THE YALE LAW JOURNAL FORUM
JANUARY 11, 2018

Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches*

Alicia Solow-Niederman

ABSTRACT. Data breaches continue to roil the headlines, yet regulation and legislation are unlikely to provide a timely solution to protect consumers. Meanwhile, individuals are left, at best, in a state of data insecurity and, at worst, in a compromised economic situation. State common law provides a path forward. Rather than rely on statutory claims or the privacy torts to protect consumer data, this Essay suggests that courts should recognize how contemporary transactions implicate fiduciary-like relationships of trust. By designating what this Essay terms *data confidants* as a limited form of information fiduciary, courts can reinvigorate the tort of breach of confidence as a remedy for aggrieved consumers.

We have a data breach problem. The recent breach of the credit-monitoring agency Equifax implicated the social security numbers, birth dates, and personal information of more than 140 million Americans.[1] Given the richness and sensitivity of this intensely personal data, this breach may be "among [the]

* This Essay reflects developments through December 2017, when it was substantively finalized for publication.

1. Tara Siegel Bernard et al., Equifax Says Cyberattack May Have Affected 143 Million in the U.S., N.Y. TIMES (Sept. 7, 2017), http://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html [http://perma.cc/3U5J-8FMX]; Tara Siegel Bernard & Stacey Cowley, *Equifax Breach Caused by Lone Employee's Error, Former C.E.O. Says*, N.Y. TIMES (Oct. 3, 2017), http://www.nytimes.com/2017/10/03/business/equifax-congress-data-breach.html [http://perma.cc/FG89-LWAX] (estimating that 146 million Americans were affected and reporting that the ex-CEO of Equifax attributed the breach to a lone employee's failure to implement necessary software updates).

wors[t] ever."[2] The incidence of breaches and number of people affected continues to climb. The first half of 2017 witnessed a twenty-nine percent increase in breaches as compared to the same period the year before.[3] And in October 2017, the media reported that three *billion* users of Yahoo! email accounts were affected by a 2013 breach.[4]

This state of affairs should concern policymakers and consumers alike. Congress has failed to enact legislative reform for years.[5] Proposals generally

---

2. Seth Berman, *Richness of Exposed Data Makes Equifax Breach Among Worse Ever*, INFO. MGMT. (Sept. 12, 2017, 6:30 AM), http://www.information-management.com/opinion/richness-of-exposed-data-makes-equifax-breach-among-worse-ever [http://perma.cc/BL8Z-7JA7].

3. *At Mid-Year, U.S. Data Breaches Increase at Record Pace*, IDENTITY THEFT RESOURCE CTR. (July 18, 2017), http://www.idtheftcenter.org/Press-Releases/2017-mid-year-data-breach-report-press-release [http://perma.cc/V7VG-B3AC].

4. *See* Brian Fung, *Actually, Every Single Yahoo Account Got Hacked in 2013*, WASH. POST (Oct. 3, 2017), http://www.washingtonpost.com/news/the-switch/wp/2017/10/03/yahoos-2013-data-breach-affected-all-3-billion-accounts-tripling-its-previous-estimate [http://perma.cc/8CRS-9V34].

   Nor are these breaches the only notable incidents in late 2017. In November 2017, the ride-sharing service Uber revealed that, for nearly a year, it had concealed the theft of sensitive data affecting 57 million riders and drivers. *See* Selena Larson, *Uber's Massive Hack: What We Know*, CNN (Nov. 23, 2017, 4:47 AM), http://money.cnn.com/2017/11/22/technology/uber-hack-consequences-cover-up/index.html [http://perma.cc/NU88-ZJCN]. Uber not only failed to disclose the theft to users and regulators, but also paid the hackers a $100,000 ransom to delete the information—though there is no guarantee that the information was in fact secured.

5. *See, e.g.*, Christin McMeley, *Federal Data Breach Legislation Introduced, But Will It Go Anywhere?*, PRIVACY & SECURITY L. BLOG (June 23, 2013) http://www.privsecblog.com/2013/06/articles/dataprotection/federal-data-breach-legislation-introduced-but-will-it-go-anywhere [http://perma.cc/7Y2B-D49Z] (expressing skepticism that a 2013 bill would be enacted, in part due to the "partisan split and inability to move legislation generally"); Brian Thompson & Sean B. Hoar, *2015 Data Breach Legislation Six Month Review: Many Proposals, Few Changes*, PRIVACY & SECURITY L. BLOG (July 8, 2015), http://www.privsecblog.com/2015/07/articles/policy-regulatory-positioning/2015-data-breach-legislation-six-month-review-many-proposals-few-changes [http://perma.cc/YC88-BET8] (documenting the "stall in Congress" regarding data breach-related legislation, despite "what appeared to be ample bipartisan support"); Martha Wrangham et al., *Calls for Federal Breach Notification Law Continue After Yahoo Data Breach*, GLOBAL IP & TECH. L. BLOG (Oct. 6, 2016) (discussing "stalled" past efforts at federal data breach legislation), http://www.iptechblog.com/2016/10/calls-for-federal-breach-notification-law-continue-after-yahoo-data-breach [http://perma.cc/FVT5-L33V]; Shawn Zeller, *Despite Massive OPM Hack, Congress Continues To Stall on Data Breach Bill*, ROLL CALL (July 22, 2015, 6:30 AM), http://www.rollcall.com/news/despite_massive_opm_hack_congress_continues_to_stall_on_data_breach_bill-242949-1.html [http://perma.cc/8UEJ-KQ75] (describing Congress's failure to move forward on a 2015 bill despite "years of preparation" by members of Congress and seeming agreement that action was in order); Press Release, Blumenthal Introduces Data Breach and Security

rise, then stall, within a familiar cycle of (1) major breach; (2) introduction of one or more data security bills; and (3) legislative inaction. Following the 2015 Target and Home Depot breaches, for instance, there were three bills proposed by Senate Democrats in the first four months of 2015 alone.[6] And once the 2016 Yahoo! breach became public knowledge, at least three draft proposals were introduced in the Senate, each backed by different partisan combinations and interest group blocs.[7] Since the 2017 Equifax breach, there has been renewed legislative attention in the form of congressional hearings,[8] and bills have again been introduced.[9] But the history of inaction seems unlikely to change given

Legislation To Protect Consumers (Sept. 12, 2011), http://www.blumenthal.senate.gov/newsroom/press/release/blumenthal-introduces-data-breach-and-security-legislation-to-protect-consumers [http://perma.cc/3GKC-SNQM] (introducing data breach legislation during the 2011–2012 congressional term).

6. *See* Cory Bennett, *Dem Preps Senate's Third Data Breach Bill*, HILL (Apr. 27, 2015, 11:45 AM), http://thehill.com/policy/cybersecurity/240160-dem-preps-senates-third-data-breach-bill [http://perma.cc/4QT5-PU68].

7. *See* Claude Barfield, *The Ongoing Saga of Yahoo's Stolen Data*, NAT'L REV. (Oct. 6, 2016, 11:16 AM), http://www.nationalreview.com/article/440796/yahoos-hacked-accounts-no-answers-no-solutions-yet [http://perma.cc/KQ3P-4ZQ3] (noting, in the Senate alone, at least three draft proposals backed by different partisan combinations and interest group blocs).

8. *See, e.g.*, *An Examination of the Equifax Breach: Hearing Before the S. Comm. on Banking, Hous., & Urban Affairs*, 115th Cong. (2017), http://www.banking.senate.gov/public/index.cfm/hearings?ID=B61BB78D-CF34-4D54-B7F2-F7F982D77D6F#RelatedFiles [http://perma.cc/68AW-QD7Z] (statement of Richard F. Smith, Adviser to the Interim CEO and Former Chairman and CEO, Equifax); *Examining the Equifax Data Breach: Hearing Before the H. Comm. on Fin. Servs.*, 115th Cong. (2017), http://financialservices.house.gov/calendar/eventsingle.aspx?EventID=402360 [http://perma.cc/8XL3-8DHL] (same); *Oversight of the Equifax Data Breach: Answers for Consumers: Hearing Before the Subcomm. on Dig. Commerce & Consumer Prot. of the H. Comm. on Energy & Com.*, 115th Cong. (2017), http://energycommerce.house.gov/hearings/oversight-equifax-data-breach-answers-consumers [http://perma.cc/CNL6-D23D] (same).

