Richmond Journal of Law and Technology

Volume 21 | Issue 1 Article 4

2014

Clapper v. Amnesty International and Data Privacy Litigation: Is a Change to the Law "Certainly Impending"?

John L. Jacobus

Benjamin B. Watson

CLAPPER V. AMNESTY INTERNATIONAL AND DATA PRIVACY LITIGATION: IS A CHANGE TO THE LAW "CERTAINLY IMPENDING"?

John L. Jacobus & Benjamin B. Watson*

Cite as: John L. Jacobus & Benjamin B. Watson, *Clapper v. Amnesty International and Data Privacy Litigation: Is a Change to the Law "Certainly Impending"?*, 21 RICH. J.L. & TECH. 3 (2014), http://jolt.richmond.edu/v21i1/article3.pdf.

I. INTRODUCTION

[1] On December 19, 2013, the retailer Target announced that unauthorized third parties had gained access to its customer payment information.[1] While Target originally estimated that the security breach affected 40 million of its customers, a subsequent investigation revealed that anywhere from 70 to 110 million people—almost one in three Americans—may have had their sensitive payment information stolen.[2] In response, the retailer offered free credit monitoring services and assured affected customers that they would not be responsible for fraudulent charges made with their payment information.[3] But these actions could not placate all customers impacted by the breach; less than a month after

* John L. Jacobus is a Partner in the Washington, D.C. office of Steptoe & Johnson LLP. Benjamin B. Watson is an Associate in the Washington, D.C. office of Steptoe & Johnson LLP.

[1] Elizabeth A. Harris & Nicole Perlroth, *For Target, the Breach Numbers Grow*, N.Y. TIMES, Jan. 11, 2014, at B1, *available at* http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html, *archived at* http://perma.cc/FV24-SJTP.

[2] *Id.*

[3] Joel Schectman, *Target Faces Nearly 70 Lawsuits Over Breach*, WALL ST. J. (Jan. 15, 2014 6:00 AM), http://blogs.wsj.com/riskandcompliance/2014/01/15/target-faces-nearly-70-lawsuits-over-breach/, *archived at* http://perma.cc/5FWA-JSNC.

its first announcement, Target faced sixty-eight class action lawsuits in twenty-one states and the District of Columbia.[4]

[2] Though of exceptional size, the Target data breach is just one of many recent incidents where businesses have lost or exposed the sensitive personal information—often referred to as personally identifiable information, or "PII"—of their customers. The frequency and extent of these breaches have grown considerably over the past decade. One organization estimates that the number of reported data-loss incidents has increased from 157 in 2005 to 1,467 in 2013.[5] According to another organization, since 2005 over 4,455 data breaches have resulted in the exposure of over 620 million records.[6] What is more, this increase in data breaches has occurred at the same time as advances in technology have enabled businesses to track, collect, and store information about their customers with unprecedented scale and sophistication.[7]

[3] The dramatic increase in both data breaches and data collection has led to a concomitant increase in litigation.[8] In particular, the past decade

[4] *Id.*

[5] *See Data Loss Statistics*, DATALOSSDB, http://datalossdb.org/statistics (last visited Sept. 11, 2014), *archived at* http://perma.cc/TN3R-FYC3.

[6] *See Data Breaches*, IDENTITY THEFT RESOURCE CENTER, http://www.idtheftcenter.org/id-theft/data-breaches.html (last visited Sept. 11, 2014), *archived at* http://perma.cc/BP93-BMTL.

[7] *See, e.g.*, Scott Thurm & Yukari Iwatani Kane, *Your Apps Are Watching You*, WALL. ST. J. (Dec. 18, 2010, 12:01AM), http://online.wsj.com/article/SB10001424052748704368004576027751867039730.html (documenting how third-party applications on smartphones can transmit information about the phone's user, including age, gender, and other personal details), *archived at* http://perma.cc/M3UP-643W.

