Restatements, the supply chain for data products keeps the potential for harm with the original consumer. Below is a traditional supply chain that has been the basis of products liability since its promulgation.

[111] RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 19(a) (AM. L. INST. 1998).

[112] *See Big Data*, *supra* note 109.

[113] RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 2 cmt. a (AM. L. INST. 1998).

[35] The traditional product begins with the manufacturer, who may sell it to a wholesaler, who might then sell it to a retailer from whom the consumer buys the product. Importantly, the traditional product carries with it the potential for harm, so the potential for harm follows the same path. Therefore, the product and the harm are coupled together. However, this chain does not tell the full story when it comes to data products. The way companies usually collect consumer data is by way of a traditional product (or, alternatively, a service[114]), which creates a new product and extends the supply chain. This point is illustrated below.



[36] The original consumer acts as a both the endpoint for the first chain (the "traditional supply chain") and the beginning of the second chain (the "data supply chain"). In the traditional supply chain, the potential harm is always tied to the traditional product. However, in the data supply chain, potential harm and the data product have been decoupled. The risk of harm never moves from the consumer in the data supply chain because the harm is inextricably tied to the consumer due to the personal nature of the data collected.[115]

[114] *See supra* Section III.b.

[115] *See generally* RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 2 cmt. a (AM. L. INST. 1998) (explaining that the data product does not pose a risk to the collector even though the collector uses, holds, and (hopefully) protects it; meanwhile the consumer bears the

[37] To offer an example of how this operates, we can look at a chain involving a Samsung Galaxy. The physical device might travel from Samsung's factory to a Best Buy where it is sold to the consumer. In traditional products liability cases, this is where the chain ends. The harm (the risk of the lithium battery exploding, for example) travels with the phone through the entirety of the traditional supply chain. However, in a data supply chain, this is merely the beginning.

[38] Once the phone is in the hands of the consumer, the data product is developed. Samsung begins collecting, using, and potentially selling[116] the consumer's personal data.[117] However, the harm remains with the user of the phone. If Samsung's database were to be breached and the user's geolocation data, bank account information, signature, browsing history, address, and more[118] were stolen, the user of the phone suffers the harm—not Samsung. Just as the manufacturer's actions in the traditional supply chain determine the safety of the traditional product for the consumer, the collector's actions in the data supply chain determine the safety of the data product for the consumer.

[39] Why then, should these types of products be treated differently? The answer is that they should not. The supply chain distinction yields no legally salient difference. Legislatures should recognize that products liability law

risk of having her personal information exposed to the world, which can lead to a myriad of different injuries).

[116] JR Raphael, *Galaxy users, take note: Samsung's probably selling your data*, COMPUTERWORLD (Jan. 22, 2020, 1:00 AM), https://www.computerworld.com/article/3514999/samsung-selling-data.html [https://perma.cc/L4GE-PH4D].

[117] SAMSUNG PRIVACY, https://privacy.samsung.com/policy/overview [https://perma.cc/C4UH-YP4H] (last visited Sept. 17, 2022).

[118] *See* Raphael, *supra* note 116.

needs to be updated for the 21st century and they should apply products liability principles to data products and breaches accordingly.

[40] The societal and economic issues presented by data breaches are also similar to the social and economic issues that led to the creation of products liability. Products liability emerged in tandem with, and because of, increased class consciousness regarding physical safety and living conditions and a fundamental change in the structure of the American economy.[119] The newfound skepticism of consumer goods was largely based on the same reasons for courts rejecting the privity requirement in products liability cases: "mass production, the introduction of middlemen and retailers into the supply chain, enhanced advertising and promotion, and expanded retail showplaces."[120]

[41] Beginning in the early 1900s, consumers sought information about product safety ranging from household appliances to food.[121] This led to congressional interest in product regulation and resulted in Congress regulating industries such as the cigarette, automobile, and children's clothing industries.[122] Moreover, a tsunami of health and safety issues was caused by commercial products in the 1940s and 1950s.[123] This combination of economic change, congressional interest, and societal support set the stage for the adoption of strict products liability and §402A and product regulation.[124]

[119] *See* Graham, *supra* note 54, at 585.

[120] *Id.*

[121] *Id*. at 585–86.

[122] *See id*. at 587–89 (listing Congressional responses for purposes of regulating these industries).

[123] *See id*. at 587–90.

[124] *See generally* Graham, *supra* note 54 at 589–92 (establishing the societal and legal interest in creating product liability tort claims).

[42] Likewise, data collection has created an entirely new industry built using consumer data as its foundation.[125] Big Data is almost a $200 billion per year industry and largely did not exist a few decades ago.[126] For reference, the U.S. market for Big Data is estimated at around $50 billion per year and growing quickly,[127] whereas the automotive manufacturing industry in the U.S. is estimated at about $86 billion per year.[128] Big Data's revenue is generated from an entirely new type of supply chain, much like the expanded supply chain seen in the industrial revolution that led to the promulgation of modern products liability law.

[43] There has also been a phenomenal push by state legislatures to pass data privacy legislation.[129] Consumer privacy legislation is currently pending in twenty-two states.[130] A majority of states have also enacted or

[125] *See Big Data*, *supra* note 109.

[126] *See id*.

[127] *See Global Big Data Market to Reach $234.6 Billion by 2026*, CISION PR NEWSWIRE (June 29, 2021,11:58 AM), https://www.prnewswire.com/news-releases/global-big-data-market-to-reach-234-6-billion-by-2026--301322252.html [https://perma.cc/LRY2-LZ82] (noting that the Big Data industry is projected to eventually surpass this $200 billion per year grossing mark).