9. *See, e.g.*, Derek B. Johnson, *House Dem Revives Data Breach Bill After Equifax Hack*, FCW (Sept. 18, 2017), http://fcw.com/articles/2017/09/18/langevin-equifax-breach-bill.aspx [http://perma.cc/S3SQ-QLPN] (recounting House Democrats' efforts to revive a data breach bill that was originally introduced in 2015); Marianne Kolbasuk McGee, *Congress Grills Equifax Ex-CEO on Breach*, DATA BREACH TODAY (Oct. 3, 2017), http://www.databreachtoday.com/congress-grills-equifax-ex-ceo-on-breach-a-10354 [http://perma.cc/Y2KL-P396] (listing seven different emerging bills introduced or reintroduced after the Equifax breach); Press Release, In Wake of Equifax Data Breach, Blumenthal, Colleagues Introduce Legislation To Hold Data Broker Industry Accountable (Sept. 14, 2017), http://www.blumenthal.senate.gov/newsroom/press/release/in-wake-of-equifax-data-breach-blumenthal-colleagues-introduce-legislation-to-hold-data-broker-industry-accountable [http://perma.cc/V3KP-MPV8].

the current political climate.[10] More likely, once the uproar fades, the status quo will return until the next big data breach spurs renewed calls for change.[11]

Timely statutory reform also seems unlikely because it is not clear what the ambitions of such a statute should be.[12] Should reform focus, for instance, on improving consumer notifications after a breach, specifying security standards to try to prevent a breach in the first instance, or some hybrid of the two? Further, these proposals have their own challenges. First, the ex post strategy of notification alone might fail to meaningfully empower consumers because it would not necessarily alter overall security standards or affect corporate incentives to invest in security. Yet if notice alone is not enough and the objective is to promulgate some form of overarching security standard ex ante (either alone or in a hybrid model), then determining what technical requirements to apply across different industries is no easy matter. There are also policy obstacles insofar as the American sector-by-sector approach to the treatment of private information largely rejects holistic regulation with regard to the collection, use, and disclosure of information.[13] Prospects for quick, overarching, top-down legislative reform are thus slim.[14]

---

10. Today's Congress is extremely polarized. *See Parties Overall*, VOTE VIEW, http://voteview.com/parties/all [http://perma.cc/GBF9-XDH2] (depicting the ideological gap between liberal and conservative members of Congress); *see also* Philip Bump, *Farewell to the Most Polarized Congress in More Than 100 Years!*, WASH. POST (Dec. 21, 2016), http://www.washingtonpost.com/news/the-fix/wp/2016/12/21/farewell-to-the-most-polarized-congress-in-over-100-years [http://perma.cc/FWG9-VVGF] (discussing the data on historic levels of polarization in the 114th Congress). To make what may be obvious explicit, this degree of polarization challenges the ability to move legislation through Congress, leading scholars to suggest that the 114th Congress, which was the last completed session for which data was available as of this writing, was the "worst ever" in terms of productivity. Norm Ornstein, *Is This the Worst Congress Ever?*, ATLANTIC, (May 17, 2016), http://www.theatlantic.com/politics/archive/2016/05/is-this-the-worst-congress-ever/483075 [http://perma.cc/CG3G-NNEQ].

11. Many participants in the political system share this view. *See* Cory Bennett & Martin Matishak, *Equifax Breach: Turning Point or More of the Same?*, POLITICO (Sept. 12, 2017, 6:13 PM), http://www.politico.com/story/2017/09/12/equifax-security-breach-hackers-242623 [http://perma.cc/74KF-L547].

12. Different policy proposals offer a range of solutions, along with distinctions within each category. *See, e.g.*, Alissa M. Dolan, CONG. RES. SERV., R44326, *Data Security and Breach Notification Legislation: Selected Legal Issues* 2-3 (2015) (discussing eight bills in the 114th Congress alone and noting disparate approaches to both data security and notification, and concluding that "[t]he details of each bill differ and close inspection of each provision and definition is required to determine its specific effect"); Barfield, *supra* note 7 (detailing divergence in recent congressional proposals).

13. With the exception of the Freedom of Information Act of 1966 (FOIA), 5 U.S.C. § 552(a)(3)(A) (2012), and regulation of government actors via the Privacy Act of 1974, 5 U.S.C. § 552a (2012), sectoral regulation of sensitive information is the norm. The core ele-

Yet the issue of data breaches will not simply resolve itself. A world without breaches is improbable,[15] and consumers are limited in how they can address the issue on their own.[16] The status quo can thus result in significant individual economic and emotional harm.[17] This Essay moves past this impasse by arguing that common law courts can and should provide a legal remedy by recognizing the tort of breach of confidentiality as a cause of action available to individuals affected by data breaches. Part I assesses why the leading common law solution, the privacy torts, represents an unsatisfying response to the harms caused by data breaches. Part II situates the tort of breach of confidentiality as a superior alternative. Part III sketches the components of the tort and suggests how a court can update the common law and apply this cause of action in the digital economy.

---

ments are regulation of personal health information (controlled by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.), and associated privacy rules, 45 C.F.R. § 164.508(a) (2007)), credit reporting and financial data (addressed by the Fair Credit Reporting Act of 1970 (FCRA), 15 U.S.C. § 1681 (2012), and Title V of Gramm-Leach-Bliley Act (GLBA), Pub. L. No. 106-102, 113 Stat. 1338 (codified at 15 U.S.C. §§ 6801-09 (2012))), and educational data (covered by the Family Educational Rights and Privacy Act of 1974 (FERPA), Pub. L. No. 93-380, 88 Stat. 484 (codified at 20 U.S.C. § 1232g (2012)).

14. *Cf.* Danielle D'Onfro, *The Best Way to Hold Equifax Accountable*, WASH. POST (Sept. 14, 2017), http://www.washingtonpost.com/opinions/equifax-doesnt-owe-anyone-anything-but-it-doesnt-have-to-be-this-way/2017/09/14/517c2ef6-98c7-11e7-b569-3360011663b4_story.html [http://perma.cc/A4E9-M5ER] (arguing that courts, not regulators, should tackle the modern data breach problem).

15. Eliminating all breaches is neither technologically feasible nor socially desirable. Technological limitations mean that breach-proof security measures are impractical. *See, e.g.*, Tsion Gonen, Data Breach Prevention is Dead, HILL (Feb. 9, 2015, 2:00 PM), http://thehill.com/blogs/congress-blog/technology/232041-data-breach-prevention-is-dead [http://perma.cc/UA7M-DAER] (discussing technological limitations). Moreover, economic and policy realities mean that companies are unlikely to invest in unlimited security measures. From the corporate perspective, it may be more economically efficient to bear the cost of a breach ex post than to invest in the security required to prevent the breach ex ante. *See* Rahul Telang, Policy Framework for Data Breaches, 13 IEEE SECURITY & PRIVACY 77, 79 (2015) (explaining corporate economic incentives). Companies unwilling to bear such risk may also choose not to engage in the activity at all, which would be an unfortunate outcome both for business development and for consumers left unable to enjoy such products and services.

16. *See infra* text accompanying notes 38-42.

17. The *New York Times*' recent interviews with data breach victims viscerally captured the "terror" and years of difficulty that many experience after their data is stolen. Tiffany Hsu, *Data Breach Victims Talk of Initial Terror, Then Vigilance*, N.Y. TIMES (Sept. 9, 2017), http://www.nytimes.com/2017/09/09/business/equifax-data-breach-identity-theft-victims.html [http://perma.cc/76QH-FLXX]; *see also infra* Part I (discussing the nature of the harm caused by data breaches in greater depth).

I. THE LIMITATIONS OF THE PRIVACY TORTS

Given legislative inertia and uncertainty regarding how legislative and regulatory action should address data breaches, a return to common law roots in state court[18] can provide an alternative remedy for aggrieved individuals. Since a breach results in the disclosure of private data, a privacy tort, such as intrusion upon seclusion,[19] public disclosure of embarrassing private facts,[20] false light,[21] or appropriation,[22] would appear the most obvious remedy. Yet, however obvious it may seem, the limitations of the privacy torts counsel in favor of a new model.