[8] *See* Dana Post & Anupreet Singh Amole, *Anticipate Litigation After Data Breaches*, LAW TECH. NEWS (Aug. 25, 2014), http://www.lawtechnologynews.com/id=1202667090150/Anticipate-Litigation-After-Data-Breaches, *archived at* http://perma.cc/HHY6-5LBZ.

has witnessed the rise of two different types of lawsuits. First, customers have begun suing companies that lose their PII in data breaches, often alleging that the breach has caused them an increased risk of falling victim to identity theft. Second, individuals have filed lawsuits challenging how businesses collect, track, and share PII. Plaintiffs in these cases, often users of social networking websites or smart devices, have alleged that the defendant businesses gathered, without consent, their contact information, web browsing history, and even physical location.

[4] Plaintiffs in both types of lawsuits, however, have frequently encountered a common hurdle: the requirement under Article III of the United States Constitution that a plaintiff have "standing" to sue.[9] In particular, some courts have been reluctant to conclude that a plaintiff who has had her PII either collected or lost has experienced the type of concrete injury—often referred to as "injury-in-fact"—that grants her access to the judicial system. Plaintiffs have responded by advancing a number of different theories for why they have suffered injury-in-fact. Plaintiffs in data breach cases have most commonly argued that their injury arises from an increased risk of identity theft.[10] Plaintiffs in data collection cases, meanwhile, have argued that their PII has intrinsic economic value or that the collection of their PII breached express or implied contracts between them and the defendant.[11] These arguments for injury-in-fact have divided federal courts. Commentators, meanwhile, have suggested different ways to address this legal issue.[12]

[9] *See* U.S. CONST. art. III, § 2.

[10] *See, e.g.*, *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig. 996 F. Supp. 2d 942, 970 (S.D. Cal. 2014).

[11] *See, e.g.*, *In re* Jetblue Airways Corp. Privacy Litig., 379 F. Supp. 299, 326 (E.D.N.Y. 2005); Katz v. Pershing, LLC, 672 F.3d 64, 74 (1st Cir. 2012).

[12] *See, e.g.*, Patricia Cave, Comment, *Giving Consumers a Leg to Stand on: Finding Plaintiffs a Legislative Solution to the Barrier from Federal Courts in Data Security Breach Suits*, 62 CATH. U. L. REV. 765, 789 (2013); Miles L. Galbraith, Comment, *Identity Crisis: Seeking a Unified Approach to Plaintiff Standing for Data Security Breaches of Sensitive Personal Information*, 62 AM. U. L. REV. 1365, 1399 (2013); Vincent R. Johnson, *Credit-Monitoring Damages in Cybersecurity Tort Litigation*, 19

[5] Although the Supreme Court has yet to weigh in on the issue of standing to challenge data collection and storage by private businesses, it recently addressed the standing of litigants to challenge data collection by the government. In *Clapper v. Amnesty International, USA*, the Supreme Court held that plaintiffs who sought to bring a constitutional challenge to a federal foreign surveillance law lacked standing because they had failed to allege that the law created a sufficiently "impending" risk of future harm to them.[13] Many commentators quickly suggested that *Clapper*, although arising from the national security sphere, could be a potential game-changer for data privacy litigation.[14] But the few data breach decisions so far to address *Clapper* in detail have reached different conclusions about its impact on existing standing law.[15] Whether *Clapper* will produce a uniform approach to data privacy claims in lower courts remains to be seen.

[6] This article provides an overview of the various theories of standing that plaintiffs have advanced in data privacy cases and the success those theories have had in federal courts. It then considers what impact the Supreme Court's decision in *Clapper* may have for these theories going forward. Part I provides a summary of the Supreme Court's decisions on standing, and in particular those decisions that have addressed claims of injury premised on an increased risk of future harm. Part II catalogs the decisions in which courts have evaluated the Article III

GEO. MASON L. REV. 113, 144 (2011) ; James Graves, Comment, *"Medical" Monitoring for Non-Medical Harms: Evaluating the Reasonable Necessity of Measures to Avoid Identity Fraud After a Data Breach*, 16 RICH. J. L. & TECH. 2, ¶¶ 39–41, 51 (2009), http://jolt.richmond.edu/v16i1/article2.pdf.

