South Carolina Law Review

Volume 67
Issue 3 *2016 South Carolina Law Review Symposium*

Article 6

Spring 2016

Current Developments in Data Breach Litigation: Article III Standing after Clapper

David W. Opderbeck
Seton Hall University Law School

Follow this and additional works at: https://scholarcommons.sc.edu/sclr

 Part of the Law Commons

Recommended Citation

Opderbeck, David W. (2016) "Current Developments in Data Breach Litigation: Article III Standing after Clapper," *South Carolina Law Review*: Vol. 67 : Iss. 3 , Article 6.
Available at: https://scholarcommons.sc.edu/sclr/vol67/iss3/6

This Article is brought to you by the Law Reviews and Journals at Scholar Commons. It has been accepted for inclusion in South Carolina Law Review by an authorized editor of Scholar Commons. For more information, please contact dillarda@mailbox.sc.edu.

CURRENT DEVELOPMENTS IN DATA BREACH LITIGATION: ARTICLE III STANDING AFTER *CLAPPER*

David W. Opderbeck*

I. INTRODUCTION

After the 9/11 attacks, Congress passed the USA Patriot Act, which included amendments to the Foreign Intelligence Security Act of 1978 (FISA).[1] These amendments ultimately facilitated mass Internet surveillance by the U.S. National Security Agency (NSA).[2] FISA was a statute designed to place limits on U.S. foreign intelligence activities after abuses during the Cold War and Vietnam War, including covert assassinations of foreign political leaders by the CIA.[3]

It is not surprising then, that after government contractor Edward Snowden disclosed classified documents that exposed the scope of the NSA's Internet surveillance, civil liberties and other groups filed civil claims that ultimately reached the U.S. Supreme Court.[4] What is perhaps surprising is that the Court's

---

*Professor of Law, Seton Hall University Law School, and Director, Gibbons Institute of Law, Science & Technology.

1. U.S. Patriot Act of 2001, Pub. L. No. 107–56, 115 Stat. 272 (2001); David W. Opderbeck, *Cybersecurity and Executive Power*, 89 WASH. U. L. REV. 795, 822–26 (2012) (citations omitted).

2. *See* Opderbeck, *supra* note 1, at 826.

3. *See* 50 U.S.C. §§ 1801–1885(c) (2012); Opderbeck, *supra* note 1, at 809–10 (citing S.413, 112th Cong. § 249 (a)(6)(c)–(d)).

4. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013).

Published by Scholar Commons, 2016

decision in that case has become one of the hottest flashpoints in legal battles over liability for consumer data breaches.

Data breaches are an enormous economic problem, costing the U.S. economy billions, if not trillions, of dollars each year.[5] Most of the data breach litigation reported to date has arisen in the wake of large scale retail breaches, such as those involving Target and Home Depot.[6] The hackers in such cases are after the credit card data that is read at the point of sale from the magnetic strips or computer chips on consumer credit cards.[7] This data usually is packaged and sold on the dark web to other criminals who use it to make fraudulent purchases of goods and services that either are consumed directly or, more often, are fenced through online retail and auction websites.[8]

Consumer credit card networks are structured through a web of contractual relationships involving at least five parties: (1) the card brand (Visa, MasterCard, American Express, or Discover); (2) the cardholder; (3) an issuing bank, which issues the card to the cardholder; (4) the merchant; and (5) an acquiring bank, which processes the merchant's card transactions.[9] The card brand issues an extensive set of regulations that govern the scope of these contractual relationships.[10] Among those regulations is a "zero liability" policy through which the issuing bank must agree to reimburse cardholders for any fraudulent charges.[11] Therefore, any charges to a cardholder's account resulting from a retail data breach will be reimbursed by the issuing bank.[12] Depending on the circumstances of the breach, the issuing bank may then pursue indemnification claims against the merchant of the acquiring bank under the card network agreement.[13]

---

5. *See* David W. Opderbeck, *Cybersecurity, Data Breaches, and the Economic Loss Doctrine in the Payment Card Industry*, 75 MD. L. REV. (forthcoming 2016) (citing Juniper Research, *Cybercrime and the Internet of Threats* (May 2015), https://www.juniperresearch.com/document-library/white-papers/cybercrime-the-internet-of-threats [hereinafter *Data Breaches*]).