First, the privacy torts raise constitutional concerns. There has been a growing sense in recent decades that a robust instantiation of the privacy torts risks infringing on the First Amendment right to freedom of speech and press.[23] Consider, for example, the tort of disclosure of private data: since this

---

18. This analysis focuses on state courts both because a common law approach is an intrinsic fit with data breaches and for instrumental reasons. Even assuming that a statute provides a federal right of action for a data breach victim, a robust literature has documented the uphill battle to achieve standing in cases involving informational injuries in general and data breach suits in particular. *See* Arthur R. Vorbrodt, Note, *Clapper Dethroned: Imminent Injury and Standing for Data Breach Lawsuits in Light of Ashley Madison*, 73 WASH. & LEE L. REV. ONLINE 61, 87-91 (2016), http://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=1046&context=wlulr-online [http://perma.cc/R4LZ-EQM6] (summarizing district courts' tendency, post ACLU v. Clapper, 785 F.3d 787 (2015), to find injury-in-fact too speculative to confer standing in data breach suits)*; see also* Courtney M. Cox, Comment, *Risky Standing: Deciding on Injury*, 8 NE. U. L.J. 75, 85-92 (2016) (discussing standing challenges in data breach suits); Seth F. Kreimer, "*Spooky Action at a Distance*"*: Intangible Injury in the Information Age*, 18 U. PA. J. CONST. L. 745, 756-83 (2015) (providing a general overview of challenges surrounding alleged informational injuries, both in national security and consumer contexts); Angelo A. Stio III et al., *Standing and the Emerging Law of Data Breach Class Actions*, 2015 N.J. LAWYER 49 (discussing "the standing hurdle"). For a recent overview of how courts tend to find inadequate injury-in-fact to support standing in federal data breach claims, see Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. (forthcoming 2018), http://papers.ssrn.com/abstract_id=2885638 [http://perma.cc/H8NY-GVYJ].

19. *See* RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST. 1977).

20. *See id.* at § 652D.

21. *See id.* at § 652E.

22. *See id.* at § 652C. *See generally* William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383 (1960) (taxonomizing the privacy torts).

23. Since the late twentieth century, many scholars have recognized this growing tension between privacy tort law and the First Amendment, and breach of confidence has been suggested as an alternative solution. *See* Susan M. Gilles, *Promises Betrayed: Breach of Confidence as a Remedy for Invasions of Privacy*, 43 BUFF. L. REV. 1, 6-9 & 9 n.41 (1995) (discussing the "severe constitutional setbacks" that face the "ill-fated privacy tort"); G. Michael Harvey,

cause of action would hold the defendant liable for publication or dissemination of information, it could permit private plaintiffs to prevent or remove the speech of others in ways that chill or censor speech and are thus antithetical to First Amendment values.[24] Accordingly, the privacy torts may be of limited practical and doctrinal utility in a society that also prioritizes freedom of speech.[25]

The privacy torts also face a conceptual hurdle because their emphasis on public exposure[26] of private information is misplaced in the data breach context.[27] The traditional model of the privacy torts entails a unitary actor (such as

Confidentiality: A Measured Response to the Failure of Privacy, 140 U. PA. L. REV. 2385, 2450-61 (1992) (discussing Cohen v. Cowles Media Co., 501 U.S. 663 (1991), and explaining why there should not be a constitutional issue with imposing damages in a breach of confidence case). The points offered here are not intended to imply that the current balancing of free speech and privacy in the common law is normatively undesirable; rather, the intent is to describe the doctrinal state of play.

24. *See* Neil M. Richards, *The Limits of Tort Privacy*, 9 J. TELECOMM. & HIGH TECH. L. 357, 357, 365-74 (2011) ("Tort privacy, especially the disclosure tort, has from its inception been in conflict with First Amendment values.").

25. *See* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049 (2000). Particularly in the wake of *Snyder v. Phelps*, the First Amendment seems increasingly likely to provide a shield against tort liability when that tort involves freedom of speech concerns. 562 U.S. 443 (2011) (finding that the First Amendment barred civil recovery for an intrusion upon seclusion claim).

26. Appropriation might be an exception to this point, as this tort involves the use of a person's image or identity for commercial purposes, and not exposure per se. *See* Prosser, *supra* note 22, at 406 (exploring how appropriation "is quite a different matter" from the other privacy torts because the protected interest is a "proprietary" and not a "mental" one). Nonetheless, with three of the four torts arguably focused on exposure, it seems fair to situate the privacy torts, as a whole, as centered on exposure.

27. This Essay does not wade into the rich literature addressing whether privacy law *overall* suffices in today's society, both generally and with particular reference to the privacy torts. For example, Daniel J. Solove's work over a decade ago in *A Taxonomy of Privacy* highlighted the ways that the legal system may fall short when it comes to protecting privacy rights in general. *See* 154 U. PA. L. REV. 477, 481 n.18 (2006) (citing Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?*, 44 FED. COMM. L. J. 195, 208 (1992) ("The American legal system does not contain a comprehensive set of privacy rights or principles that collectively address the acquisition, storage, transmission, use and disclosure of personal information within the business community.")); *see also* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1611 (1999) ("At present, however, no successful standards, legal or otherwise, exist for limiting the collection and utilization of personal data in cyberspace."). And twenty-five years ago, Randall P. Bezanson focused on the limitations of the privacy torts given contemporary realities. *See* Randall P. Bezanson, *The Right to Privacy Revisited: Privacy, News, and Social Change, 1890-1990*, 80 CALIF. L. REV. 1133, 1135 (1992) (arguing that society must adapt the legal concept of privacy and "embed[] [it] in a context different than external and social norms, one allowing its contours to fit the [contemporary] social and economic conditions," and advancing a privacy

a newspaper[28]) broadcasting a private person's information and thereby interfering with the right to be "let alone."[29] The tort of public disclosure of embarrassing private facts, for example, contemplates that there are certain intimate facts about each person, the public exposure of which could wrong them such that there would be no need to plead or prove special damages to obtain a legal remedy.[30] This framework construes privacy in terms of content that is disseminated (and thereby exposed), with an emphasis on publication as the cause of the harm.

Such a focus on the actual public exposure and dissemination of private information is a poor analytic fit for data breaches, which involve a data holder's failure to securely *maintain* private information in the first instance. Imagine I share my name, address, and telephone number with a company as part of a business transaction. Even if just one person (the thief) gains access to this information, injury occurs at the moment that the information is stolen, as soon as the data holder's operational and systemic security decisions have allowed a breach to occur. The company has violated my trust that any initial disclosure of information was limited to the particular context of the transaction with that distinct entity.[31] Furthermore, if my disclosure of data to a commercial actor led

---

model rooted in "the individual's control of information" and "on an enforceable obligation of *confidentiality* for those possessing private information" (emphasis added)).

This Essay treats these debates as foundational and endeavors to move towards legal solutions by focusing more precisely on both a specific problem (data breaches) and a specific remedial path (state common law). Its instantiation of a state common law solution, moreover, builds from the critiques and analysis that have come before by taking seriously Benzanson's proposal that a model of privacy that suits the contemporary era "is more aptly described as a tortious breach of confidence than as an invasion of privacy." *Id*.

28. Neil M. Richards' analysis of the privacy torts' origins explains that a newspaper was the "core defendant" for the tort of disclosure, as originally envisioned. Richards, *supra* note 24, at 362 (2011).

29. Olmstead v. United States, 277 U.S. 438 (1928) (Brandeis, J., dissenting) (describing the "right to be let alone" as "the most comprehensive of rights and the right most valued by civilized men"); *see also* Prosser, *supra* note 22, at 389 (quoting THOMAS M. COOLEY, LAW OF TORTS 29 (2d ed. 1888)).

30. Prosser, *supra* note 22, at 409.

31. As explored in more depth later in the analysis, *see infra* text accompanying notes 49-52, this move builds upon Jack Balkin's proposal for information fiduciaries, which suggests that "[t]he idea of an information fiduciary matters when the fiduciary discloses or uses sensitive information about the beneficiary to the beneficiary's disadvantage without permission." Jack M. Balkin, *Information Fiduciaries in the Digital Age*, BALKINIZATION (Mar. 5, 2014, 4:50 PM) [hereinafter Balkin, *Information Fiduciaries in the Digital Age*], http://balkin.blogspot.com/2014/03/information-fiduciaries-in-digital-age.html [http://perma.cc/5Z6L-APRT]; *see also* Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U. CAL. DAVIS L. REV. 1183 (2016) [hereinafter Balkin, *Information Fiduciaries and the First Amendment*] (refin-

the original business to share information with a third party in order to complete the transaction, then I impliedly trusted that third party to maintain my data securely as part of the chain of commerce—and my confidences are also violated if it is the third party that is breached. In either instance, the core point is how the nature of the harm resulting from the data holder's failure to secure personal information is distinct from the privacy torts' focus on information's publication, dissemination, and use.