[13] Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1143 (2013).

[14] *See, e.g.*, Alison Frankel, *How SCOTUS Wiretap Ruling Helps Internet Privacy Defendants*, REUTERS, Mar. 12, 2013, http://blogs.reuters.com/alison-frankel/2013/03/12/how-scotus-wiretap-ruling-helps-internet-privacy-defendants/, *archived at* http://perma.cc/H4UU-CX5J.

[15] *See infra* section IV.

standing of plaintiffs seeking damages for the collection, transfer, or disclosure of their PII. Part III evaluates the effect that *Clapper* has had on these cases so far, and explores what potential effects *Clapper* may have in the future. Part IV sets forth some tentative conclusions about what *Clapper* means for future data privacy litigation.

II. PROVING INJURY-IN-FACT UNDER ARTICLE III

[7] Article III of the Constitution permits federal courts to hear only "cases" or "controversies."[16] These two words are the basis for the legal doctrine known as Article III "standing": the idea that a plaintiff must demonstrate she has an actual, concrete interest at stake in her case and therefore may invoke the jurisdiction of a federal court.[17] Courts most often describe Article III standing as having three separate components: (1) injury, (2) causation, and (3) redressability. The Supreme Court has described these requirements as follows:

> First, the plaintiff must have suffered an "injury in fact"—an invasion of a legally protected interest which is (a) concrete and particularized, and (b) "actual or imminent, not 'conjectural' or 'hypothetical.'" Second, there must be a causal connection between the injury and the conduct complained of—the injury has to be "fairly . . . traceable to the challenged action of the defendant, and not . . . the result [of] the independent action of some third party not before the court." Third, it must be "likely," as opposed to merely "speculative," that the injury will be "redressed by a favorable decision."[18]

Establishing the first of these requirements—injury-in-fact—is often straightforward. If a plaintiff has suffered some sort of injury, be it

[16] U.S. CONST. art. III, § 2.

[17] *See* Lujan v. Defenders of Wildlife, 504 U.S. 555, 560–61 (1992).

[18] *Id.* (citation omitted).

monetary, physical, or even aesthetic, then she has suffered injury-in-fact. With respect to present injuries, standing problems typically arise only if the injury is a "generalized grievance" shared by a large number of people.[19] With respect to *future* injuries, however, the law of standing becomes more complex. The Supreme Court has decided a significant number of decisions on how likely an alleged future injury must be before it can support standing under Article III: in other words, whether an injury is, as the Court in *Lujan v. Defenders of Wildlife* described, "actual or imminent" or "conjectural or hypothetical."[20]

A. Standing and the Risk of Future Injury

[8] *Clapper* was not the first Supreme Court decision to consider when a risk of future harm is sufficiently probable to support Article III standing. Indeed, the Supreme Court has considered iterations of this question a number of times before. Below is a brief a summary of some of the Court's more notable decisions on the issue.

[9] Perhaps the Court's most influential case on the topic of future harm and injury-in-fact is *City of Los Angeles v. Lyons*.[21] The plaintiff in *Lyons* sued the City of Los Angeles after being stopped by Los Angeles police officers and subjected to what he alleged was an illegal chokehold.[22] He sought damages as well as an injunction preventing the Los Angeles Police Department from using the same chokehold in the future.[23] While the Supreme Court agreed that the plaintiff had standing to pursue damages for his past encounter with police, it held that he did not have standing to pursue injunctive relief because he had not

[19] *See id.* at 575.

[20] *Id.* at 560.

[21] City of Los Angeles v. Lyons, 461 U.S. 95 (1983).

[22] *Id.* at 97.

