STANDING ON UNSETTLED GROUND: WHAT THE COURT IN *FERO V. EXCELLUS HEALTH PLAN, INC.* GOT WRONG AND WHY CONGRESS SHOULD ENACT COMPREHENSIVE DATA SECURITY LEGISLATION

Introduction

Beginning in late 2013, hackers illegally breached the computer systems of the healthcare provider Excellus Health Plan, Inc., and subsequently gained access to the personal information of millions of individuals serviced by the company.[1] In the wake of this incident, the company hired an independent cybersecurity firm to investigate which found that the breach affected approximately 10 to 10.5 million individuals while exposing numerous forms of personal information.[2] This, in turn, spurred several putative class action suits against a group of eight defendants tied to the breach for various causes of actions.[3] In response to the litigation, the defendants moved to dismiss for lack of standing[4] which the Federal District Court for the Western District of New York granted in part and denied in part.[5]

Under Article III of the U.S. Constitution[6], federal court jurisdiction is dependent upon reviewing an actual "case" or "controversy".[7] In fact, the U.S. Supreme Court held in *Clapper v. Amnesty Int'l USA* that this standard is central to the design of the judicial branch[8] in that, "[n]o principle is more fundamental to the judiciary's proper role in our system of government than the constitutional limitation of federal-court jurisdiction to actual cases or controversies."[9] Accordingly, from this principle flows the requirement that parties in federal lawsuits must have Article III standing in order for a federal court to judge the merits of a case.[10] In fashioning a standard for this constitutional requirement, the Court has articulated that standing requires a party to allege an injury which is, "[1] concrete, particularized, and actual or imminent; [2] fairly traceable to the challenged action; and [3] redressable by a favorable ruling."[11] However, in the context of litigation involving data breaches, federal courts have struggled to find consensus on

whether the heightened threat of identity theft from these breaches satisfies these elements.[12] This disagreement, highlighted by the issues raised in *Fero v. Excellus Health Plan, Inc.*, will only command greater attention as data breaches become more acute in both frequency and magnitude in our modern society.[13]

Because circuit courts continue to diverge on the question of standing in data breach litigation and the Supreme Court has (to date) been reluctant to address this issue,[14] this Comment proposes that Congress should enact comprehensive legislation which sets a minimum national standard for data protection as well as enhances present state efforts by mandating disclosure when data is breached. Additionally, this Comment proposes that Congress should create a private right of action for consumers whose data is breached to recover reasonable expenses for mitigating potential identity theft. Part I discusses how various courts have approached standing in data breach litigation as well as previous scholarship on this topic. Part II explores the *Fero* Court's holdings and rationale for its decision. Finally, Part III addresses the proposed solution to clarify standing in data breach litigation including: strengthening data security and disclosure laws, creating a private right of action for certain types of data breaches, and encouraging the Supreme Court to recognize this new right as satisfying standing in data breach cases.

I. Background

As the Supreme Court and recent scholarship has recognized, the concept of standing represents one of the most crucial restraints on the federal judiciary's power.[15] Though integral to the separation of powers, it has presented victims of data breaches difficulties[16] in bringing suit against parties whom they entrusted with personal information. The current circuit split on the viability of these suits centers primarily on the interpretation of the Supreme Court's opinion

in *Clapper v. Amnesty Int'l USA* which held that a necessary component of standing is either a "certainly impending" injury[17] or a "substantial risk of harm".[18] Some courts have found that *Clapper* does not preclude these suits because the heightened risk of identity theft from the release of personally identifiable information is an injury sufficient to establish standing.[19] However, others have held that the risk of future identity theft does not satisfy either of these standards.[20] Moreover, many of these courts find that *Clapper's* bar[21] on manufacturing standing by incurring mitigation costs for a potential non-imminent harm precludes these future injury suits.[22]

Complicating matters further, courts have also leaned on *Clapper's* dismissal of harms based on a "highly attenuated chain of possibilities"[23] which are dependent on the "decisions of independent actors"[24] to either uphold or dismiss data breach litigation. On the one hand, some courts such as the Seventh Circuit[25] and the Northern District of California[26] have held that a data breach caused by hackers implicates the possible misuse of personal data which is neither "highly speculative" nor "highly attenuated". In fact, the court in *Remijas v. Neiman Marcus Grp.* summarized the goal of deliberate data breaches by noting that, "[w]hy else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."[27] Alternatively, other courts like the Fourth Circuit[28] have found that the, "enhanced risk of future identity theft [is] too speculative"[29] because it relies on predicting the decision-making of unknown third parties.