Before turning to the technical details of such an explicit or implied duty in Part III below, it is worth further underscoring the human dynamics that motivate the proposed legal intervention. The Equifax and Yahoo! data breaches cast the harmful impact on human beings into especially vivid relief. In the case of Equifax, the breach of a credit-monitoring agency potentially affected anyone who has ever obtained a credit report,[32] even if an individual did not intentionally give information to Equifax. The only way a consumer might have maintained the security of their data would have been to refrain from opening any credit or debit card, an unreasonable solution in today's economy. Yet if a data breach ensues, the cost of engaging in such a transaction might be years of rebuilding credit, potentially inhibiting an individual's ability to purchase a home, fund a business, or pursue other financial objectives.[33] And even if there is no immediate, measurable effect on an individual's credit score, a person who learns their data has been breached must be ever vigilant and wary of the threat that their identity will be stolen in the future.[34] The ongoing emotional and economic impacts of data breaches are thus profound.[35]

---

ing and elaborating on the information fiduciary model); Jonathan Zittrain, Response, *Engineering an Election: Digital Gerrymandering Poses a Threat to Democracy*, 127 HARV. L. REV. F. 335, 339-40 (2014), http://harvardlawreview.org/2014/06/engineering-an-election [http://perma.cc/S223-258H] (exploring the power of online intermediaries and making the case for information fiduciaries); *cf.* Ari Ezra Waldman, *Privacy as Trust: Sharing Personal Information in a Networked World*, 69 U. MIAMI L. REV. 559 (2015) (explicating privacy as built on relations of trust between individuals).

32. The Equifax breach affected people whose data was collected by the company simply because they had obtained a credit report. *See* Seena Greesin, *The Equifax Breach: What to Do*, FED. TRADE COMM'N (Sept. 8, 2017), http://www.consumer.ftc.gov/blog/2017/09/Equifax-data-breach-what-do [http://perma.cc/474U-838V].

33. *See* Solove & Citron, *Risk and Anxiety*, *supra* note 18, at 15-27 (situating the risk and anxiety that consumers face after data breaches as a form of harm); Hsu, *supra* note 17 (relating the experiences of consumers whose data was breached).

34. Recognizing the ongoing threat, myriad newspaper articles published after the Equifax breach advised that consumers pay a $5 to $10 fee with each of the three major credit bureaus (Experian, Transunion, and Equifax) to implement credit freezes, which restrict who is permitted to view one's credit without ex ante consumer consent. *See, e.g.*, Brian Fung, *After the Equifax Breach, Here's How To Freeze Your Credit To Protect Your Identity*, WASH. POST (Sept. 9, 2017), http://www.washingtonpost.com/news/the-switch/wp/2017/09/09/after-the-equifax-breach-heres-how-to-freeze-your-credit-to-protect-your-identity [http://

Equifax is not the first to expose a large swath of American adults to the ongoing "terror" and years of financial difficulties potentially caused by a breach.[36] As illustrated by an October 2017 announcement from Yahoo![37] revealing that three billion email accounts were hacked in 2013, the choice to participate in the information economy by opening an email account creates similar risks. Once a company to which an individual discloses data has been breached, there is little that the individual can do to prevent unauthorized access to their information. It is true that consumers can attempt self-help measures such as changing passwords, monitoring credit information, and exercising vigilance in subsequent online activity by, for instance, using extra caution before clicking on links in emails and confirming that an allegedly encrypted link is in fact properly secured before transmitting sensitive data.[38] But such self-help measures only go so far to prevent a breach outright,[39] and may be of especially limited efficacy after the fact.

The reality is that even hyper-vigilant consumers affected by data breaches may face ongoing problems. Some consumers even find themselves unable to prevent the breached entity itself from continuing to access their data, as was the case after the Equifax breach.[40] Furthermore, ex post remedial measures such as the provision of free credit card monitoring, which Equifax offered

perma.cc/FG89-LWAX] (recommending credit freezes because "[m]aking it even a little bit harder for criminals to put your stolen identity to use could save you an enormous headache").

35. *Cf.* Solove & Citron, *Risk and Anxiety*, *supra* note 18 (appraising the nature of the harm in data breach suits, arguing that legal foundations support the recognition of data breach harms, and suggesting ways that courts can concretely and coherently evaluate the risk and anxiety that data breaches engender).

36. *See* Hsu, *supra* note 17.

37. *See* Fung, *supra* note 34.

38. Heather Kelly, *What To Do If Your Yahoo Account Was Hacked*, CNN TECH (Sept. 22, 2016, 5:38 PM), http://money.cnn.com/2016/09/22/technology/yahoo-hack-password-tips/index.html [http://perma.cc/WF6Q-RWC4] (offering guidance for consumers affected by the first Yahoo! incident).

39. *See, e.g.*, Chris Smith, *New Yahoo Hack: Hackers Didn't Even Need Your Password To Breach Your Account*, BGR (Feb. 16, 2017, 6:50 AM), http://bgr.com/2017/02/16/yahoo-says-hackers-breached-your-account-in-new-attack-without-stealing-your-password [http://perma.cc/DX8T-MFT2] (reporting that changing one's password would do little to redress the "forged cookie" incident involved in the 2016 Yahoo! breach).

40. *See* Farhad Manjoo, *Seriously, Equifax? This Is a Breach No One Should Get Away With*, N.Y. TIMES (Sept. 8, 2017), http://www.nytimes.com/2017/09/08/technology/seriously-equifax-why-the-credit-agencys-breach-means-regulation-is-needed.html [http://perma.cc/LAE9-ETQ2].

after its breach,[41] cannot undo the fact that a customer's social security number has been stolen, creating a heightened risk of identity theft for the foreseeable future.[42] Data breaches, in short, cause myriad, lasting harms that begin the moment a company fails to maintain data securely.

II. AWAY FROM PRIVACY, TOWARD CONFIDENTIALITY

Taking seriously the idea that the harm experienced in a data breach begins the moment that the data holder fails to secure the data that the consumer[43] has provided to it, this Essay advances the tort of breach of confidentiality[44] as an alternative to the privacy torts.[45] The envisioned cause of action would be available when one party (the data holder) has a legal duty to refrain from disclosing specific information provided to it by another party (the consumer).

---

41. *See* Larry Light, *Six Things Not To Do Post-Equifax*, FORBES (Oct. 2, 2017, 12:35 PM), http://www.forbes.com/sites/lawrencelight/2017/10/02/6-things-not-to-do-post-equifax [http://perma.cc/BVV9-AGKD] (describing Equifax's free credit monitoring service, and warning that it may not be enough to protect consumers' data security); Michelle Singletary, *Equifax Has Offered Free Credit Monitoring After Its Epic Data Breach. Here's What Happened When Some People Tried to Sign Up*, WASH. POST (Sept. 21, 2017), http://www.washingtonpost.com/news/get-there/wp/2017/09/21/equifax-has-offered-free-credit-monitoring-after-its-epic-data-breach-heres-what-happened-when-some-people-tried-to-sign-up [http://perma.cc/CJ38-MHP9] (reporting on consumers' experiences trying to enroll in Equifax's credit monitoring services).

42. *See* Solove & Citron, *Risk and Anxiety*, *supra* note 18; Tara Siegel Bernard & Stacy Cowley, *Equifax Hack Exposes Regulatory Gaps, Leaving Consumers Vulnerable*, N.Y. TIMES (Sept. 8, 2017) (surveying regulatory gaps that fail to robustly protect consumers), http://www.nytimes.com/2017/09/08/business/equifax.html [http://perma.cc/SAW4-KEQY]; *cf.* Ari Lazarus, *How Fast Will Identity Thieves Use Stolen Info?*, FED. TRADE COMM'N (May 17, 2017), http://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info [http://perma.cc/HTL8-LNR5] (describing an FTC experiment in which it only took nine minutes for thieves to attempt to use consumer credentials that were posted publicly).

43. For the sake of consistency, this Essay uses the word "consumer" and employs the language of commerce here and in the text that follows; however, as detailed *supra* Part III, the actual inquiry would be fact-sensitive, and potential plaintiffs could include other categories, such as a patient whose medical data was stolen after they entrusted an online health platform with their data.