[23] *Id.* at 98.

demonstrated a "real and immediate threat" of being subjected to the chokehold again in the future.[24] For the plaintiff's alleged harm to be sufficiently "real" to support standing, the Court explained, would require the "incredible assertion" that (1) the plaintiff would be stopped by the police again, and (2) that either all police officers employed such a chokehold in every encounter or there was an official policy for them to do so.[25]

[10] The Supreme Court has addressed standing based on the risk of future harm a number of times since *Lyons*. In *Whitmore v. Arkansas*, the Court found no injury-in-fact for an Arkansas death row inmate who sought to intervene on behalf of another inmate who had been sentenced to death but had waived his right to appeal. [26] The plaintiff argued that he had standing because Arkansas' system of "comparative review" in death penalty cases meant that a favorable resolution of the second inmate's sentence could affect his own, though only if his current sentence was vacated in a habeas corpus proceeding and he was then retried, reconvicted, and re-sentenced.[27] The Court held that this chain of future events was "too speculative" to support standing.[28] It explained that "[a]llegations of possible future injury do not satisfy the requirements of Art. III," and that "[a] threatened injury must be 'certainly impending' to constitute injury in fact."[29]

[11] In *Friends of the Earth, Inc. v. Laidlaw Environmental Services (TOC), Inc.*, the Court held that a group of plaintiffs did have standing to

[24] *Id.* at 105.

[25] *Id.* at 106.

[26] Whitmore v. Arkansas, 495 U.S. 149, 151, 156–57 (1990).

[27] *Id.* at 156.

[28] *Id.* at 157.

[29] *Id.* at 158 (citation omitted).

seek declaratory and injunctive relief against the owners of a waste treatment plant that was allegedly discharging illegal amounts of mercury into a local river.[30] The plaintiffs had filed affidavits explaining how their fear of excessive mercury had limited their recreational use of the river.[31] The Court concluded that these "reasonable concerns" about pollution "directly affected [plaintiffs'] recreational, aesthetic, and economic interests" and therefore established injury-in-fact.[32] The Court distinguished the plaintiffs' declarations from declarations made by the plaintiffs in *Lujan*; the *Lujan* plaintiffs had failed to establish injury-in-fact, the Court explained, because they made "conditional" statements about how they would "some day" visit areas affected by challenged government action.[33] The Court distinguished *Lyons*, meanwhile, on the ground that the "unlawful conduct—discharging pollutants in excess of permit limits—was occurring at the time the complaint was filed."[34]

[12] The Court more recently found the risk of future harm to establish injury-in-fact in *Monsanto Co. v. Geertson Seed Farms*.[35] The plaintiffs in *Monsanto* were a group of conventional alfalfa farmers who had challenged a government decision to deregulate a variety of genetically engineered alfalfa.[36] The plaintiffs filed declarations stating that if the

[30] Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167, 175–76, 183, 189 (2000).

[31] *Id.* at 181-83.

[32] *Id.* at 184.

[33] *Id.* (citing Lujan v. Defenders of Wildlife, 504 U.S. 555, 564 (1992)).

[34] *Id.* at 184.

[35] Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 155 (2010).; *see also* Davis v. FEC, 554 U.S. 724, 734–35 (2008)(finding standing based on future harm); Mass. v. EPA, 549 U.S. 497, 521–23 (2007)(finding standing based on future harm). *But see* Summers v. Earth Island Inst., 555 U.S. 488, 495–97 (2009) (rejecting argument of standing based on future harm).

[36] *Monsanto*, 561 U.S. at 139.

deregulation proceeded their crops would be close enough to farms with the genetically engineered alfalfa that cross-pollination between the two varieties could occur.[37] The Court held that the farmers had standing to seek injunctive relief because the "substantial risk" of gene flow would injure them in several ways, including by requiring them to test their alfalfa for genetically engineered crops and to take measures to minimize the risk of gene flow.[38] The Court observed that the farmers would suffer these injuries from deregulation whether or not gene flow actually occurred.[39]

[13] As these decisions indicate, the Supreme Court has articulated different formulations as to when a risk of future harm may constitute injury-in-fact. Unsurprisingly, lower courts have done the same. As commentators have noted, different circuits have applied arguably different substantive standards for determining whether a risk of future harm constitutes injury-in-fact under Article III.[40] Some circuit decisions have stated that this risk of future injury must be "credible" or realistic.[41] Other circuits, meanwhile, have suggested that nearly *any* increase in a risk of future harm may be sufficient to establish injury-in-fact. For example, the Second Circuit concluded in a 2003 decision that an "enhanced risk" of contracting food-borne illnesses established injury-in-fact.[42] The Seventh Circuit has stated "even a small probability of injury is sufficient to create a case or controversy."[43]

---

[37] *Id.* at 153.