6. For a discussion of the Target breach, *see* Data Breach FAQ, TARGET, https://corporate.target.com/about/shopping-experience/payment-card-issue-faq (last visited Mar. 16, 2016). For a discussion of the Home Depot breach, *see* Robin Sidel, *Home Depot's 56 Million Card Breach Bigger than Target's*, WALL STREET J. (Sept. 18, 2014), http://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571.

7. *See, e.g.*, *Data Security*, NATIONAL RETAIL FEDERATION, https://nrf.com/advocacy/policy-agenda/data-security (last visited Mar. 16, 2016).

8. See *Stolen Target Cards and the Black Market: How the Digital Underground Works*, TRIPWIRE (Dec. 21, 2013), http://www.tripwire.com/state-of-security/vulnerability-management/how-stolen-target-credit-cards-are-used-on-the-black-market/.

9. *See Data Breaches*, *supra*, note 5.

10. *See id.*

11. *See id.*

12. *See id.* (citing VISA CORE RULES AND VISA PRODUCT AND SERVICE RULES, VISA § 1.10.7.1, 1.11.2 (Apr. 15, 2015), https://usa.visa.com/dam/VCOM/download/about-visa/15-April-2015-Visa-Rules-Public.pdf).

13. *See id.*

Since card holders are fully reimbursed for fraudulent charges, claims by card holders against the party directly responsible for the breach face challenge on Article III standing grounds.[14] This is where the Supreme Court's decision resulting from the Snowden disclosures comes into play.

II. THE INFLUENCE OF *CLAPPER* IN CONSUMER CREDIT CARD BREACH CASES

A. The Clapper Decision

The standing analysis in recent data breach cases has focused on the requirements for Article III standing discussed in the Supreme Court's *Clapper v. Amnesty International* opinion.[15] *Clapper* involved a challenge to the National Security Agency's bulk metadata collection program under FISA.[16] The plaintiffs, including a number of attorneys and human rights, labor, legal, and media organizations, alleged that the NSA surveillance program violated their constitutional and civil rights.[17] None of the plaintiffs, however, could prove that the NSA had collected information about any of their specific conversations, because the details of what was collected were classified.[18] Instead, the plaintiffs suggested that the possibility or likelihood that they could be subject to surveillance had a chilling effect on their ability to "locate witnesses, cultivate sources, obtain information, and communicate confidential information to their clients."[19]

In a 5-4 opinion written by Justice Alito, the Court held that the plaintiffs lacked standing to challenge the NSA surveillance program.[20] According to the Court, "[t]o establish Article III standing, an injury must be 'concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.'"[21] To be imminent, the Court noted, the "threatened injury must by *certainly impending*" and "[a]llegations of *possible* future injury" are insufficient.[22] Justice Alito also noted the particular separation of powers concerns arising from judicial review of Executive branch decisions about intelligence gathering and foreign affairs.[23]

---

14. *Id.* (citing Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1155 (2013)).
15. *Clapper*, 133 S. Ct. at 1146–55.
16. *See id.* at 1144.
17. *Id.* at 1145–46.
18. *Id.* at 1148–49.
19. *Id.* at 1145.
20. *Id.* at 1142, 1155.
21. *Id.* at 1147 (quoting Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 149 (2010)).
22. *Id.* (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)) (emphasis in original).
23. *Id.* at 1146 (citing Summers v. Earth Island Institute, 555 U.S. 488, 493 (2009)); DaimlerChrysler Corp. v. Cuno, 547 U.S. 332, 341–342 (2006); Raines v. Byrd, 521 U.S. 811 at 818–820 (1997); Valley Forge Christian College v. Americans United for Separation of Church and State, Inc., 454 U.S. 464, 471–474 (1982); Schlesinger v. Reservists Comm. to Stop the War, 418 U.S. 208, 221–222 (1974)).