Resolving the glaring ambiguity surrounding standing in data breach litigation is crucial at this point in time as data breaches inflict greater harms.[30] According to recent figures compiled by the Ponemon Institute, the average per capita cost of a data breach is nearly $200[31] and this

amount increases when the figures are broken out by industry classification with the average healthcare data breach topping out with the highest loss for any industry at more than $230 per capita.[32] Despite the increasing frequency of malicious data breaches, to this point, Congress has attempted,[33] but failed, to pass comprehensive data security legislation which would help protect consumers' personal information and provide victims remedies to mitigate damages from identity theft. For example, in 2009 a bipartisan group of senators proposed the Personal Data and Security Act which had the stated purpose of "prevent[ing] and mitigat[ing] identity theft. . .[and] provid[ing] notice of security breaches."[34] The bill also found that, "individuals whose personal information has been compromised or who have been victims of identity theft should receive the necessary information and assistance to mitigate their damages and to restore the integrity of their personal information and identities."[35] More recently, Senator Nelson has proposed the Data Security and Breach Notification Act which would require companies to report data breaches within a month or face criminal penalties.[36]

On the other hand, states[37] and foreign governments[38] have fared better in passing data security legislation; with some spurred to act by recognition of the right to privacy as a fundamental right.[39] For example, California requires persons or businesses conducting business in the state to disclose data breaches as expediently as possible.[40] Among foreign governments, the Philippines enacted legislation requiring companies to: implement reasonable measures and safeguards to prevent unlawful access and fraudulent misuse of data;[41] conduct regular monitoring for security breaches;[42] notify affected parties when there is a reasonable belief that unauthorized acquisition of data could lead to a "serious risk of harm";[43] and indemnify consumers for damages sustained due to unlawfully obtained or unauthorized use of personal information.[44]

Although some have called for the U.S. to pass similar measures including a private right of action for victims of data breaches,[45] there is an open question of whether the Supreme Court's decision in *Spokeo, Inc. v. Robins* foreclosed the possibility of violations of such a law as sufficient to invoke standing.[46] In *Spokeo,* the court held that a mere procedural violation of the Fair Credit Reporting Act was insufficient to establish standing because the alleged harm was not concrete.[47] Additionally, the Court held that, "injury in fact is a constitutional requirement, and '[i]t is settled that Congress cannot erase Article III's standing requirements by statutorily granting the right to sue to a plaintiff who would not otherwise have standing.'"[48] However, the court also noted that when considering standing, "it is instructive to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts."[49] This statement is particularly relevant to the discussion of standing in data breach litigation because an invasion of privacy was traditionally seen as a common law harm.[50]

II. Case Description

In *Fero v. Excellus Health Plan, Inc.*, the district court dismissed some of the plaintiffs, but rejected dismissing others based on the requirements set forth in *Clapper v. Amnesty Int'l USA*.[51] Although the Second Circuit had previously held that a data breach did not confer standing absent fraudulent charges or the release of personally identifiable information,[52] the district court was not bound by precedent because this ruling occurred in a summary order which lacks precedential value per local rule.[53] Thus, the court relied primarily on *Clapper's* "certainly impending standard" along with attenuation to determine whether the plaintiffs lacked standing.