[128] *Automotive Software Market Is Expected to Grasp the Value of USD 86,283.47 Million by 2029: Industry Share, Size, Industry Analysis, Key Growth Drivers, Trends and Segments*, GlobeNewswire (Sept. 7, 2022), https://www.globenewswire.com/news-release/2022/09/07/2511938/0/en/Automotive-Software-Market-Is-Expected-to-Grasp-the-Value-of-USD-86-283-47-Million-by-2029-Industry-Share-Size-Industry-Analysis-Key-Growth-Drivers-Trends-and-Segments.html [hereinafter ASM] [https://perma.cc/3TRV-RVXN].

[129] *See* David Stauss, *State data privacy legislation: Takeaways from 2022 and what to expect in 2023*, IIAP (Aug. 23, 2022), https://iapp.org/news/a/state-data-privacy-legislation-takeaways-from-2022-and-what-to-expect-in-2023/# [https://perma.cc/D3UR-LFFF].

[130] Deborah George, *At Least 22 States Have Consumer Privacy Legislation Pending – Will 2022 Be the Year for More State Privacy Laws*?, NAT'L L. REV. (Feb. 24 2022),

are currently considering biometric privacy legislation.[131] At the federal level, Senator Kirsten Gillibrand has introduced legislation to create an entire agency dedicated to data privacy.[132] While not active legislation, Texas has filed a lawsuit under its biometric privacy law against Facebook for its "Tag Suggestions" feature alleging upwards of $25 trillion in damages.[133] It is clear that the state and federal governments are actively interested in consumer data privacy.

[44] Americans are increasingly uneasy regarding the proliferation of data collection. Over half of Americans support regulating even some of the more mundane uses of personal data, such as "mak[ing] it illegal for social media companies to use personal data to recommend content via algorithms."[134] Moreover, 81% of U.S. adults believe they lack control over their personal data and that the risks of data collection by companies outweigh the benefits, 79% are concerned about how their data is used, and 59% don't understand what their data is used for. [135]

---

https://www.natlawreview.com/article/least-22-states-have-consumer-privacy-legislation-pending-will-2022-be-year-more#google_vignette [https://perma.cc/PF7U-MU6F].

[131] BRYAN CAVE LEIGHTON PAISNER LLP, U.S. BIOMETRIC LAWS & PENDING LEGISLATION TRACKER, https://www.bclplaw.com/a/web/320807/BIPA-Tracker-II-603732145.3.pdf [https://perma.cc/2UDV-7SCQ].

[132] Sara Morrison, *Sen. Kirsten Gillibrand wants to create a new agency to deal with data privacy*, VOX (June 17, 2021, 6:00 AM), https://www.vox.com/recode/2021/6/17/22536907/gillibrand-data-protection-act-privacy [https://perma.cc/Z66A-4NRL].

[133] *See* Complaint, *State v. Meta Platforms, Inc.*, No. 22-0121 (Tex. 71st Jud. Dis. Ct. Feb. 14, 2022).

[134] C. Blair Robinson, *New Poll Underscores Growing Support for National Data Privacy Legislation*, JD SUPRA (Jan. 28, 2022), https://www.jdsupra.com/legalnews/new-poll-underscores-growing-support-8066824/ [https://perma.cc/2LZC-LR7V].

[135] Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019),

[45] Adapting products liability law to apply to data privacy regulation would also allow Congress and state legislatures to utilize the wealth of knowledge developed in products liability over the last century to inform liability for data breaches. Courts and the Restatement Third have developed detailed exceptions and tests attempting to strike a delicate balance between the interests of consumers and manufacturers, including those regarding risk-utility balancing factors, unreasonably dangerous designs, and reasonable alternative designs. Moreover, the widespread adoption and acceptance of products liability law shows that courts and legislatures believe that industry cannot be trusted to act as its own regulator. Additionally, courts, consumers, and companies are familiar with products liability and its concepts. Rather than having society learn and implement new concepts, it would be efficient to simply apply existing products liability concepts to data privacy regulation. It would be unnecessarily burdensome to start from scratch when there is an existing template that has proven to be effective.

[46] Finally, the same policy rationales are implicated because the original manufacturer's actions control the safety of the consumer's data. The Restatement Third's rationales apply to data products because, like a manufacturer in the traditional supply chain, the collector would be incentivized to safeguard the data, invest in safety protocols, and take affirmative steps to safeguard consumer data. As such, the collector is best positioned to spread the costs of defective products and is in the best position to prevent the injury altogether.[136] The risk-utility balancing test in products liability[137] would also benefit both industry and society at large

https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ [https://perma.cc/474Y-8EHN].

[136] *See* RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 2 cmt. a (AM. L. INST. 1998).

[137] *See id.* § 2 cmt. d; Keith N. Hylton, *The Law and Economics of Products Liability*, 88 NOTRE DAME L. REV. 2457, 2494–95 (2013) (stating that the risk-utility test encourages welfare-enhancing product innovation); Benjamin R. Sachs, Note, *Consumerism and*

because it would enable innovation, which has benefits for society, while minimizing harm to those whom data collection has negatively affected or will negatively harm in the future. Additionally, the risks of data breaches and the harms flowing therefrom are foreseeable to those collecting data. Accordingly, data collectors should be tasked with protecting against those harms. Finally, consumers often share information with the expectation that it will not be shared—intentionally or unintentionally—with others.[138] Thus, courts should recognize that there is an expectation that this shared data will be protected and impose liability on those who fail to do so.

[47] Given the similarities between data breaches and products liability, legislators should review products liability law to help solve the problems posed by data breaches.

Information Privacy: How Upton Sinclair Can Again Save Us from Ourselves, 95 VA. L. REV. 205, 242 (2009) (discussing how the risk-utility balancing test should be used to address data breaches because most probably stem from weaknesses in the design of a security system rather than a fluke defect).

[138] *Your Data Is Shared and Sold…What's Being Done About It?*, KNOWLEDGE AT WHARTON (Oct. 28, 2019), https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/ [https://perma.cc/SZ9V-QA5L] (stating that "Up to 73% of American adults incorrectly believe that the existence of a privacy policy means a website cannot share their data with other parties without their permission[.]"); *see also How Much Privacy Do You Have Online?*, UNIV. DAYTON (Jan. 17, 2019), https://onlinelaw.udayton.edu/resources/how-much-privacy-do-you-have-online/ [https://perma.cc/R736-TQA7] ("We expect that when we post pictures or about activities we did that day, it's only for our friends and family to see, but that's not really true[.]").

b. Why the Restatement Third and not the Restatement Second?