44. In a widely-cited note from 1982, Alan B. Vickery discusses breach of confidence as "an emerging tort" and proposes a "standard for liability . . . [based on] nonpersonal relationships customarily understood to carry an obligation of confidence." Alan B. Vickery, Note, *Breach of Confidence: An Emerging Tort*, 82 COLUM. L. REV. 1426, 1468 (1982). The analysis that follows understands the terms "tort of breach of confidence" and "breach of confidentiality tort" to be interchangeable.

45. *Cf.* Ari Ezra Waldman, *A Breach of Trust: Fighting Nonconsensual Pornography*, 102 IOWA L. REV. 709 (2017) (arguing that practitioners should turn to the tort of breach of confidentiality as an alternative to other solutions to so-called "revenge porn").

Where the elements of the tort are met,[46] a court may impose liability for disclosure of the information shared by the original party as a breach of the duty of confidentiality.[47] This framework is rooted in the belief that when a consumer discloses personal, potentially sensitive information to an entity, they trust that this data will remain secure.[48]

To delineate the nature of the relationship between data holders and consumers, this Essay argues that data holders are properly understood as a subtype of what Jack Balkin calls "information fiduciaries."[49] Balkin presents information fiduciaries as a class of entities that have "a relationship of trust with a [beneficiary] party" and are "authorized to hold something valuable" on behalf of that beneficiary.[50] Given this relationship of trust, such entities should properly be understood as possessing "special duties to act in ways that do not harm the interests of the people whose information they collect, analyze, use, sell, and distribute."[51] Extrapolating from Balkin's suggestion that information fiduciaries could have duties that differ from traditional fiduciaries,[52] it is appropriate to tailor subcategories of information fiduciaries to fit different sorts of information-sharing relationships.

This Essay argues that given their relationship to consumers, the holders of consumer data in commercial transactions should be labeled with a distinct term: *data confidants*. Data confidants have a duty to securely maintain the information that they receive from customers. This envisioned confidential relationship does not arise from an explicit contractual agreement. It is instead akin to an implied fiduciary relationship[53] that may develop after "one party

---

46. *See supra* Part III.

47. *Id.*

48. This point builds from analysis offered by Jessica Litman, who underscores the connection between trust and "the reuse, correlation, and sale of consumer transaction data." Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1307-08 (2000).

49. Jack M. Balkin, *Information Fiduciaries and the First Amendment*, *supra* note 31, at 1186; *see also* Zittrain, *supra* note 31, at 339-40; Balkin, *Information Fiduciaries in the Digital Age*, *supra* note 31.

50. Balkin, *Information Fiduciaries in the Digital Age*, *supra* note 31.

51. Balkin, *Information Fiduciaries and the First Amendment*, *supra* note 31, at 1186.

52. *Id.* ("[T]here are many types of fiduciary duties. We do not have to treat Facebook or Google exactly the same as your pediatrician, psychotherapist, or accountant. The kinds of obligations that online service providers assume should be carefully calibrated to the kinds of services they actually provide, and the kinds of dependence they produce and encourage in their end users.").

53. To permit ongoing iteration, this Essay intentionally does not resolve whether duties arising from the proposed confidential relationship are classified as a form of limited fiduciary duty, *see* Woodrow Hartzog, *Reviving Implied Confidentiality*, 89 IND. L.J. 763, 770-72 (2014), or as

places trust and confidence in a second person with that second person's knowledge."[54] Even if this sort of relationship may not be "exceptional" in the manner required to find a duty under current tort law, it coheres with the sense of frustration, disappointment, or even outrage that a person may feel when someone they trusted with their personal information fails to maintain that trust. Furthermore, if customers did not voluntarily disclose their information in the first place by entering into a formal relationship with the breached entity,[55] then they may feel even more outraged if that entity knew it had their data, yet made operational choices that failed to secure it. The proposed tort of breach of confidence can address and respond to these facts on the ground,[56] and would thus permit the common law to evolve to meet the challenges posed by contemporary social and economic conditions.[57]

---

a wholly separate obligation, *cf.* R.G. Hammond, Comment, *Is Breach of Confidence Properly Analysed in Fiduciary Terms?*, 25 McGILL L.J. 244, 253 (1979) (deemphasizing doctrinal debates with regard to breach of confidence). The core point here is to surface this way of thinking about the issues, while taking seriously the need for additional research and litigation to develop them with even more precision.

54. Robert A. Kutcher, *Breach of Fiduciary Duties*, *in* 2 BUSINESS TORTS LITIGATION 3 (David A. Soley et al. eds., 2d ed. 2005) (discussing fiduciary relationships created by case law as a result of the relationships and transactions at issue).

55. The individuals affected by the Equifax breach never entered into any sort of contractual agreement with the credit-monitoring agency. *See* Fung, *supra* note 34; Hsu, *supra* note 17.

56. This proposal represents a natural evolution because breach of confidentiality suits are not foreign to the American common law system; U.S. state courts have already recognized versions of this tort, typically in the medical context. *See* Lan Sang v. Ming Hai, 951 F. Supp. 2d 504, 528 & n.8 (S.D.N.Y. 2013) (referring to the breach of fiduciary duty in confidentiality terms); Biddle v. Warren Gen. Hosp., 715 N.E.2d 518 (Ohio 1999) (recognizing the tort of breach of confidentiality in a medical care suit); Tabata v. Charleston Area Medical Center, Inc., 759 S.E.2d 459 (W. Va. 2014) (addressing the breach of confidentiality tort); *see also* Maglio v. Advocate Health & Hosps. Corp., 40 N.E.3d 746, 755 (Ill. 2015) (discussing *Tabata* and distinguishing case); Vickery, *supra* note 44, at 1449-51 (compiling cases); David A. Elder, Privacy Torts § 5:2 (2006) (describing the American "breach of fiduciary relationship-duty of confidentiality tort"); *cf.* Hartzog, *supra* note 53 (discussing suits that involve an implied duty of confidentiality). By tying the breach to the data confidant relationship, this Essay proposes a way to build from what state courts have already done without introducing unbounded liability.

57. This move also has historic roots. Neil Richards and Daniel Solove have traced the American "right to privacy" developed by Samuel Warren and Louis Brandeis in their seminal *Right to Privacy* analysis back to a nineteenth-century British case, Prince Albert v. Strange (1849) 64 Eng. Rep. 293, 295 (Ch.), that applied breach of confidentiality and literary property claims to bar a printer from displaying etchings that Prince Albert had entrusted to him. *See* Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 Geo. L.J. 123 (2007) [hereinafter Richards & Solove, *Privacy's Other Path*]; *see also* Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 Cal. L. Rev. 1887, 1909-11 (2010) (discussing *Prince Albert* and arguing that Brandeis and Warren's omission of confidentiality principles later permitted torts scholar William Prosser to exclude breach of

III. THE NATURE OF THE TORT: ENVISIONING DATA CONFIDENCE

To understand how the tort of confidentiality would function in practice, it is helpful both to contextualize the tort within existing doctrine and to consider its elements with more specificity. The remainder of this Essay presents a framework inspired by the development of products liability tort law as a form of consumer protection. Just as courts expanded manufacturers' duty of care partly in response to the burgeoning automobile industry,[58] so should courts reconsider the liability regime for data holders, whose choices regarding systems design and maintenance affect consumers in increasingly significant ways.[59] Recognizing the need for iteration and further scholarship as common law courts address particular cases on the ground, the following Sections begin the conversation by sketching core components of the proposed tort of confidentiality.

A. Duty

An entity should adhere to the duties of a data confidant if a similarly-situated consumer would disclose data only if they reasonably understood there

---

confidence from his categorization of privacy torts in the highly influential *Second Restatement of Torts*); Vickery, *supra* note 44, at 1452 & n.131 (citing *Prince Albert* to argue that "[h]istorical and comparative precedent exist for the emerging tort [of breach of confidence]"); Waldman, *supra* note 45 at 723-26 (recounting the history of the tort and its development in both Britain and the United States). Other scholars have also suggested that breach of confidentiality might be an alternate way to conceptualize privacy claims. *See, e.g.*, Gilles, *supra* note 23, at 4-6; Hammond, *supra* note 53, at 252 n.38.

58. MacPherson v. Buick Motor Co., 111 N.E. 1050 (N.Y. 1916) (expanding an automobile manufacturer's duty of care beyond a contract-based privity rule).