The court dismissed the "non-misuse" plaintiffs because it found they failed to allege that harms were "certainly impending", noting that at no point in the three years since the breach

occurred could these parties point to a misuse of personal information.[54] It also declined to find standing because doing so would require relying "on a chain of possibilities about the actions of independent actors."[55] The court also rejected arguments that these plaintiffs plead an injury-in-fact by incurring mitigation expenses because per *Clapper*, mitigation efforts for a non-imminent harm cannot confer standing.[56] Finally, the court upheld the standing of "misuse" plaintiffs who alleged tax fraud and identity theft among other misuses and rejected the defendants' argument that the alleged misuse was not "fairly traceable" because it could have resulted from other breaches.[57] At the pleading stage, the court found the allegations were sufficient to establish traceability.[58]

III. Analysis

Though the *Fero* Court was correct in declining to apply a stringent causation test in order to uphold standing for the "misuse" plaintiffs, it missed the mark on the "non-misuse" plaintiffs who, despite experiencing an elevated risk of identity theft, were left out with an opportunity for recourse in the federal courts. With some circuit courts aligning with the legal reasoning in *Fero* and others in opposition, the time is ripe for Congress to step in and vitiate this quandary by passing comprehensive data security legislation and creating a private right of action for victims of certain types of data breaches. This solution would serve the dual goals of enhancing data security and bringing certainty to a legally divisive question.

A. Congress Should Pass Comprehensive Data Security Legislation

The mishmash of federal court decisions upholding or dismissing standing in data breach litigation has created pockets of consumers whose ability to seek redress for the hacking of their personally identifiable information is dependent on their geographic location.[59] In order to standardize treatment across the country, Congress should pass legislation requiring entities that

maintain personally identifiable information[60] like social security numbers, dates of birth, and credit card numbers to institute administrative, technical, and physical safeguards to protect consumer data.[61] These measures should include best practices such as mandating incident response plans—which have been shown to reduce the costs of data breaches[62]—and privacy risk assessments periodically evaluated by independent auditors.[63] Additionally, these mandates should be coupled with disclosure and coordination with technical experts[64] and government regulators like the Federal Trade Commission when breaches do occur. Such public disclosures incentivize stakeholders to apply institutional pressure in order to encourage organizations to improve data security controls.[65] Disclosure laws also directly prompt organizations to improve data controls and deter individuals from conducting data breaches.[66] To assuage concerns that federal legislation would be a chance to water down requirements,[67] any law Congress enacts should institute minimum standards which supplement rather than preempt state regulation of data security and disclosure.

Although the *Fero* Court found that the "misuse" plaintiffs alleged harms that were "fairly traceable" to the defendants' data breach, others have noted the difficulty in tracing identity theft to any one particular breach.[68] Moreover, once personally identifiable information is breached, identity thieves can use this information for years after the unauthorized acquisition because information like Social Security numbers and dates of birth remain unchanged.[69] In fact, many identity thieves will tailor their use of stolen personal information with time sensitive data like credit card numbers used quickly and more ossified data like Social Security numbers used after several years.[70] Thus, it is imperative to institute a longer statute of limitations for data breach litigation—certainly longer than the two years used in other federal statutes dealing with specific types of data breaches.[71]

B. Congress Should Also Create Private Rights of Action When Data Breaches Occur

With many calling on Congress to pass data security legislation,[72] it is equally important for Congress to also create a private right of action for parties whose personal information is breached. Although the *Fero* Court and others have held that consumers who have not yet suffered misused data or did not suffer any unreimbursed costs lack standing, these decisions miss the mark. As noted above, identity theft can take years to materialize, yet victims of breaches have to incur costs in the present to minimize the risk of future injury.[73] These costs include spending time monitoring credit reports and placing credit freezes/fraud alerts.[74] Moreover, services like credit monitoring which have been offered by companies in the wake of data breaches[75] cannot protect against all forms of identity theft.[76] Various forms of non-credit identity theft[77] including medical ID theft and tax fraud can be especially pernicious.[78] Therefore, the private right of action should extend to victims of data breaches involving the unauthorized disclosure of certain types of personal information which are difficult to change. Lost in the debate between federal courts is that not all data breaches are equal. Data breaches involving sticky personal information like Social Security numbers and dates of birth cast a shadow of future identity theft over victims' lives more acutely than the disclosure of credit card numbers. With these types of breaches, the personal losses can be staggering.[79]

Accordingly, the substantial in the "substantial risk of harm" standard discussed in *Clapper* can apply not only as a metric of the likelihood of identity theft, but also as an indicator of the potential magnitude of identity theft that could befall a victim.[80] A breach of this type of data should then trigger liability on the defendant(s) behalf for all reasonable mitigation expenses as determined by Congress. Any reasonable mitigation expenses which are not paid by the defendant can then give victims an injury-in-fact and grounds for standing in a federal lawsuit.