The Court held that the plaintiffs' claimed harms were not immanent because the claims rested on a

> highly speculative fear that (1) the Government will decide to target the communications of non-U.S. persons with whom they communicate; (2) in doing so, the Government will choose to invoke its authority under [the FISA statute] rather than utilizing another method of surveillance; (3) the Article III judges who serve on the Foreign Intelligence Surveillance Court will conclude that the Government's proposed surveillance procedures satisfy [the FISA statute's] many safeguards and are consistent with the Fourth Amendment; (4) the Government will succeed in intercepting the communications of respondents' contacts; and (5) respondents will be parties to the particular communications that the Government intercepts.[24]

The plaintiffs also claimed that they were compelled to take "costly and burdensome measures to protect the confidentiality of their communications" in light of the possibility of NSA surveillance.[25] The Second Circuit had held that these kinds of costs could support Article III standing so long as the feared harm was not "fanciful, paranoid, or otherwise unreasonable."[26] Justice Alito stated that this standard "improperly waters down the fundamental requirements of Article III."[27] According to Justice Alito, "respondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."[28] Otherwise, Justice Alito suggested, "an enterprising plaintiff would be able to secure a lower standard for Article III standing simply by making an expenditure based on a nonparanoid fear."[29] Therefore, the Court held that the plaintiffs lacked Article III standing.[30]

Justice Breyer wrote a dissenting opinion, joined by Justices Ginsburg, Sotomayor and Kagan.[31] Based on the evidence provided by the plaintiffs about their work and the history of the NSA surveillance program, Justice Breyer was convinced there was "a very high likelihood" that the government would intercept some of plaintiffs' communications.[32] Justice Breyer further argued that the phrase "certainly impending" used by the majority was used more flexibly in the Court's prior precedents.[33] "Taken together," Justice Breyer

---

24. *Id.* at 1148.
25. *Id.* at 1151.
26. *Id.* (Amnesty Int'l USA v. Clapper, 638 F.3d 118, 134 (2d Cir. 2011)).
27. *Id.*
28. *Id.*
29. *Id.*
30. *Id.* at 1155.
31. *Id.*
32. *Id.* at 1157.
33. *Id.* at 1160–61.

stated, "the case law uses the word 'certainly' as if it emphasizes, rather than literally defines, the immediately following term 'impending.'"[34] In particular, according to Justice Breyer, "*probabilistic*" injuries have often sufficed to confer standing.[35] This must be the case, Justice Breyer argued—"[h]ow could the law be otherwise?"—because many claims seeking injunctive or other immediate relief necessarily are based on less than 100 percent certainty.[36]

B. Clapper in the Retail Credit Card Data Breach Setting

The holding and majority opinion in *Clapper* have been invoked by district courts in a number of recent prominent data breach cases to deny Article III standing to consumer cardholders and other plaintiffs. These include litigation arising from data breaches involving Michael's Stores, SuperValu supermarkets, Advocate Health (an Illinois-based hospital-physician network), Zappos.com, eBay, Paytime (a payroll service provider), Nationwide Mutual Insurance Company, and Trustwave Holdings (a data security company).[37]

The *SuperValue* case is typical of this group of cases in its evaluation of potential harm from a data breach.[38] The plaintiffs claimed that, even if their credit card information had not been misused, there was a substantial likelihood of misuse in the future. According to the *SuperValue* court, this harm is speculative because it is unclear whether the hacker "(1) read, copied, and understood [Plaintiffs'] personal information; (2) intends to commit future criminal acts by misusing the information; and (3) is able to use such information to the detriment of [Plaintiffs] by making unauthorized transactions in [Plaintiffs'] names."[39] This litany of uncertainties obviously was designed to parallel Justice Alito's skeptical list of events that would need to ensue for the *Clapper* plaintiffs to suffer any concrete harm.[40]

Not all courts, however, have reached the same conclusion. Courts addressing claims arising from data breaches involving Adobe, Uber, Sony, and

---

34. *Id.* at 1161.
35. *Id.* at 1162.
36. *Id.*
37. *See* Whalen v. Michael's Stores, No. 14-CV-70006(JS)(ARL), 2015 WL 9462108 (E.D.N.Y 2015); In re: SuperValue, Inc. Customer Data Security Breach Litigation, No. 14-MD-2586(ADM/TNL), 2016 WL 81792 (D. Minn. 2016); Maglio v. Advocate Health and Hospitals Corp., 40 N.E.3d 746 (Ill. App. 2d Dist. 2015); *In re*: Zappos.com, Inc., 108 F. Supp.3d 949 (D. Nev. 2015); Green v. eBay, Inc., No. 14-1688, 2015 WL 2066531 (E.D. La. 2015); Storm v. Paytime, Inc., 90 F. Supp.3d 359 (M.D. Pa. 2015); Galeria v. Nationwide Mutual Ins. Co., 998 F. Supp.2d 646 (S.D. Ohio 2014); Strautins v. Trustwave Holdings, Inc., 27 F. Supp.3d 871 (N.D. Ill. 2014). It should be noted that Strautins likely would have been decided differently after the Seventh Circuit's decision in Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688 (7th Cir. 2015). *See infra* note 24 and accompanying text.
38. *See In re: SuperValue*, 2016 WL 81792, at *1.
39. *Id.* at *5 (quoting Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011)).
40. *Cf. Clapper*, 133 S. Ct. at 1147–49.