59. A large body of scholarship explores how the networked sphere has altered the fundamental nature of contemporary consumer-corporate relations. *See, e.g.*, FRANK PASQUALE, THE BLACK BOX SOCIETY (2015) (analyzing how the corporate collection of big data permits the construction of "black box" algorithms that opaquely influence and manipulate human behavior); Paul Langley & Andrew Leyshon, *Platform Capitalism: The Intermediation and Capitalisation of Digital Economic Circulation*, 3 FIN. & SOC'Y 11, 11 (2017) (assessing how platform capitalism "capitalises on the potential of platforms to realise monopoly rents"); Frank Pasquale, *Two Narratives of Platform Capitalism*, 35 YALE L. & POL'Y REV. 309, 309 (2016) (presenting a "counternarrative" to the neoliberal, economic account and considering how "platform capitalism" has transformed consumer experiences and societal dynamics); Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 J. INFO. TECH. 75, 75 (2015) (discussing how companies' ability to profit from data they collect creates a system of "surveillance capitalism"); Litman, *supra* note 48 (providing a prescient early account of how individualized data collection creates a market for consumers' personal data).

to be an implicit or explicit guarantee of confidentiality.[60] Positioning data confidants as a form of fiduciary[61] is the key to invoking the tort in this flexible, yet still bounded, manner. Fiduciary law relies on fact-bound analysis to identify implied as well as explicit relationships of trust,[62] making its application appropriate when the consumer—as a condition of engaging in a transaction—would reasonably expect the data holder to treat their personal information securely.[63]

To assess such expectations and determine whether there is in fact a data confidant duty in a given case, a trier of fact might ask whether a reasonable person would have shared the information in question if they had believed the data would not be secure. If the answer is "no," then it is reasonable to expect confidentiality in the transaction. As a simple example, consumers expect their transaction data to remain secure when they purchase a good, and presumably would not use a credit card to make a purchase if they knew that their financial information would not be securely maintained.[64] Accordingly, in either online or in-store transactions that involve online information processing or electronic

60. *See* Vickery, *supra* note 44, at 1456 (proposing that the duty of confidence would arise if "a reasonable person would conclude that confidentiality is expected" given the nature of the parties' interaction, regardless of the existence of any previously "established relationship between confider and receiver"). Some state courts already implement a cause of action along these lines. For example, California permits a breach of confidence tort based on "a duty not to disclose confidential information where the parties had an understanding that the information was confidential, and that the receiving party would maintain that confidentiality." Berkla v. Corel Corp., 66 F. Supp. 2d 1129, 1151 (E.D. Cal. 1999).

61. *See supra* Part II.

62. *See* Hartzog, *supra* note 53, at 771 (2014) (noting the need for highly contextual determinations about implied confidentiality); *see also* text accompanying notes 49–54.

63. One ironic consequence of the rapid recent increase in data breaches may be that it appears less objectively reasonable for consumers to expect their data to remain secure. Yet the status quo of frequent breaches is not objective in the sense that it reflects a neutral state of play. Rather, it is equally likely to be a refraction of a system in which information and power asymmetries have led consumers to become resigned to the possibility of breaches—not because such frequent breaches are objectively reasonable in a vacuum. The envisioned cause of action would need to take such dynamics into account in setting the appropriate initial benchmark for what represents a reasonable expectation. Furthermore, the proposed intervention is suggested as a start; over time, if it becomes clear that it is not reasonable for consumers to expect companies to keep their information secure, then it may be a signal that legislative or regulatory intervention is in fact necessary to craft a sustainable solution.

64. This approach accords with the White House's 2012 report on consumer data, which proposed a Consumer Privacy Bill of Rights; here, the reasonable expectation of confidentiality would be triggered when an interaction involves the "commercial uses of personal data" described in the report. *See* WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012).

storage of information, a business such as Target or Neiman Marcus would have a general duty to keep its consumers' credit card and associated identifying information confidential if that data was initially disclosed in the context of purchasing a good.[65] In addition, the guarantee of confidentiality should impliedly extend to third-party actors associated with the initial transaction. Equifax's treatment of consumer data, which involved individuals who were not even aware that Equifax had their information, is an example of this class of interactions. To capture the complex relationships entailed in today's data-driven commercial transactions, courts should assess whether data holders owe a duty regardless of whether the person explicitly engaged with them in a commercial interaction. The critical question from a confidentiality standpoint remains whether consumers would have disclosed the data in the first instance, absent the expectation that their personal, private data would remain secure throughout the transaction.

There is space, moreover, to consider further winnowing if liability proves too expansive to permit the common-law system to handle claims in the nuanced, fact-sensitive manner espoused in this Essay. For example, one option would be to narrow the available categories of liability based on the sensitivity of the data, requiring a consumer to prove that the breach of confidentiality involved, say, health or financial data before the data confidant duty would apply. Although this approach might reproduce some of the disadvantages of sectoral regulation,[66] it would target the harm engendered by data security intrusions in a way that current law does not. The tort of breach of confidence is, in short, a flexible and practical remedy.

B. Breach

Inspired by the manner in which products liability law evolved throughout the twentieth century, this Essay advocates for tort law to develop a strict liability model for breach of confidence. This approach would shift the cost of harms

---

65. The standard would therefore apply to incidents such as the 2014 Home Depot breach, which occurred after a third party installed malware on its in-store payment card systems. *See* Kate Vinton, *With 56 Million Cards Compromised, Home Depot's Breach Is Bigger Than Target's*, FORBES (Sept. 18, 2014, 8:21 PM), http://www.forbes.com/sites/katevinton/2014/09/18/with-56-million-cards-compromised-home-depots-breach-is-bigger-than-targets [http://perma.cc/8VL3-FRFA]. Case studies of the incident have concluded that basic security measures, namely implementing P2P encryption and properly segregating the network, could have prevented the breach. *See* Brett Hawkins, *Case Study: The Home Depot Data Breach*, SANS (2015), http://www.sans.org/reading-room/whitepapers/breaches/case-study-home-depot-data-breach-36367 [http://perma.cc/CF8D-T9YN].

66. *See supra* note 13 (summarizing the United States' sectoral approach to privacy regulation).

resulting from data breaches to data holders whose commerce relies on consumer data, rather than requiring these costs to be borne by injured consumers who may be unable to protect themselves.[67]

The recommendation of a strict liability regime in the data breach context is distinct from the negligence claims filed in the wake of Equifax[68] and several other data breaches.[69] Assuming that some data breaches will inevitably occur,[70] a traditional negligence-based cause of action might initially seem more appropriate to avoid raising the duty of care so high as to make the cost of engaging in a socially desirable activity (here, data transactions) prohibitive. However, Guido Calabresi's classic theory of "optimal deterrence" points toward a different approach.[71] If data breaches are understood as a form of accident, then the proper inquiry is how to allocate costs to achieve optimal deter-

---

67. This formulation paraphrases the case that launched modern products liability law, *Greenman v. Yuba*, which noted that "[t]he purpose of such liability is to insure that the costs of injuries resulting from defective products are borne by the manufacturers that put such products on the market rather than by the injured persons who are powerless to protect themselves." 377 P.2d 897, 901 (Cal. 1963) (en banc).

68. As of this writing, a Panel on Multidistrict Litigation had transferred and consolidated 76 civil actions associated with the Equifax breach. *See* In re *Equifax, Inc., Customer Data Security Breach Litigation*, MDL No. 2800 (J.P.M.L. Dec. 18, 2017). District courts had previously stayed multiple putative class action suits involving claims of negligence and/or statutory violations, pending resolution of the motions of consolidation and transfer. *See, e.g.*, Young v. Equifax Inc., No. Case No: 2:17-cv-538-FtM-38CM, 2017 BL 412155 (M.D. Fla. Nov. 16, 2017 (staying claims brought in a Florida district court and reporting over two hundred putative class action suits); Tirelli v. Equifax Info. Servs., LLC, No. 7:17-cv-06868-VB, 2017 BL 364678 (S.D.N.Y. Oct. 06, 2017) (staying claims brought in New York's Southern District); Knepper v. Equifax Information Services, No. 2:17–CV–02368–KJD–CWH, 2017 WL 4369473 (D. Nev. Oct. 2, 2017) (staying claims brought in Nevada). For an overview of one early claim, see Polly Mosendz, *Equifax Faces Multibillion-Dollar Lawsuit Over Hack*, BLOOMBERG (Sept. 8, 2017, 8:55 AM ET), http://www.bloomberg.com/news/articles/2017-09-08/equifax-sued-over-massive-hack-in-multibillion-dollar-lawsuit [http://perma.cc/56MR-3B4E] (describing a class action negligence suit filed in response to the Equifax breach).