[48] While § 402A is more popular[139] and adopts strict liability for manufacturing, design, and warning defects,[140] the Restatement Third offers the better option as applied to data breaches because it adopts strict liability for manufacturing defects and negligence for design and warning defects.[141]

[49] The negligence standard for design and warning defects is simply more palatable for legislatures and consumers to adopt because strict liability has the potential to put a severe dent in a $200 billion per year industry that provides modern benefits Americans have grown to love and depend on, whereas a negligence standard would be slightly more favorable to the industry than strict liability and strike an appropriate balance.[142] To be sure, there is great bipartisan support for a data privacy law. Around 90% of both democrats and republicans support data privacy regulation.[143] Such legislation has been proposed at the federal level as well. Last year, a bipartisan group of senators, including Senators Klobuchar (D), Kennedy (R), Manchin (D), and Burr (R) proposed a federal privacy statute that,

[139] *See* Sorenson, *supra* note 81, at 264.

[140] *See* RESTATEMENT (SECOND) OF TORTS § 402A (AM. L. INST. 1965).

[141] *See* RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 2 cmt. a (AM. L. INST. 1998); *see also* Alan Butler, *Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices?*, 50 U. MICH. J. L. REFORM 913, 918 (2017) ("[T]he problem of insecure devices and networks is precisely the kind of issue that strict products liability was designed to solve.").

[142] *Big Data*, *supra* note 10.9

[143] *New Data Reveals Americans' Overwhelming and Bipartisan Support for Federal Privacy Legislation*, PRIV. FOR AM. (Nov. 18, 2021), https://www.privacyforamerica.com/new-data-reveals-americans-overwhelming-and-bipartisan-support-for-federal-privacy-legislation/ [https://perma.cc/JF4W-UDX4] [hereinafter *Bipartisan Support*].

among other things, would have required companies to have a data privacy program in place.[144] But while there is great support for data privacy legislation, it is important to note that many people are driven by a desire for personal protection against abuse and misuse of their information rather than a desire to punish companies.[145] Congress had concerns that Klobuchar's bill would have too great an impact on industry, signaling that ambitious proposals like strict liability for data breaches may not be realistic.[146] Thus, legislatures may favor a negligence-based law that is less punitive than strict liability in order to balance consumer concerns of protection with economic concerns raised by potentially hampering an entire industry.

1. Design Defects

[50] Negligence should be the preferred standard for evaluating design defects because there is no data security design that is 100% secure and holding companies liable under a strict liability regime would be unreasonable.[147] After all, as former director of the FBI Robert Mueller once

[144] *Klobuchar, Kennedy, Manchin, Burr Introduce Bipartisan Legislation to Protect Privacy of Consumer's Online Data*, SENATE: AMY KLOBUCHAR (May 20, 2021), https://www.klobuchar.senate.gov/public/index.cfm/2021/5/klobuchar-kennedy-manchin-burr-introduce-bipartisan-legislation-to-protect-privacy-of-consumers-online-data [https://perma.cc/L3KY-N63M].

[145] *Bipartisan Support*, *supra* note 143.

[146] Adam Kovacevich, *A guessing game: How Sen. Klobuchar's tech bill will impact consumers*, ROLL CALL (Feb. 11, 2022, 4:30 PM), https://rollcall.com/2022/02/11/a-guessing-game-how-sen-klobuchars-tech-bill-will-impact-consumers/ [https://perma.cc/3M4V-UAQZ].

[147] *See generally* Davey Winder, *U.S. Government Says It's Building A 'Virtually Unhackable' Quantum Internet*, FORBES (July 25, 2020, 5:59 AM), https://www.forbes.com/sites/daveywinder/2020/07/25/us-government-to-build-virtually-unhackable-quantum-internet-within-10-years/?sh=660b49472b70 [https://perma.cc/FM7K-TNLL] (demonstrating the potential for secure data in the future through the Quantum Internet).

said, "[t]here are only two types of companies: [t]hose that have been hacked and those that will be hacked."[148] The collector, then, has little incentive to spend time and money on security research when a breach is simply a matter of time rather than an entirely preventable occurrence. The entire industry could be destroyed by exorbitant penalties if collectors were held strictly liable for data breaches.[149]

[51] Additionally, a negligence standard strikes the appropriate balance between competing interests because it allows the industry to continue operating and innovating, strongly incentivizes collectors to do everything in their power to avoid breaches and provides consumers with recourse if collectors ignore their duty to protect the information properly. It would not be unduly burdensome for plaintiffs to prove a breach of this duty either. A collector's security system and data security protocols should be easily discoverable through requests for production, interrogatories, and depositions. Moreover, once a breach occurs, the company is on notice that its security system has failed. Thus, a failure to inquire into the cause of the breach would constitute a strong showing of negligence for later breaches. The company itself should determine the cause of the breach so the plaintiff does not have to. Once the fault has been established, plaintiffs will know exactly where to look. There is also a litany of data security experts available to analyze a company's practices once all of the facts have been discovered.[150]

---

[148] *E.g.*, Stephen Barnes, *There are two types of companies: Those who know they've been hacked & those who don't*, DYNAMIC BUS. (Mar. 29, 2018), https://dynamicbusiness.com/topics/technology/there-are-two-types-of-companies-those-who-know-theyve-been-hacked-those-who-dont.html [https://perma.cc/BYR3-66AA].

[149] Furthermore, data security systems are working against people actively trying to undermine and bypass the security system. Requiring data security systems to outpace hackers 100% of the time would be impractical.