C. A Private Right of Action Should Satisfy the Supreme Court's Decision in *Spokeo*

As discussed in Part I, the Supreme Court held in *Spokeo* that a plaintiff, "cannot satisfy the demands of Article III standing by alleging a bare procedural violation,"[81] and also held that Congress cannot simply grant Article III standing when a plaintiff would not otherwise have standing.[82]Thus, some defendants would likely argue that enacting federal data security legislation which includes a private right of action for data breaches is insufficient to invoke standing if affected plaintiffs do not suffer a "concrete" injury.[83] However, the *Spokeo* Court also held that comparing an alleged intangible harm to common law harms is informative in evaluating whether a party has standing.[84] Because the invasion of the right to privacy was considered a common law harm,[85] federal legislation creating a private right of action for breaches of private personal information should satisfy *Spokeo's* requirements—especially if the proposed right of action is limited to plaintiffs with unreimbursed reasonable mitigation expenses. These unreimbursed expenses should satisfy the concrete and particularized prongs as discussed in *Spokeo*.[86] The proposed legislation would ensure that the breach of personal information like that which occurred in *Fero* would not go uncompensated and that affected parties would have recourse to recover for reasonable mitigation expenses.

Conclusion

In *Fero v. Excellus Health Plan, Inc.*, the court for the Western District of New York held that certain plaintiffs in data breach litigation lacked Article III standing because their failure to allege a misuse of their personal information meant that they did not suffer an injury-in-fact as required by the Supreme Court's prior jurisprudence. The *Fero* court also rejected the "non-misuse" plaintiffs' claims that incurring expenses to mitigate the risk of future identity theft

accorded them standing because the Supreme Court held in *Clapper v. Amnesty Int'l USA* that plaintiffs cannot manufacture standing by incurring expenses for a non-imminent harm.

However, the *Fero* Court's decision was predicated on the incorrect view that the heightened risk of identity theft was insufficient to establish standing because the release of personal information such as Social Security numbers and dates of birth represents a long-term threat of identity theft in line with *Clapper's* "substantial risk of harm" standard. Because federal courts have divided on whether parties who have not yet suffered losses from data breaches have standing, Congress should step in and answer this question in the affirmative. By enacting comprehensive data security legislation and creating a private right of action for victims of certain types of data breaches, Congress can ensure that victims of data breaches are compensated for the heightened risk of identity theft and entities are held responsible when they allow hackers to penetrate their security systems.

[1] Fero v. Excellus Health Plan, Inc., 236 F. Supp. 3d 735 (W.D.N.Y. 2017).

[2] *Id*. at 744 (noting that the hackers were able to access "individuals' names, dates of birth, social security numbers, mailing addresses, telephone numbers, member identification numbers, financial payment information (including credit card numbers), and medical insurance claims information.").

[3] *Id*. at 743, 745 (bringing, among others, claims for negligence and violation of state consumer protection laws).

[4] *See Standing*, BLACK'S LAW DICTIONARY (10th ed. 2014) ("A party's right to make a legal claim or seek judicial enforcement of a duty or right.").

[5] *Fero*, 236 F. Supp. 3d at 743.

[6] *See* U.S. CONST. art. 3, § 2, cl. 1, *amended by* U.S. CONST. amend. XI.

[7] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 408 (2013).

[8] *Id*. at 408 (holding that Article III standing serves separation of powers principles by preventing the judiciary from, "usurp[ing] the powers of the political branches). *See generally* THE FEDERALIST NO. 78 (Alexander Hamilton) (writing that an independent judicial branch does not pose a threat to individual liberty, "so long as the judiciary remains truly distinct from both the legislature and the [e]xecutive.").

[9] *Clapper*, 568 U.S. at 408 (quoting DaimlerChrysler Corp. v. Cuno, 547 U.S. 332, 341 (2006)).

[10] *Clapper*, 568 U.S. at 409.

[11] *Id*. at 409 (citing Lujan v. Defenders of Wildlife, 504 U.S. 555, 560-61 (1992)).