69. *See, e.g.*, Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688 (7th Cir. 2015); *In re* Anthem, Inc. Data Breach Litigation, 162 F. Supp. 3d 953 (N.D. Cal. 2016); *In re* Sony Gaming Networks and Customer Data Security Breach Litigation, 996 F. Supp. 2d 942 (S.D. Cal. 2014); *In re* Target Corp. Customer Data Security Breach Litigation, 64 F. Supp. 3d 1304 (D. Minn. 2014).

70. *See supra* note 15.

71. *See* Guido Calabresi, *Optimal Deterrence and Accidents*, 84 YALE L.J. 656 (1974). Danielle Keats Citron has similarly invoked Calabresi's theory in support of a strict liability approach to "leaking databases of sensitive personal information." Danielle Keats Citron, *Mainstreaming Privacy Torts,* 98 CAL. L. REV. 1805, 1845 & nn. 318-19 (2010) (discussing how Calabresi's efficient deterrence theory and Gregory Keating's fairness theory support strict liability). As suggested previously, what distinguishes this Essay's proposed tort is the way in which it locates the harm earlier on—breach of trust occurs at the moment that consumers' personal information is stolen, rather than after the exposure of private content.

rence.[72] A limited rule of strict liability can shift costs to the defendant in a way that is especially appropriate where plaintiffs can do little to prevent or mitigate the resulting harm and defendants are better positioned to avoid the cost of the accident. Both of these conditions obtain in the data breach context. First, even an informed and security-sensitive consumer may be unable to pursue effective self-help measures.[73] Second, as discussed in more detail below, the data holder is better positioned to pinpoint the steps that would bolster security for that entity in an efficient manner[74] as compared to the consumer, who is unlikely to be privy to the data holder's technological and operational practices.

Out of fairness to the data holder, the proposed strict liability framework would be appropriate only in instances in which the plaintiff can establish that a company's conduct has failed to meet a well-instantiated security guideline or otherwise fallen below an established security standard.[75] As an element of the

---

72. *See* Calabresi, *supra* note 71; *see also* Jules Coleman, Scott Hershovitz, & Gabriel Mendlow, *Theories of the Common Law of Torts*, STAN. ENCYCLOPEDIA PHIL. (Dec. 17, 2015), http://plato.stanford.edu/archives/win2015/entries/tort-theories [http://perma.cc/9QQ6-JNP9] (discussing the economic view that the "goal of tort law is to minimize the sum of the costs of accidents and the costs of avoiding them—so-called[] optimal deterrence"). This idea also motivates strict products liability for manufacturing defects: "[a]n often-cited rationale for holding wholesalers and retailers strictly liable for harm caused by manufacturing defects is that, as between them and innocent victims who suffer harm because of defective products, the product sellers as business entities are in a better position than are individual users and consumers to insure against such losses." RESTATEMENT (THIRD) OF TORTS, § 2 cmt. a (AM. LAW INST. 2010).

73. *See supra* text accompanying notes 38-42 (describing limited consumer self-help options or legal recourse).

74. As Calabresi explains, at a theoretical level, this analysis "ask[s], both at the starting point of liability and at however many exception levels are deemed appropriate: who is best suited to make the cost-benefit analysis between accident costs and accident avoidance costs?" *See* Calabresi *supra* note 71, at 670-71. With an eye to the power dynamics at play and the nature of the harm, the company (defendant) appears far better positioned to weigh this balance than the consumer (plaintiff).

75. This proposal might seem to confuse strict liability and negligence. The suggested procedural measure in fact draws from strict products liability law, which distinguishes between a "'strict-liability' regime (in which liability does not depend on negligence, but still signals the breach of a duty) . . . [and] an 'absolute-liability' regime (in which liability does not reflect the breach of any duties at all, but merely serves to spread risk)." Mut. Pharm. Co. v. Bartlett, 133 S. Ct. 2466, 2473 (2013). The common law of strict products liability thus requires a more fine-grained analysis to determine whether a manufacturer is liable in a particular instance. Similarly, the proposed strict liability approach in data confidant suits would include a fact-sensitive analysis of the data holder's conduct before assigning liability. In drawing on the procedural innovations of products liability law, this Essay does not intend to suggest that there is a direct substantive parallel between this cause of action and the tort of breach of confidence, which entail different relationships between actors in the chain

prima facie case, a court could require the plaintiff to establish that the company did not comply with a known standard such as the FTC's Fair Information Practice Principles (FIPPs).[76] The 2017 Equifax breach, for instance, involved basic operational errors, such as the failure to install a software patch.[77] Similarly, the breaches affecting Yahoo! appear to have occurred after the company repeatedly failed to update what was known to be a flawed encryption method.[78] Both of these company's actions arguably fall short of the FIPP guidance on data integrity/security, which stipulates that "[s]ecurity involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data".[79]

To be sure, this framework would not hold data confidants liable across the board, and some data breach victims would still be left without redress. If, for instance, a company complied with all known security standards and there was still a breach that affected a consumer's data, then that plaintiff would not be able to meet the requisite strict liability burden of proof.[80] What would change under the proposed strict liability formulation, however, is that a data confidant could no longer avoid liability if a breach occurred after that data confi-

---

of commerce. Rather, strict products liability illustrates how the common law can adapt to contemporary challenges.

76. Precisely what suffices as such a standard, and who can set them, remains an important question that would need to emerge over time through adjudication of specific controversies. As a start, this Essay points to well-known industry security standards, most notably the FTC's FIPPs (particularly those involving data and security). For an accessible overview of the FIPPs, see *FIPPS: Fair Information Practice Principles*, BERKELEY PRIVACY OFF. (2012), http://ethics.berkeley.edu/sites/default/files/fippscourse.pdf [http://perma.cc/XLC6-B258]. In addition, there are also other well-known industry standards, including the ISO/IEC 27000 family for Information Security Management Systems (ISMS), which delineates over a dozen standards that specify a "systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process." *See ISO/IEC 27000 Family - Information Security Management Systems*, INT'L ORG. FOR STANDARDIZATION, http://www.iso.org/isoiec-27001-information-security.html [http://perma.cc/P9Q4-TJB5]

77. *See* Dan Goodin, *Failure To Patch Two-Month-Old Bug Led to Massive Equifax Breach*, ARS TECHNICA (Sept. 13, 2017, 11:12 PM), http://arstechnica.com/information-technology/2017/09/massive-equifax-breach-caused-by-failure-to-patch-two-month-old-bug [http://perma.cc/LB9P-8GDS].

78. *See* Joseph Menn et al., *Yahoo Security Problems a Story of Too Little, Too Late*, REUTERS (Dec. 18, 2016, 5:18 PM), http://www.reuters.com/article/us-yahoo-cyber-insight-idUSKBN1470WT [http://perma.cc/DG9P-EVDK].

79. *See Fair Information Practice Principles,* FTC, http://web.archive.org/web/20090331134113/http://www.ftc.gov/reports/privacy3/fairinfo.shtm [http://perma.cc/3VRH-74AM].

80. Common sense is in order here; the plaintiff could not, for instance, make a claim that their password was stolen and offer as proof the fact that the company failed to encrypt birthdate information, yet securely stored all password data.

dant did not implement a known security standard or best practice and thereby failed to protect known consumers. Accordingly, in situations where the plaintiff can provide such concrete proof, and where the data confidant relationship is clearly established, shifting from negligence to a strict liability approach to address breaches provides a way to take seriously the harm to consumers when those whom they reasonably expect to secure their data fail to do so.

A critic might still find this approach problematic. Since a third-party hacker commits the illicit actions that are the direct cause of a data breach,[81] one could contend that the data confidant should not be held responsible for the third party's misdeeds. However, the principles drawn from the strict liability manufacturing defects branch of products liability law[82] demonstrate why this intervening act should not necessarily eliminate the data confidant's liability. Here, strict liability obtains if a data confidant engages in data transactions without implementing established security standards, with the knowledge that its organization will use personal data, and its operations in fact permit a breach of that data. From a policy perspective, strict liability is appropriate; an intervening act should not cut off liability if the data confidant's security practices and operational choices increased the probability that the intervening act could occur or made the act possible in the first instance.[83]

---

81. Under the Computer Fraud and Abuse Act (CFAA), the activities involved in theft of consumer data potentially constitute a number of criminal offenses. *See* H. Marshall Jarrett et al., PROSECUTING COMPUTER CRIME, OFF. LEGAL EDUC.: EXECUTIVE OFF. U. S. ATTORNEYS, 1–56 (2010), http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf [http://perma.cc/C98P-NHAP].