[150] *See* Scott Schober, *Top 30 Cybersecurity Experts You Should Follow In 2022*, CYBERSECURITY VENTURES (Dec. 8, 2021), https://cybersecurityventures.com/top-30-cybersecurity-experts-you-should-follow-in-2021/ [https://perma.cc/6RV2-6VYT].

[52] Furthermore, legislatures should allow plaintiffs suing under this law to bring a class action, which would greatly enhance the resources plaintiffs can employ to investigate a collector's data security practices. Class actions may even be preferred by defendants in these suits because it could be easier to defend one claim rather than tens of thousands of individual ones.[151] Finally, legislatures should also consider cost shifting provisions, such as allowing plaintiffs to recover attorney's fees and investigative costs, to mitigate the burden on plaintiffs imposed by negligence rather than strict liability. For particularly egregious displays of carelessness on the part of collectors, like Equifax,[152] the statute should permit punitive damages to deter reckless behavior.

[53] Taken together, the company's duty to find the cause of the breach, the discoverability of data security protocols and code, the availability of experts in the data security field, and the potential for class actions and cost shifting make negligence a manageable burden for plaintiffs to carry while still protecting the interests of the defendant company.

2. Warning Defects

[54] Negligence is also the appropriate standard for data breach warnings because there is no universal warning that is perfect for every consumer.[153] This is especially true when collectors need to convey copious amounts of information about their data privacy policy in a way that is concise and impresses upon the mind of a reasonable user the potential for harm. Even

[151] Andrew Faisman, Note, *The Goals of Class Actions*, 121 COLUM. L. REV. 2157, 2173 (2021).

[152] Barrett, *supra* note 26.

[153] *See* RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 2 cmt. i (AM. L. INST. 1998) (noting that it is impossible to identify the perfect level of detail that should be communicated in product disclosures as different users may benefit from different types of warnings).

a slightly insufficient warning containing some of the information outlined below[154], including *inter alia*, what information is collected and who the information is shared with, would be a dramatic step forward from the lack of transparency consumers currently face. Moreover, the negligence standard for failure to warn would pose few difficulties for plaintiffs because the warnings will be readily apparent. Then, the question is simply what kind of warning would be reasonable under those circumstances and whether the collector acted reasonably in selling the product with those warnings. Thus, the difficulty arises in establishing what the exact duty is (a legal question) rather than proving breach (a factual question).[155] Strict liability and negligence are substantially the same in this respect.

c. Who Would be Liable for the Data Breach?

[55] The collector, as the manufacturer of the data product, would be the main entity held liable. Individuals shed collectible data at all times: our location, heart rate, calorie intake, sexual orientations, religious beliefs, and more are potential data points.[156] However, this data is not a product until someone collects it for use or distribution. Thus, because the collector turns the stray data into a product, it should be held liable for a data breach.

[56] The Restatement Third, much like Comment f of § 402A, imposes liability on all sellers in the supply chain prior to the product reaching the consumer.[157] In the traditional supply chain, this means all sellers upstream of the consumer (i.e., the retailer, the wholesaler, and the manufacturer).

---

[154] *See infra* Section IV(f).

[155] *See Carl v. City of Overland Park,* 65 F.3d 866, 869 (10th Cir. 1995).

[156] Louise Matsakis, *The WIRED Guide to Your Personal Data (and Who Is Using It)*, WIRED (Feb. 15, 2019, 7:00 AM), https://www.wired.com/story/wired-guide-personal-data-collection/ [https://perma.cc/D8UH-ZF4E].

[157] *See* RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 2 cmt. o (AM. L. INST. 1998); RESTATEMENT (SECOND) OF TORTS § 402A cmt. f (AM. L. INST. 1965).

The same principle would apply in data breach cases, except those downstream of the consumer would be liable, including the collector and those to whom the collector distributes the data product. There are three reasons for this slight modification: the data benefits those downstream, not upstream, of the consumer;[158] the harm remains with the consumer in the data supply chain and does not move downstream with the data product; and those downstream of the consumer are in the best position to protect the data.[159] This modification also incentivizes collectors to deal with other reputable data collectors that have proper data security measures in place.

[57] Those downstream of the consumer are to be held liable even though the Restatement Third states that the defect must exist "at the time of sale or distribution."[160] This requirement is best understood as a consequence of the traditional supply chain. In the traditional supply chain, manufacturers have no control of the product once it leaves their possession. This is simply not true for data products: the collector possesses the data product and, thus, the collector's protection (or lack thereof) of the product will dictate whether harm befalls the consumer. In fact, it is only *after* the product is sold or distributed that the risk of harm arises. As a result of the decoupling of the harm and the product in the modern supply chain, the requirement that the defect exist at the time of sale or distribution is obsolete when dealing with data products.

---

[158] *See* Julia N. Mehlman, Note, *If You Give a Mouse a Cookie, It's Going to Ask for your Personally Identifiable Information: A Look At The Data-Collection Industry And A Proposal For Recognizing The Value Of Consumer Information*, 81 BROOK. L. REV. 329, 342–47 (2015).

[159] This is not to say that retailers and wholesalers cannot be liable if they do, in fact, receive the consumer's data downstream. Instead, this simply means that one is not necessarily liable for the misuse of a consumer's data simply by being upstream of the consumer.

[160] RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 2 (AM. L. INST. 1998).

[58] It is also worth noting that this timing issue is not limited to data products. With the widespread proliferation of Internet-of-Things (IoT) devices,[161] manufacturers maintain a phenomenal amount of control over traditional products after their sale. Since these devices are connected to the internet, they can be updated after sale.[162] A software update could be pushed out to an IoT device that renders it defective.[163] For instance, an update to a smart oven (yes, even ovens connect to the internet now[164]) pushed out by the manufacturer could cause it to overheat or fail to turn off, resulting in injury. Modern technology is changing even traditional supply chains, so the "time of sale" limitation should not be recognized when the main purposes of products liability would still be served.