[12] *Compare* Adobe Sys. Inc. Privacy Litig., 66 F. Supp. 3d (N.D. Cal. 2014) (holding that the plaintiffs had standing because they alleged concrete and imminent future harms sufficient to establish injury in fact at the pleading stage based on substantial risk of harm from *Clapper*),

with Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017) (finding that the increased risk of identity theft was too attenuated and insufficient to establish standing). *See also* Fero v. Excellus Health Plan, Inc., 236 F. Supp. 3d 735, 749 (W.D.N.Y. 2017) (noting that the Sixth, Seventh, and Ninth Circuits have endorsed standing based on an increased risk of identity theft, whereas the Third and Fourth Circuits have rejected this theory as too speculative to constitute an injury in fact).

[13] *See, e.g.*, Edvard Patterson, *Equifax May be Happy Paying $1 Per Customer for Their Hassle*, BLOOMBERG (Sep. 20, 2017, 5:14 PM), https://www.bloomberg.com/news/articles/2017-09-20/equifax-may-be-happy-to-spend-1-per-customer-for-their-trouble (personal information of 143 million consumers breached); FOX 5 Atlanta, *Officials Say Residents' Data Possibly Hacked in Data Breach*, YOUTUBE (Mar. 27, 2018), https://www.youtube.com/watch?v=TVkJZwEjdh8 (data breach by local government); Reuters, Target Settles 2013 Hacked Customer Data Breach for $18.5 Million, NBC NEWS (May 24, 2017, 10:49 AM), https://www.nbcnews.com/business/business-news/target-settles-2013-hacked-customer-data-breach-18-5-million-n764031 (Target data breach expected to cost over $200 million); *cf.* Mark Zuckerberg, FACEBOOK (Mar. 21, 2018, 2:36 PM), https://www.facebook.com/zuck/posts/10104712037900071 (discussing Cambridge's Analytica's misuse of users' data). Despite the growing incidence of data breaches in recent times, the concept of identity theft has longstanding historical roots. *E.g.*, *Genesis* 27:24 (King James) (discussing the story of Jacob impersonating his brother Esau); WILLIAM SHAKESPEARE, OTHELLO act 3, sc. 3 ("[H]e that filches from me my good name [r]obs me of that which not enriches him [a]nd makes me poor instead.").

[14] Attias v. CareFirst, Inc., 865 F.3d 620 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018).

[15] *See Clapper*, 568 U.S. at 409; *see also* Martin H. Redish & Sopan Joshi, *Litigating Article III Standing: A Proposed Solution to the Serious (but Unrecognized) Separation of Powers Problem*, 162 U. PA. L. REV. 1373, 1384 (2014) (arguing that "standing doctrine limits the unelected judiciary's ability to interfere with . . . decisions made by the democratically elected political branches.").

[16] *E.g.*, Nicole Hong, *For Consumers, Injury is Hard to Prove in Data-Breach Cases*, WALL ST. J. (June 26, 2016, 8:06PM), https://www.wsj.com/articles/for-consumers-injury-is-hard-to-prove-in-data-breach-cases-1466985988 (discussing the split between the Seventh Circuit and other courts while also noting that it is difficult to trade identity theft to a particular breach).

[17] *Clapper*, 568 U.S. at 401 (holding that a threatened injury must be "certainly impending") (citing Whitmore v. Arkansas, 495 U.S. 149, 158 (1990).

[18] *Clapper*, 568 U.S. at 414 n.5 ("Our cases do not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about. In some instances, we have found standing based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm.") (citations omitted).

[19] *E.g.*, Attias, 865 F.3d at 626; *see also* Galaria v. Nationwide Mut. Ins. Co., 663 Fed. App'x 384 (6th Cir. 2016) (unpublished opinion) ("[T]here is a sufficiently substantial risk of harm that incurring mitigation costs is reasonable."); *cf.* Remijas v. Neiman Marcus Grp., 794 F.3d 688, 694 (7th Cir. 2015) (distinguishing *Clapper* by noting that that case addressed speculative harm whereas this case involves an actual breach).