Neiman Marcus have found sufficient grounds for standing despite *Clapper*.[41] Most notably, the Seventh Circuit—the only federal appellate court to decide the issue of standing in a date breach case after *Clapper*—refused to dismiss a plaintiffs' putative class action in *Remijas v. Neiman Marcus Group* on standing grounds.[42]

The plaintiffs in *Remijas*, like plaintiffs in many other data breach cases, claimed damages including

> 1) lost time and money resolving the fraudulent charges, 2) lost time and money protecting themselves against future identity theft, 3) the financial loss of buying items at Neiman Marcus that they would not have purchased had they known of the store's careless approach to cybersecurity, and 4) lost control over the value of their personal information.[43]

The Seventh Circuit concluded that plaintiffs whose credit card information was improperly used as a result of the breach suffered ascertainable damages, even though the card issuer reimbursed the charges and Neiman Marcus provided free credit monitoring insurance, noting that "there are identifiable costs associated with the process of sorting things out."[44] As to plaintiffs whose information had not yet been misused, the court concluded that "*Clapper* does not, as the district court thought, foreclose any use whatsoever of future injuries to support Article III standing."[45] According to the Seventh Circuit, *Clapper* was decided under the same "substantial risk" standard that has always governed standing in claims for possible future harms.[46]

The Seventh Circuit had little trouble finding standing for the *Remijas* plaintiffs under that substantial risk standard because the hackers clearly intended to use the stolen information to make fraudulent purchases.[47] As the court asked rhetorically, "[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'

---

41. *In re Adobe Sys., Inc. Privacy Litig.* 66 F. Supp. 3d 1197, 1213 (N.D. Cal. 2014) (stating that "Clapper did not change the law governing Article III standing. The Supreme Court did not overrule any precedent, nor did it reformulate the familiar standing requirements of injury-in-fact, causation, and redressability."); Antman v. Uber Techs., Inc., No. 3:15-CV-01175-LB, 2015 WL 6123054, at *10 (N.D. Cal. 2015) (stating that "[t]he court thinks that a credible threat of immediate identity theft based on stolen data is sufficiently different than the speculative harm articulated in *Clapper*"); Corona v. Sony Pictures Entertainment, Inc., 2015 WL 3916744, *3 (C.D. Cal. 2015); Remijas 794 F.3d 688, 690.

42. *Remijas*, 794 F.3d at 692–96.

43. *Id.* at 692.

44. *Id.*

45. *Id.*

46. *Id.* at 693.

47. *Id.*

identities."[48] Concerning mitigation expenses, such as extra identity theft monitoring insurance purchased by some plaintiffs, the court noted that Neiman Marcus' offer of one year of free credit monitoring was "telling" and that it was "unlikely that it did so because the risk is so ephemeral that it can safely be disregarded."[49]

The court found "dubious" plaintiffs' other damage claims asserting that plaintiffs would not have shopped at Neiman Marcus had they known of the store's lax security policies, but held the credit remediation and monitoring claims were sufficient to survive dismissal based on standing.[50] Finally, the court concluded that plaintiffs had sufficiently demonstrated causation between the Neiman Marcus breach and the claimed harms and that the claims for costs associated with repairing and monitoring credit were redressable even if fraudulent charges themselves were reimbursed by the issuing banks.[51]

C. Clapper and the Internet of Things

The Internet of Things (IoT) refers to physical devices that are connected to the Internet, aside from desktop computers, laptops, tablets, or smart phones.[52] While the IoT offers great promise in fields as diverse as healthcare, transportation, consumer products, and even food, it opens vast new potential for malicious hacking.[53] There have been very few cases arising from hacking of IoT devices, but one recent case suggests that *Clapper* will present hurdles in that domain as well as in consumer credit card cases.