[161] *See* Steve Ranger, *What is the IoT? Everything you need to know about the Internet of Things right now*, ZDNET (Feb. 3, 2020), https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/ [https://perma.cc/2Q7Q-5A4N] (defining an IoT device to be any device that can be connected to the internet, such as a car, child's toy, wearable, and other "smart" devices).

[162] *See* Erica Mixon & Colin Steele, *OTA update (over-the-air update)*, TECHTARGET (Oct. 2020), https://www.techtarget.com/searchmobilecomputing/definition/OTA-update-over-the-air-update [https://perma.cc/4BQ5-NFSM].

[163] *See* Graham Cluley, *No over-the-air update means GM has to recall four million cars to fix fatal software defect*, BITDEFENDER (Sept. 13, 2016), https://www.bitdefender.com/blog/hotforsecurity/no-over-the-air-update-means-gm-has-to-recall-four-million-cars-to-fix-fatal-software-defect [https://perma.cc/49Z3-LX87].

[164] *See Bosch ovens (Home Connect)*, BOSCH, https://bosch-iot-suite.com/iot-devices/bosch-ovens/ [https://perma.cc/62D3-PRFX].

d. Design Defects and Data Breaches

[59] The Restatement Third adopts a negligence standard for proving design defects.[165] The Restatement Third provides that:

> A product is defective when, at the time of sale or distribution, it contains a manufacturing defect, is defective in design, or is defective because of inadequate instructions or warnings. A product:
> .
> .
> (b) is defective in design when the foreseeable risks of harm posed by the product could have been reduced or avoided by the adoption of a reasonable alternative design by the seller or other distributor, or a predecessor in the commercial chain of distribution, and the omission of the alternative design renders the product not reasonably safe.[166]

[60] To begin, as applied to data breaches, the language "by the seller or other distributor, or a predecessor in the commercial chain of distribution" would need to be altered to encompass those downstream of the consumer in the data supply chain for reasons discussed *supra*. [167]

[61] The Restatement Third expands on the risk-utility balancing test, defining it as "whether a reasonable alternative design would, at reasonable cost, have reduced the foreseeable risks of harm posed by the product and, if so, whether the omission of the alternative design by the seller or a predecessor in the distributive chain rendered the product not reasonably

[165] *See* RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 2(b) (AM. L. INST. 1998).

[166] *Id.*

[167] *Id.* § 2 cmt. d.

safe."[168] It further clarifies that the idea that "a product is defective in design if the foreseeable risks of harm could have been reduced by a reasonable alternative design is based on the commonsense notion that liability for harm caused by product designs should attach only when harm is reasonably preventable."[169]

[62] The Restatement Third provides factors to be considered in determining whether a RAD renders a product not reasonably safe, including: "the magnitude and probability of the foreseeable risks of harm," "warnings accompanying the product," "the nature and strength of consumer expectations regarding the product," and "advantages and disadvantages of the product as designed and as it alternatively could have been designed," such as "costs," "longevity, maintenance, [and] repair."[170] Importantly, Comment f notes that these factors interact with one another.[171]

[63] These factors apply to data breaches as well. In evaluating the magnitude and foreseeable risks of harm regarding data breaches, courts should consider several factors, including the type of information collected and stored, the potential for harm to the consumer, the risk of breach, the utility of the information for the collector and others using it, and the benefits the consumer receives from the collector and others storing the consumer's information.[172] In considering the magnitude of potential harm,

[168] *Id.*

[169] *Id.* § 2 cmt. f.

[170] RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 2 cmt. f (AM. L. INST. 1998).

[171] *Id.*

[172] *See, e.g.*, *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1308–1310 (N.D. Ga. 2019) (finding that the data breach was so severe because the type of information obtained by hackers involved personal and financial data which could be used to create fake identities and destroy a consumer's credit-worthiness; also emphasizing the fact that Equifax had experienced previous data breaches but failed to mitigate the risk of future breaches).

the main consideration should be the type of information that is collected. For instance, biometric information, which is incredibly sensitive and cannot be changed,[173] should receive the utmost security, whereas information like email addresses is not as sensitive and may require a less sophisticated security system. In evaluating the foreseeable risks of harm, courts should deeply consider the fact that no data security systems are impenetrable. As such, data breaches are very foreseeable and should be treated as such. Courts should also recognize that consumers expect their information to be kept private, even though the average consumer is aware of the possibility of a data breach.[174] To hold otherwise would absolve companies of protecting the data at all. The relevant advantages and disadvantages of the data security system will require a case specific analysis involving the costs of security and type of information stored.

[64] Additionally, the Restatement Third provides that state of the art is a defense and industry practice can be argued by both the plaintiff and the defendant.[175] State of the art would certainly be a powerful defense in data breach cases. Companies that employ the best software available at the highest price point they can afford could claim state of the art. However, plaintiffs also have a powerful rebuttal: if this really is the best system available, then how did a group of hackers find their way in? Based on the fact specific nature of this inquiry, collectors may be more willing to settle rather than risk a battle of the experts at trial, giving plaintiffs an advantage during negotiations. Regarding industry practice, it is not dispositive that an industry uses a certain data security system. The system employed, and thus the entire industry, can lag behind acceptable data security practices.[176]

[173] *See* 740 ILL. COMP. STAT. ANN. 14/5(c) (2022).

[174] *See* Auxier et al., *supra* note 135.

[175] RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 2 cmt. d (AM. L. INST. 1998).

[176] *See generally Pearce v. Feinstein*, 754 F. Supp. 308, 311–12 (W.D.N.Y. 1990) (finding that a hospital's liability in using defective medical equipment met a simple

Thus, this defense will likely be weak as the merits of the security system itself would still be attacked.