[20] *See In re* Supervalu, Inc. v. Supervalu, Inc., 870 F.3d 763 (8th Cir. 2017) (finding that some of the plaintiffs did not allege a substantial risk of harm because the data breach spurring the litigation did not involve the release of personally identifiable information such as "social

security numbers, birth dates, or driver's license numbers"); Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017).

[21] *Clapper*, 568 U.S. at 422 (holding a plaintiff "cannot manufacture standing by incurring costs in anticipation of non-imminent harm").

[22] Fero v. Excellus Health Plan, Inc., 236 F. Supp. 3d 735, 754 (W.D.N.Y. 2017); *In re Supervalu, Inc.*, 870 F.3d at 771–772.

[23] *Clapper*, 568 U.S. at 410.

[24] *Id.* at 413.

[25] Remijas v. Neiman Marcus Grp., 794 F.3d 688, 693 (7th Cir. 2015).

[26] *In re* Adobe Sys. Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014)

[27] *Remijas*, 794 F.3d at 693.

[28] Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017)

[29] *Id.* at 264; *see also Jor*dan Z. Dillon, Comment, *Standing on the Wrong Foot: The Seventh Circuit's Eccentric Attempt to Rescue Risk-Based Standing in Data Breach Litigation*, 56 WASHBURN L.J. 123, 130 (2017) (noting the Third Circuit distinguished data breaches from other future harm cases like medical malpractice or toxic torts because "identity theft depends on third party actions, which are inherently speculative").

[30] *See* Patterson, *supra* note 13; Merritt Baer, *Your Voter Records are Compromises. Can You Sue? Theories of Harm in Data-Breach Litigation*, LAWFARE (Aug. 7, 2017, 11:03 AM), https://lawfareblog.com/your-voter-records-are-compromised-can-you-sue-theories-harm-data-breach-litigation (198 million voter records breached).

[31] PONEMON INST., 2013 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS 5 (2013).

[32] *Id*. at 6. *See generally* Vincent Liu et al., *Data Breaches of Protected Health Information in the United States*, 313 J. AM. MED. ASS'N 1471, 1471 (2015) (breaches of sensitive healthcare information rose every year from 2010 to 2013).

[33] *See* Personal Data and Security Act, S. 1490, 111th Cong. (2009); Kim Zetter, *National Data Breach Laws Move Through Senate*, WIRED (Nov. 6, 2009, 5:29 PM), https://www.wired.com/2009/11/breach-laws/ (noting proposed bills would set standards for protecting sensitive personal identifying information and impose civil penalties for those violating them); Ifrah PLLC, *The Data Breach Legal Limbo on Consumers' Ability to Sue Hacked Companies*, FTC BEAT (Jan. 16, 2018), https://www.jdsupra.com/legalnews/the-data-breach-legal-limbo-on-62346/ (noting Senator Leahy is advocating for data security legislation);

[34] S. 1490.

[35] *Id*. § 2.

[36] Louise Matsakis, *Uber 'Surprised' by Totally Unsurprising Pennsylvania Data Breach Lawsuit*, WIRED (Mar. 5, 2018, 5:52 PM), https://www.wired.com/story/uber-pennsylvania-data-breach-lawsuit/.

[37] *See id.* (noting that forty-eight states—excluding South Dakota and Alabama—mandate disclosure of data breaches and regulate when disclosure is triggered); 201 MASS. CODE REGS. 17.03(1), (2)(b) (2018) (mandating that any person who owns or licenses personal information about a state resident to have a comprehensive security program designed with administrative, technical, and physical safeguards); *cf.* COLO. REV. STAT. § 6-1-713(1) (2017) (requiring every public and private entity in the state to develop a policy for destroying or disposing of paper documents containing personal identifying information).

[38] Data Privacy Act of 2012, Rep. Act No. 10173, (Aug. 15, 2012) (Phil.).

[39] Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. I-3 (European Convention of Human Rights recognizes the right to privacy as fundamental; *accord* U.N. Global Pulse, *Data Privacy, Ethics and Protection: Guidance Notice on Big Data for Achievement of the 2030 Agenda*, U.N. Dev. Grp. 2–3 (noting the right to privacy is enshrined in the Universal Declaration of Human Rights); *see also* CAL. CONST. art. I, § 1 (guaranteeing the right to privacy).