In *Cahen v. Toyota*, plaintiffs filed a putative class action in the U.S. District Court for the Northern District of California against Toyota, Ford, and General Motors, alleging that electronic control units in cars made by these manufacturers can be remotely hacked.[54] Plaintiffs claim that software that allows various control units to communicate with each other can be accessed through Bluetooth connections that enable consumers to link their cell phones with the cars.[55] The plaintiffs' Complaint refers to a journalist's report in a popular media outlet about a test hack of one of the vehicles in 2011: "As I drove

---

48. *Id.*
49. *Id.* at 694.
50. *Id.*
51. *Id.* at 696–97.
52. *See, e.g.*, *Smart Products, Smart Makers*, THE ECONOMIST (November 21, 2015), http://www.economist.com/news/business-and-finance/21678748-old-form-capitalism-based-built-obsolescence-giving-way-new-one-which (discussing how "mundane things [such] as fizzy drinks and washing powder" are becoming "smart").
53. *See, e.g.*, *The Internet of Things (To Be Hacked)*, THE ECONOMIST (July 12, 2014), http://www.economist.com/news/leaders/21606829-hooking-up-gadgets-web-promises-huge-benefits-security-must-not-be (discussing how greater connectivity "gives malicious hackers an easy way to burrow deeper into people's lives").
54. Cahen v. Toyota Motor Corp., F.3d, 2015 WL 7566806, * 1 (N.D. Cal. 2015).
55. *Id.* at *1.

to the top of the parking lot ramp, the car's engine suddenly shut off, and I started to roll backward . . . This wasn't some glitch triggered by a defective ignition switch, but rather an orchestrated attack performed wirelessly, from the other side of the parking lot, by a security researcher."[56] The plaintiffs did not allege, however, that any of their own vehicles had been hacked.[57] The court found these circumstances analogous to "product liability cases where there has been no actual injury and the injury in fact theory rests only on an unproven risk of future harm" and dismissed the claims for lack of standing under *Clapper* and related authority.[58]

III. CONCLUSION: LOOKING AHEAD

The pace of data breach litigation filings shows no signs of abating.[59] A recent docket search limited to December 2015 through February 2016 revealed putative consumer class actions filed in federal courts around the U.S. arising from data breaches involving Experian (a financial credit reporting company), Scottrade (an online stock broker), Ashley Madison (an adult dating site), Hyatt Hotels, Lime Crime (a makeup retailer), Wendy's (a restaurant chain), and Web.com (a third party web design and hosting company).[60] Retailers and other companies that hold customer data can continue to expect consumer class action

---

56. *Id.* at *2 (quoting Plaintiffs' First Amended Complaint). Although it is not clear from the court's opinion, the reference seems to refer to a 2014 article and video on the computer and hacker Website "Motherboard." *See* Xavier Aaronson, *We Drove a Car While it Was Being Hacked*, MOTHERBOARD (May 29, 2014, 1:05 PM) http://motherboard.vice.com/read/we-drove-a-car-while-it-was-being-hacked.

57. *Cahen*, F.3d, 2015 WL 7566806, at *1.

58. *Id.* at *10. The court also relied on U.S. Resort and Hotel Management, Inc. v. Onity, Inc., 2014 WL 3748639, *1 (D. Minn. 2014), which involved an electronic door locking system that was susceptible to hacking using a physical device that could read the code in the lock's memory. Onity is not an IoT case because there was no allegation that the locks were Internet-enabled and accessible to remote hackers. Nevertheless, Onity is another example of a "hacking" case concerning physical computer embedded-devices in which a court found a lack of standing absent a showing of actual injury.

59. *See, e.g.*, *The Internet of Things (To Be Hacked)*, *supra* note 53 (discussing how in 2013 "more than 800m digital records, such as credit- and debit-card details, were pinched or lost, more than three times as many" the year before and an increase in connectivity over the years will give hackers "an easy way to burrow deeper into people's lives").