[65] The Restatement Third also dictates that whether a harm is open and obvious may be relevant but is not dispositive.[177] This defense will seldom, if ever, be relevant in data breach cases. The open and obvious theory is founded on the premise that consumers know, or should know, to take certain precautions when the risk posed by the product is inherent and clear.[178] This is of little relevance in data breach cases because the harm and the product are decoupled, meaning that only the collector can prevent harm to the consumer once the data is collected. Thus, whether the consumer knows of some abstract risk of potential harm is of little relevance in evaluating the data security system used by the collector because the consumer's actions will not dictate the safety of the data product.[179]

negligence standard instead of medical malpractice and therefore did not require expert testimony).

[177] *Id.*

[178] James P. End, *The Open and Obvious Danger Doctrine: Where Does it Belong in Our Comparative Negligence Regime?*, 84 MARQ. L. REV. 445, 445–47 (2000) (discussing the premise of the open and obvious theory as it relates to consumers assuming risk when using a product).

[179] Moreover, without an exhaustive list of all relevant data that is collected and the parties that data is being disclosed to, the actual risk of a data breach cannot be open and obvious to a consumer since she would have no way of calculating the risk. For instance, a consumer may agree to share her email address with the manufacturer of her smart watch, but not her health information gathered through the watch; or, she may be comfortable sharing her health information with the manufacturer, but not with thirty other collectors because having the information in additional databases could increase the chances the information would be disclosed in a data breach.

[66] Finally, while § 2(b) of the Restatement Third is the primary means of proving design defect, it may also be proven by alternative means, as discussed below.[180]

e. Warning Defects and Data Breaches

[67] The Restatement Third adopts a negligence standard for warning defects.[181] The Restatement Third provides that:

> A product is defective when, at the time of sale or distribution, it contains a manufacturing defect, is defective in design, or is defective because of inadequate instructions or warnings. A product:
> .
> .
> (c) is defective because of inadequate instructions or warnings when the foreseeable risks of harm posed by the product could have been reduced or avoided by the provision of reasonable instructions or warnings by the seller or other distributor, or a predecessor in the commercial chain of distribution, and the omission of the instructions or warnings renders the product not reasonably safe.[182]

[68] The Restatement Third also states that "[w]arnings alert users and consumers to the existence and nature of product risks so that they can prevent harm either by appropriate conduct during use or consumption or by choosing not to consume."[183] It also notes how it adopts a reasonableness

[180] *See infra* Sections IV.h.

[181] RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 2(c) (AM. L. INST. 1998).

[182] *Id.*

[183] *Id.* § 2 cmt. i.

test because it is not possible to achieve "a perfect level of detail that should be communicated in product disclosures."[184] Importantly, Comment i states that:

> [W]arnings also may be needed to inform users and consumers of nonobvious and not generally known risks that unavoidably inhere in using or consuming the product. Such warnings allow the user or consumer to avoid the risk warned against by making an informed decision not to purchase or use the product at all and hence not to encounter the risk. In this context, warnings must be provided for inherent risks that reasonably foreseeable product users and consumers would reasonably deem material or significant in deciding whether to use or consume the product. Whether or not many persons would, when warned, nonetheless decide to use or consume the product, warnings are required to protect the interests of those reasonably foreseeable users or consumers who would, based on their own reasonable assessments of the risks and benefits, decline product use or consumption. When such warnings are necessary, their omission renders the product not reasonably safe at time of sale.[185]

[69] First, collectors must provide the proper content in the warning. As applied to data breaches, legislatures should require a warning to inform consumers of the type(s) of information being collected, how many entities that data will be shared with, and the purposes for which that data may be used. Because many types of data can be collected and stored, a collector should specifically warn that it collects data that could reasonably cause a consumer to reject the product, including private, personal, and identifying information (even if it is later de-identified). Legislatures are best suited to

[184] *Id.*

[185] *Id.*

determine what types of information could reasonably cause a consumer to reject a product. Requiring collectors to disclose what information is being collected serves another very important purpose: collectors will be forced to make their data collection practices public, thereby encouraging collectors to engage in less risky data collection practices. Furthermore, because common consumers are unlikely to understand the ramifications of the data collection, the warning should also include the potential ramifications of a data breach, such as identity theft and the publication of personal information (if applicable).

[70] The number of entities the data is shared with is pertinent because the chances that a consumer's information could be involved in a data breach increase as the information is stored in more databases. A consumer cannot make a fully informed decision on whether to encounter the risk without knowing the full extent of the risk. Additionally, consumers may be more or less willing to share data for certain reasons and this can affect the risk-utility analysis performed by the consumer. For instance, an owner of a "self-driving" car may be willing to share her location and camera information with the collector (in this case, the original manufacturer) for performance purposes to reap the benefits of an enhanced "self-driving" experience, but the consumer may not wish to share the same information with third parties for advertising purposes. Also, unlike traditional products, a consumer's risk calculus can change based on subsequent actions taken by the collector, such as a change to the entity's privacy policy. Thus, the duty to warn constitutes a continuing duty whereby the collector must alert the consumer to any changes in its initial warning. The collector who initially collects the data should be held responsible for informing the consumer of the disclosure and use policies of those to whom the collector discloses the data. This ensures that other downstream collectors cannot escape the requirements imposed by this proposal.

[71] A collector would not be required to warn of open and obvious risks for the same reasons discussed under design defects.[186] Additionally, the risk would not be "open and obvious" without a full disclosure of the controller's data practices—which necessarily implicates the warning.

[72] Second, warnings must be properly structured. One of the most crucial factors in determining the adequacy of a warning is the way in which it is presented. The warning "must be in such form that it could reasonably be expected to catch the attention of the reasonably prudent man in the circumstances of its use."[187] "No easy guideline exists for courts to adopt in assessing the adequacy of product warnings and instructions. In making their assessments, courts must focus on various factors, such as content and comprehensibility, intensity of expression, and the characteristics of expected user groups."[188] Whether a warning is adequately conspicuous for data breaches does not differ from other warnings that products liability consistently deals with. Thus, courts, jurors, and existing products liability law are already well equipped to deal with the question of warning adequacy.