[40] CAL. CIV. CODE § 1798.82(a) (2018). For a discussion of the benefits of disclosure laws, see Sasha Romanosky et al., *Do Data Breach Disclosure Laws Reduce Identity Theft?*, 30 J. POL'Y ANALYSIS & MGMT. 256, 281 (2011) (noting disclosure laws reduce identity theft by 6.1%).

[41] Data Privacy Act of 2012, ch. V, § 20(b).

[42] *Id.* at ch. V, § 20(c)(4).

[43] *Id.* at ch. V, § 20(f).

[44] *Id.* at ch. IV, § 16(e).

[45] *See* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737 (2018). *Contra* Louise Matsakis, *Uber 'Surprised' by Totally Unsurprising Pennsylvania Data Breach Lawsuit*, WIRED (Mar. 5, 2018, 5:52 PM), https://www.wired.com/story/uber-pennsylvania-data-breach-lawsuit/ ("I would be skeptical . . . that a unified data security protection law [would] . . . provide . . . better data protection . . . [a] movement to have a singled unified standard among the United States would be seen as an opportunity to water down those requirements.").

[46] *Compare* Brief of Chamber of Commerce of the United States of America as Amicus Curiae Supporting Appellees, Attias v. CareFirst, Inc., 865 F.3d 620 (D.C. Cir. 2017) (No. 16-7108), 2017 WL 632533 at *8 (noting that a substantive or procedural violation with harm is

insufficient for standing) (citation omitted), *with* Brief of Electronic Privacy Information Center as Amicus Curiae Supporting Plaintiffs-Appellants, *In re* Supervalu, Inc. v. Supervalu, Inc., 870 F.3d 763 (8th Cir. 2017) (No. 16-2378, 16-2528), 2016 WL 4150897 at *28 ("[I]t is necessary only to allege that a legal injury has occurred.").

[47] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1550 (2016).

[48] *Id*. at 1547–48.

[49] *Id.* at 1549.

[50] Patrick J. Lorio, Note, *Access Denied: Data Breach Litigation, Article III Standing, and a Proposed Statutory Solution*, 51 COLUM. J.L. & SOC. PROBS. 79, 125 (2017) (citing *In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 639 (3d Cir. 2017)).

[51] Fero v. Excellus Health Plan, Inc., 236 F. Supp. 3d 735, 786 (W.D.N.Y. 2017).

[52] Whalen v. Michaels Stores, Inc., 689 Fed. App'x 89 (2d Cir. 2017) (unpublished summary order).

[53] 2d Cir. R. 32.1.1(a).

[54] *Fero*, 236 F. Supp. 3d at 753.

[55] *Id.*

[56] *Id.* at 754.

[57] *Id.* at 758.

[58] *Id.*

[59] *Compare* Attias v. CareFirst, Inc., 865 F.3d 620 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018), *and* Galaria v. Nationwide Mut. Ins. Co., 663 Fed. App'x 384 (6th Cir. 2016) (unpublished opinion), *and In re* Adobe Sys. Inc. Privacy Litig., 66 F. Supp. 3d 1197 (N.D. Cal. 2014), *and* Remijas v. Neiman Marcus Grp., 794 F.3d 688 (7th Cir. 2015), *with In re* Supervalu,

Inc. v. Supervalu, Inc., 870 F.3d 763 (8th Cir. 2017), *and* Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017).

[60] For an example of a model statute defining personally identifiable information, see CAL. CIV. CODE § 1798.80 (2018).

[61] *See generally* Data Privacy Act of 2012, Rep. Act No. 10173, ch. 5, § 20(a)–(c) (Aug. 15, 2012) (Phil.) (requiring entities handling personal data to institute reasonable security measures proportional to the data being handled).

[62] PONEMON INST., 2013 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS 19, fig. 9 (2013).

[63] *E.g.*, Google, Inc., 102 F.T.C. 3136 (2011), 2011 WL 5089551 (requiring Google to implement and maintain a comprehensive data security program including reasonable privacy controls, regular testing of those controls, privacy risk assessments, and independent reviews).