82. *Greenman v. Yuba Power Products* enumerated this cause of action, stipulating that a manufacturer is strictly liable in tort if they place a product on the market without inspecting it for defects, with the knowledge that a buyer will use the product, and the item in fact has a defect that injures the purchaser. 377 P.2d 897 (Cal. 1963) (en banc). Others have also suggested connections between technological developments and products liability law. *See, e.g.*, Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1533-39 (2012) (drawing an analogy between cyber attacks and products liability law).

83. This point is conceptually similar to Citron's argument regarding the negligence tort of enablement. *See* Citron, *supra* note 71, at 1836–39. This Essay's invocation of tort law is distinct in that it applies these points in the breach of confidentiality context, via a strict liability cause of action triggered by breaches of duties owed by data confidants. Whereas Citron concludes that the tort of breach of confidentiality "would likely not apply to data brokers and others who lack a relationship with individuals whose information they release," *id.* at 1850 (citing Richards & Solove, *supra* note 18), this Essay's fiduciary-driven, data confidant framework is based in the idea that there *is* in fact an explicit or implied relationship between data holders and consumers, *see supra* Part II, such that the breach of confidentiality tort is apposite.

C. Damages

Finally, a court must address the question of remedies for a data breach. Until there is further study of the number of potential lawsuits and the scope of data confidant liability under the proposed tort, it would be premature to offer too much prescription regarding damages awards. Rather, this Essay focuses on a more fundamental point: common law courts possess the functional capacity to appraise breach of confidentiality as a harm that merits damages. This analytic move is not only pragmatic, insofar as such common law analysis is tied to facts on the ground, but also instrumental from a policy perspective. Regardless of the amount of the damages award, the possibility of liability (especially if claims are aggregated via class action suits, as has been the case for recent data breaches[84]) could incentivize companies to invest in basic steps that would better secure consumer data—and protect the trust that consumers reasonably expect in transactions with data confidants. This approach thus supports this Essay's basic contention that the common law can adapt to provide a legal remedy given the improbability of a timely regulatory or legislative response to data breaches.

As one possible path forward, courts could adapt the Restatement (Second) of Torts's approach to damages in privacy cases.[85] Under such a rubric, damages would be available for harm to the confidentiality interest in cases where the plaintiff has proven that they were injured because an entity that they reasonably expected to act as a data confidant failed to secure their data.[86] Though some may find it troubling to ask a court to assign monetary value to the violation of a person's confidence and the associated invasion of personal information, it is in reality quite similar to the analysis already conducted by common law courts with regard to privacy (for privacy torts[87]) and reputation (for

---

84. *See, e.g.*, *supra* notes 68-69.

85. *See* RESTATEMENT (SECOND) OF TORTS § 652H (AM. LAW INST. 1977). This Essay's approach to damages, which builds from the privacy torts' approach, is inspired by Sarah Ludington's analysis. *See Reining in the Data Traders-A Tort for the Misuse of Personal Information*, 66 MD. L. REV. 140, 186 (2006).

86. *See supra* Parts III.A-B.

87. *See, e.g.*, Socialist Workers Party v. Att'y Gen. of U.S., 642 F. Supp. 1357, 1422 (S.D.N.Y. 1986) (assessing damages in privacy tort suit); Monroe v. Darr, 559 P.2d 322, 327 (Kan. 1977) (assessing damages in tort suit for invasion of privacy); Sabrina W. v. Willman, 540 N.W.2d 364, 370-72 (Neb. Ct. App. 1995) (discussing damages in both privacy torts and defamation suits, and compiling cases); Turner v. General Adjustment Bureau, Inc., 832 P.2d 62, 67 (Utah Ct. App. 1992) (assessing the existence of damages in intrusion upon seclusion tort claim).

defamation[88]).[89] Damages need not be an element of the prima facie case, but instead could be assessed separately through a "prudential," case-specific filter.[90] Where the plaintiff meets their burden of proof, damages could also be awarded for mental distress, such as anxiety and loss of peace of mind,[91] that can result from a failure to maintain private data securely. Regardless of the precise formulation, the bottom line is that the award of monetary remedies can be crafted to foster doctrinal continuity at the same time that the distinctive requirements of the proposed breach of confidence tort permit evolution of the law.

* * *

If the security of information is to be taken seriously in the face of recent breaches like the Equifax incident, then the common law should update its content to ensure that personal, private data is robustly protected. This Essay contends that such an update requires recourse to a remedy when an entity that holds itself out as a data confidant fails to adopt established best practices and industry standards for its operations and security protocols. Such an actor has

---

88. *See, e.g.*, *In re* Lipsky, 460 S.W.3d 579, 593-94, 595-97 (Tex. 2015) (first discussing how Texas state law awards damages in defamation suits, then applying the rule); Smith v. Durden, 276 P.3d 943, 952 (N.M. 2012) (detailing New Mexico's state law of defamation, and underscoring what the plaintiff must prove to recover damages); Greenmoss Builders, Inc. v. Dun & Bradstreet, Inc., 461 A.2d 414, 419-21 (Vt. 1983) (summarizing, then applying, rules that controlled the availability of general and punitive damages at the time of adjudication), *aff'd*, 472 U.S. 749 (1985), *abrogated by* Lent v. Huntoon, 470 A.2d 1162 (Vt. 1983).

This Essay does not take a position on whether the data breach harm should be seen as analogous to defamation *per se* (which does not require the plaintiff to plead special damages, *see, e.g.*, Gertz v. Robert Welch, Inc., 306 F. Supp. 310, 311 (N.D. Ill. 1969); *see also* Gertz v. Robert Welch, Inc., 418 U.S. 323, 327 (1974) (discussing the *per se* standard), or *per quod* (which does require the plaintiff to plead special damages). As in defamation law, this decision should be a matter of state law. The key point here is that common law courts can and do determine when plaintiffs should recover for alleged damages to reputation and are functionally equipped to make similar assessments with regard to violations of confidentiality.

89. By requiring the plaintiff to make a clear prima facie showing as to how the defendant has fallen short of its duty to protect reasonable security expectations, this approach respects the common law's careful differentiation between injury and damages. *See*, *e.g.*, City of N. Vernon v. Voegler, 2 N.E. 821, 824 (1885) ("There is a material distinction between damages and injury. Injury is the wrongful act or tort which causes loss or harm to another. Damages are allowed as an indemnity to the person who suffers loss or harm from the injury. The word "injury" denotes the illegal act; the term "damages" means the sum recoverable as amends for the wrong."); Restatement (Second) of Torts § 902 (1979).

90. *See* John C.P. Goldberg & Benjamin C. Zipursky, *The Fraud-on-the-Market Tort*, 66 VAND. L. REV. 1755, 1772 (2013) (describing how "proof of damage" can operate as "a *prudential limit* designed to screen out *valid* but de minimis [] claims, not as an *element* of the wrong").

91. *See supra* text accompanying notes 31-42 and associated sources.

not maintained the trust that its consumers vested in it. It is past time to wait for a regulatory fix that may never come. A common law solution rooted in tort law's confidentiality principles is worth pursuing to empower consumers in today's information economy.

Alicia Solow-Niederman is a fellow at the UCLA School of Law's Program on Understanding Law, Science, and Evidence (PULSE). She graduated from Stanford University with distinction in communication and political science and received her J.D. from Harvard Law School, cum laude, *where she served on the editorial board of the* Harvard Law Review. *She would like to thank the following individuals for their insightful comments, suggestions, and encouragement: Amy Johnson, Greg Muren, Leah Plunkett, Richard Re, Morgan Weiland, Jordi Weinstock, and the editors of the* Yale Law Journal. *She is grateful to Jonathan Goldberg and Henry Smith, whose 2016 Private Law Workshop inspired and informed the arguments advanced in this Essay, to the Berkman Klein Center for Internet & Society faculty and staff, especially Yochai Benkler, Urs Gasser, and Jonathan Zittrain, for their guidance along the way, and to her family for their tireless support. The views presented here as well as any errors are hers alone.*

Preferred Citation: Alicia Solow-Niederman, *Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches*, 127 YALE L.J. F. 614 (2018), http://www.yalelawjournal.org/forum/beyond-the-privacy-torts.