[73] Importantly, the fact that a person has signed (or otherwise agreed to) the terms and conditions of a product or service would not be dispositive on the conspicuousness of the warning. Therefore, a company that buries its data policy disclosures in the terms and conditions would not be able to escape liability by arguing that the consumer agreed to the terms and conditions.

[74] Finally, the warning guidelines outlined above would help restore Americans' sense of privacy by helping them understand the risks associated with data collection. To reiterate, 81% of consumers feel like

[186] *See supra* Section IV.e.

[187] *Spruill v. Boyle-Midway, Inc.*, 308 F.2d 79, 85 (4th Cir. 1962).

[188] RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 2 cmt. i (AM. L. INST. 1998).

they lack control of how companies use their data, 79% are concerned about how their data is being used, and 59% don't understand how it is being used.[189] This is not surprising because companies are intentionally vague about their data collection policies.[190] The warnings outlined above will force companies to tell consumers exactly what data is being collected, how it is being used, who it is being disclosed to, and the risks associated with its collection. If a company fails to comply and their database is breached, consumers will have recourse through this law. These warnings represent a shift toward equalizing bargaining power between consumers and tech companies by giving consumers the tools to make informed decisions about how their data is used. Additionally, this newfound transparency may lead to competition regarding data privacy policies such that companies compete to offer consumers greater protections.

f. Manufacturing Defects and Data Breaches

[75] The Restatement Third applies strict liability to manufacturing defects. The relevant language in the Restatement Third is:

> A product is defective when, at the time of sale or distribution, it contains a manufacturing defect, is defective in design, or is defective because of inadequate instructions or warnings. A product:
>
> > (a) contains a manufacturing defect when the product departs from its intended design even though all possible care was exercised in the preparation and marketing of the product.[191]

[189] Auxier et al., *supra* note 135.

[190] *See* Complaint, *supra* note 133, at 2 (stating that Facebook avoided using the term "biometric data" because it "tends to scare people off").

[191] RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 2(a) (AM. L. INST. 1998).

[76] This proposal differs from both Restatements in one, relatively minor, way: strict liability for data products looks at the conduct of the collectors rather than at the product itself.[192] This is because the product is the data, not the data security system, and the harm arises from a failure to protect the data. The data security system is only implicated because it reflects the steps taken to protect the data. Thus, consideration of the security system necessitates considering the conduct of the collector. Strict liability can still apply, but the focus is on the collector's conduct (i.e., the data security system used) rather than the state of the product (i.e., the data).[193] The trigger for strict liability under this proposal is when the data security system is not updated to the newest available version, as discussed below.

[77] The term "manufacturing defect" becomes a misnomer in relation to data breaches. Data security systems are not manufactured in the sense that they come from an assembly line in a factory; rather, data security systems consist of code that is simply copied. The more appropriate term for data breaches would be "failure to update." When an entity knows of a vulnerability in its data security system and identifies a patch for said vulnerability but fails to implement the identified patch, the security system *departs from its intended design*. At the moment the patch is created, the system with the patch becomes the intended design, so a system left without the update becomes defective and the entity will be held strictly liable. Although a company failing to do something as simple as updating their data security system seems unlikely, this is exactly how the Equifax data breach, one of the largest and most publicized data breaches, occurred.[194]

---

[192] *Cf. id*. (focusing on the product rather than the conduct of an actor).

[193] *See also* Personal Data Protection and Breach Accountability Act, S. 1995, 113th Cong. (2014) (showing how Congress has begun to consider punishing the collector's conduct of surreptitiously covering up data breaches).

[194] Nathan Bomey, *How Chinese military hackers allegedly pulled off the Equifax data breach, stealing data from 145 million Americans*, USA TODAY (Feb. 10, 2020, 7:26

[78] The policy incentives for strict liability for a failure to update mirror those of manufacturing defects. Both incentivize those who manufactured the product to invest in product safety, "discourage[] the consumption of defective products," and "reduce[] the transaction costs involved in litigating [the issue of fault]."[195] Additionally, failure to update cases would almost certainly arise from the collector's negligence, so it would be unnecessary and wasteful to require the plaintiffs to prove it.[196] The collector is also best positioned to spread costs and eliminate risks. Finally, because the burden of updating the data security system is so minimal, the resulting financial burden caused by strict liability on collectors would not be too great of a penalty.

[79] Of course, plaintiffs would still need to prove injury and causation.[197] The injury prong occurs once the data is accessed by an unauthorized third party. This proof should not be burdensome for the plaintiffs to procure in the event of a breach because each state has a data breach notification law.[198] Plaintiffs would also need to prove that the data was breached as a result of the failure to update. So, if the hackers breached the system through a defect other than the defect for which the patch was designed, the collector would not be liable for a failure to update. The burden of proof on the causation element will be minor for plaintiffs

PM), https://www.usatoday.com/story/tech/2020/02/10/2017-equifax-data-breach-chinese-military-hack/4712788002/ [https://perma.cc/YS32-X4M8].

[195] *See* RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 2 cmt. a (AM. L. INST. 1998).

[196] *See id.*

[197] *Id.* § 2 cmt. q.

[198] *See generally Security Breach Notification Chart*, PERKINS COIE (Sept. 2021), https://www.perkinscoie.com/en/news-insights/security-breach-notification-chart.html [https://perma.cc/7G38-RCDN] (listing the different data breach notification laws of each state).

because collectors would be required to determine the source of the breach themselves.[199]

g. Alternative Means of Proving Defect

[80] Sections 3 and 4 of the Restatement Third provide for alternative ways for a plaintiff to prove a defect exists in a product.[200]

[81] While § 2(b) explicitly adopts the RAD test in design defect cases, § 3 provides that a plaintiff can prove a defect by showing the incident is of the type "that ordinarily occurs as a result of product defect" and "was not ... solely the result of causes other than product defect."[201] Section 3 essentially adopts *res ipsa loquitur* as a way of proving design defect. This form of proof would be unavailable to plaintiffs in a data breach case involving any theory of defect because data breaches are not something that are "of a kind that ordinarily occurs as a result of [a] product defect[.]"[202] Because there is no data security system that is completely secure,[203] every data security system would have to be defective for this section to apply.