60. Pierpont v. Experian Information Solutions, No. 8:15-CV-01965 (C.D. Cal.), Complaint filed November 24, 2015 (multiple consolidated cases); Martin v. Scottrade, No. 8:15-CV-02791 (E.D. Mo.), Complaint filed December 4, 2015 in M.D. Fla., transferred to E.D. Mo.; Lee v. Avid Life Media (Ashley Madison), No. 2:15-CV-09475 (C.D. Cal.), Complaint filed December 8, 2015; Affinity Gaming v. Trustwave Holdings, No. 2:15-CV-02464 (D. Nev.), Complaint filed December 24, 2015; Taylor v. Hyatt Hotels, No. 1:16-CV-00702 (N.D. Ill.), Complaint filed January 18, 2016; Koenig v. Lime Crime, Inc., No. 2:16-CV-00503 (C.D. Cal.), Complaint filed January 21, 2016; Torres v. The Wendy's Company, No. 6:16-cv-210-Orl-18DAB (M.D. Fla.), Complaint filed February 8, 2016; Mohorne v. Web.com Group, Inc., No. 5:16-cv-00190 (C.D. Cal.), Complaint filed February 2, 2016;

litigation after notifying customers of breaches under state law.[61] Although many of these cases likely will be dismissed by trial courts for lack of Article III standing under *Clapper*, other courts may apply the Seventh Circuit's *Remijas* analysis and allow some claims to proceed. As a result, it is likely that other circuit courts of appeal will decide the issue of standing in the credit card breach context. While this could conceivably result in a circuit split, it seems unlikely that the Supreme Court would take another Article III standing case in this area, particularly when the commercial interests involved can manage the risks through contracts and insurance.

Between *SuperValue* and *Remijas*, on the question of whether future misuse of credit card information is likely, the *Remijas* analysis clearly makes more sense. Hackers steal credit card information to use it and profit from it, and if they know how to steal it, they know how to use it. This is a far cry from the claims in *Clapper*, which involved possible government surveillance or use of stored metadata that had not yet taken place and that would likely require some kind of judicial authorization or action under and existing FISA court order. Nevertheless, a more fundamental question raised by Justice Alito in *Clapper*—that of the separation of powers—still lurks beneath the surface of all mass consumer data breach cases. The question is whether a "mass tort" litigation model is an effective way to manage the systemic risks of data breaches or whether the legislative branch should act.

In addition to consumer litigation, large scale consumer data breaches likely will continue to provoke disputes among the commercial parties in the consumer credit chain: the issuing and acquiring banks, the merchant, and the card issuer. Some of these disputes have already resulted in settlement agreements.[62] The role of cyber risk insurance in both commercial and consumer data breach compliance, disputes and settlements remains at an early stage.[63]

The rapid growth of the IoT also will certainly foster additional waves of litigation as large scale breaches of connected consumer devices are discovered and reported. The unique circumstances of the consumer credit card industry, in which consumers are always reimbursed for fraudulent charges because of the issuing bank agreements and the risks are spread among various commercial parties by contract, do not usually obtain in most of the IoT world. The IoT context often is much more akin to more familiar product liability and consumer warranty settings. Courts will continue to grapple with the question raised in

---

61. Most states require individual notification to consumers after discovery of a data breach. *See Security Breach Notification Laws*, NAT'L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last visited Jan. 4, 2016).

62. *See* "Target Reaches Another Data Breach Settlement," WALL STREET J. (December 2, 2015), http://www.wsj.com/articles/target-reaches-another-data-breach-settlement-1449085790; Tracy Kitten, *Will Banks Reject Home Depot Settlement*, BANKINFO SECURITY (December 7, 2015), http://www.bankinfosecurity.com/home-depot-a-8729/op-1.

63. *See* NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS, *Cybersecurity* (Jan. 25, 2016), http://www.naic.org/cipr_topics/topic_cyber_risk.htm; *Data Breaches*, *supra* note 5.

Cahen: whether a civil claim for damages is only cognizable after someone is actually injured or killed. The IoT may stretch our usual understanding of the boundaries between contracts (warranties and limitations of liability) and torts (negligence and product liability), often expressed in terms of the economic loss doctrine, beyond the breaking point.[64] Since a large scale legislative framework does not seem politically likely, these issues are certain to occupy a significant portion of court dockets for years to come.

64. *Cf. Data Breaches*, *supra* note 5.