[64] *C.f.* S.M. Furnell & M.J. Warren, *Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium?*, 18 COMPUTERS & SECURITY 28, 33 (1999) (noting the US has established the National Infrastructure Protection Center to combat e-intrusions of critical infrastructure with inter-agency coordination among entities like the CIA and NASA).

[65] Ravi Sen & Sharad Borle, *Estimating the Contextual Risk of Data Breach: An Empirical Approach*, 32 J. MGMT. INFO. SYS. 314, 320 (2015).

[66] *Id.*

[67] See Louise Matsakis, *Uber 'Surprised' by Totally Unsurprising Pennsylvania Data Breach Lawsuit*, WIRED (Mar. 5, 2018, 5:52 PM), https://www.wired.com/story/uber-pennsylvania-data-breach-lawsuit/.

[68] *See* Nicole Hong, *For Consumers, Injury is Hard to Prove in Data-Breach Cases*, WALL ST. J. (June 26, 2016, 8:06PM), https://www.wsj.com/articles/for-consumers-injury-is-hard-to-prove-in-data-breach-cases-1466985988.

[69] *See* Adam Shell, *Equifax Data Breach Could Create Lifelong Identity Theft Threat*, USA TODAY (Sep. 9, 2017, 10:08 AM), https://www.usatoday.com/story/money/2017/09/09/equifax-data-breach-could-create-life-long-identity-theft-threat/646765001/ (noting that the breach of personal data can persist for years because information like Social Security numbers don't change unlike CC #s which can be cancelled quickly).

[70] Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 757–58 (2018).

[71] Privacy Act of 1974, 5 U.S.C. § 552(g)(5) (2016) (two year statute of limitations from the date on which the cause of action arises); 18 U.S.C. § 2710(c)(3) (2013) (two year statute of limitations for claims from date complained of or of date of discovery).

[72] Julie Brill, Comm'r, Fed. Trade Comm'n, Back to the Future: Meeting Privacy Challenges Through a Strong Transatlantic Relationship, Remarks Before the 6th Annual Privacy and Data Protection Conference at *5 (Dec. 10, 2015). *See generally* John Biglow, Note and Comment, *It Stands to Reason: An Argument for Article III Standing Based on the Threat of Future Harm in Data Breach Litigation*, 17 MINN. J.L. SCI. & TECH. 943, 975 (2016) ("[T]he FTC . . . remains a poor avenue for most data breach victims seeking compensation."). *But c.f.* Amanda Bronstad, *Regulators, Not Class Actions, Could Drive Legal Response to Uber Data Breach*, RECORDER (Nov. 29, 2017, 8:23 PM), https://www.law.com/therecorder/sites/therecorder/2017/11/29/regulators-not-class-actions-

could-drive-legal-response-to-uber-data-breach/ (arguing government regulators are better poised than class actions to hold companies accountable).

[73] *E.g.*, FED. TRADE COMM'N, THE EQUIFAX DATA BREACH: WHAT TO DO (2017), https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do.

[74] *Id.*

[75] *See* Fero v. Excellus Health Plan, Inc., 236 F. Supp. 3d 735, 744 (W.D.N.Y. 2017) ("Defendants offered two years of free credit monitoring to adult victims of the breach.").

[76] *See* Solove, *supra* note 45, at 766 ("Although credit monitoring will detect fraud appearing on a person's credit report, not all fraud will be documented in a victim's credit report.").

[77] *See* Shell, *supra* note 69.

[78] For example, see Claire Wilka, Note, *The Effects of* Clapper v. Amnesty International USA: *An Improper Tightening of the Requirement for Article III Standing in Medical Data Breach Litigation*, 49 CREIGHTON 467, 489 (2016) ("[M]edical identity theft following a medical data breach has cascading, dangerous effects.").

[79] The median loss from identity theft in 2012 was $300. *See* Solove, *supra* note 45, at 757.

[80] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 414 n.5 (2013).

[81] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1550 (2016)

[82] *Id.* at 1547–48.

[83] *Spokeo*, 136 S. Ct. at 1548–49.

[84] *Id.* at 1549.

[85] *See* Lorio, *supra* note 50, at 125.

[86] *Spokeo*, 136 S. Ct. at 1545.