[82] On the other hand, § 4 provides that a product may be defective when it fails to comply with government safety regulations in a way that, had it complied, would have advanced the interests of the statute.[204] This is essentially negligence per se. Negligence per se easily coexists with the

[199] *See supra* Section IV. (b)(i).

[200] *See* RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. §§ 3–4 (AM. L. INST. 1998).

[201] *Id.* § 3.

[202] *See id.*

[203] *See* Winder, *supra* note 147.

[204] RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 4 (AM. L. INST. 1998).

standards set forth in this proposal. Government regulation in the area of data security design and warnings for companies would help guide courts in their decision-making, even though compliance with the regulation is not dispositive of whether the product is defective. [205] Government agencies should be encouraged to promulgate standards to accompany this law by lending their expertise to help guide courts, consumers, and collectors.

h. Disclaimers, Waivers, and the Economic Loss Rule

[83] Section 18 of the Restatement Third provides that "[d]isclaimers and limitations of remedies by product sellers or other distributors, waivers by product purchasers, and other similar contractual exculpations, oral or written, do not bar or reduce otherwise valid products-liability claims against sellers or other distributors of new products for harm to persons."[206] The Restatement Third further explains the rationale behind the rule is that "[i]t is presumed that the ordinary product user or consumer lacks sufficient information and bargaining power to execute a fair contractual limitation of rights to recover."[207]

[84] As applied to data breaches, this rule clarifies that a consumer cannot waive her right to recover for the harm of a data breach. This rule applies for injuries outside of "harm to property or for economic loss," which is governed under § 21 and is more commonly known as the Economic Loss Rule ("ELR").[208] Appropriately, § 18 does not extend to more sophisticated parties with "full information and sufficient bargaining

[205] *See id.* § 4 cmt. a.

[206] *Id.* § 18.

[207] *Id.* § 18 cmt. a.

[208] *Id.* § 18 cmt. c; *see id.* § 21 cmt. f.

power."[209] Thus, in the data breach context, the average consumer would be covered by the protection of § 18 against waivers but one "with full information and sufficient bargaining power" would not be.[210] It is hard to imagine someone ordering a product from Amazon or Best Buy as possessing any sort of bargaining power. The person accepts the product as

is with no bargaining done whatsoever. The carve-out more readily applies to corporate consumers whom this law does not concern.[211] Thus, this section should remain undisturbed.

[85] While the ELR has denied some data breach victims recovery,[212] the statute can provide a cause of action to sidestep the issue entirely. In fact, one of the benefits of addressing this issue with legislation is that a plaintiff asserting a common law negligence claim may be barred by the ELR,[213] but a plaintiff asserting a statutory claim, rather than a tort or contract claim, would not be barred.

[86] Ideally, legislation would provide for a minimum amount of pre-determined damages for a data breach, plus any actual damages the plaintiff may have experienced. The damages should be tiered so the minimum damages are higher for more sensitive information. Legislatures would be wise to remember when crafting the damage amounts that (1) no data is

[209] RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 18 cmt. d (AM. L. INST. 1998).

[210] *Id.*

[211] *See id.*

[212] Nicolas N. LaBranche, Note, *The Economic Loss Doctrine & Data Breach Litigation: Applying the "Venerable Chestnut of Tort Law" in the Age of the Internet*, 62 B.C. L. REV. 1665, 1669 (2021).

[213] *Id.* at 1688–89.

truly anonymous,[214] (2) seemingly non-sensitive data can be aggregated with other identifying information to yield a potential for harm that is greater than the sum of its parts,[215] (3) some information, like biometric information, inherently carries with it greater potential for harm to the consumer,[216] and (4) one of the main purposes of the law is to promote vigilance on the part of the collectors. Legislatures are particularly well-suited to identify the specific value of the harm associated with the theft of certain pieces of information.

V. CONCLUSION

[87] Given the frequency of data breaches and the amount of sensitive information collected by companies, consumers are in need of a data breach law that would provide recourse when their data is exposed. The adaptation of the Restatement Third outlined above would provide consumers with an appropriate cause of action while promoting responsible industry innovation. This adaptation recognizes that the policies promoted by products liability still apply in the data breach context despite a change in the supply chain that decouples the harm from the product.

[88] Products liability principles should be applied to data breaches because data collectors are in the best position to prevent harm to the consumer, much like manufacturers and other sellers are in the traditional supply chain. The Restatement Third strikes the right balance because it recognizes that data breaches can occur even if a data user institutes rigorous data protection practices. In contrast, the Restatement Second's strict liability standard, while more popular, would be too onerous a burden on data users for this same reason. Of course, both Restatements apply strict

[214] *See* Kolata, *supra* note 43.

[215] *See Russian Conspirators*, *supra* note 18 (noting how the hackers used different pieces of information to more easily weaponize seemingly mundane information like email addresses).

[216] *See* 740 ILL. COMP. STAT. 14/5(c) (2022).

liability to manufacturing defects, which in this proposal transforms into a "failure to update" because both occur when the product comes out of conformity with its intended design.

[89] Perhaps the most significant protections that this proposal provides are the required warnings necessary for a consumer to be sufficiently warned of the danger posed by the data collection. Under this proposal, data users would be required to warn consumers of how many entities will have access to the data, what data will be collected, and more. In addition to providing a remedy for harmed consumers, these warning requirements would help bring companies' data policies into the light. Finally, this proposal notes how waivers would be inapplicable in the data breach context and that legislation would be able to circumvent the economic loss rule. Overall, the Restatement Third is the most applicable, cost-effective, and adaptive solution to data breaches. It offers protections for consumers and holds data collectors responsible while simultaneously acknowledging the nuances of the industry and its importance to the economy.