[38] *Id.* at 153–54.

[39] *Id.* at 155.

[40] *See* F. Andrew Hessick, *Probabilistic Standing*, 106 NW. U. L. REV. 55, 58 (2012).

[41] *See, e.g.*, Stewart v. Blackwell, 444 F.3d 843, 855 (6th Cir. 2006) (increased risk of harm must be "neither speculative nor remote"), *vacated as moot by* 473 F.3d 692, 694 (6th Cir. 2007) (en banc); Ctr. for Law & Educ. v. Dep't of Educ., 396 F.3d 1152, 1161 (D.C. Cir. 2005) (requiring plaintiff to establish "demonstrably increased risk" of harm); Cent. Delta Water Agency v. U.S., 306 F.3d 938, 950 (9th Cir. 2002) (requiring "credible threat of harm").

B. *Clapper v. Amnesty International*

[14] With the foregoing cases as a backdrop, the Supreme Court again addressed the subject of standing and future harm in *Clapper v. Amnesty International USA*.[44] At issue in *Clapper* were amendments to the Foreign Intelligence Surveillance Act ("FISA"), which, among other things, regulates the government's interception of communications for foreign intelligence purposes.[45] Before the amendments' enactment in 2008, section 702 of FISA, 50 U.S.C. § 1881a, allowed the government to conduct electronic foreign intelligence surveillance only if it could establish before the Foreign Intelligence Surveillance Court ("FISC") that it had probable cause both that "the target of the electronic surveillance is a foreign power or [its] agent" and that each of the places to be monitored were being used by that foreign power or agent.[46] The 2008 amendments replaced these requirements with a more permissive rule that the government need only use procedures "reasonably designed" to limit surveillance of United States citizens and to comply with the Fourth Amendment.[47]

[15] The day the amendments were enacted, plaintiffs—a group of lawyers, journalists, and activists—filed suit seeking a declaration that the changes to FISA's probable cause requirements were unconstitutional.[48]

---

[42] *See* Baur v. Veneman, 352 F.3d 625, 634 (2d Cir. 2003).

[43] Am. Bottom Conservancy v. U.S. Army Corps of Eng'rs, 650 F.3d 652, 658 (7th Cir. 2011) (quoting Elk Grove Vill. v. Evans, 997 F.2d 328, 329 (7th Cir. 1993)).

[44] Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013).

[45] *Id.* at 1140, 1147.

[46] *See* 50 U.S.C. § 1805(a)(2)(A)–(B) (2012).

[47] *See Clapper*, 133 S. Ct. at 1145.

[48] *Id.* at 1140, 1142.

The plaintiffs argued that they had standing to sue because their work "requires them to engage in sensitive international communications with individuals who they believe are likely targets of surveillance" under the amended FISA.[49] They claimed that the amendments to § 1881a would compromise their ability to communicate with clients or sources and that the risk of surveillance under § 1881a would compel them to undertake "costly and burdensome measures," including traveling abroad to meet clients in person, to protect confidentiality.[50]

[16] While the district court held that the plaintiffs lacked standing, the Second Circuit reversed.[51] According to the Second Circuit, the plaintiffs had standing due to the "objectively reasonable likelihood" that their communications would be subject to the newly authorized government surveillance.[52] The plaintiffs also had standing, the Second Circuit explained, because their expenditures to avoid government surveillance were "*present* injuries" that stemmed "from a reasonable fear of *future* harmful government conduct."[53]

[17] The Supreme Court reversed.[54] Justice Alito, writing for the majority, noted two aspects of the case that he viewed as counseling for a conservative approach to the standing issue.[55] First, the plaintiffs' suit challenged the constitutionality of actions taken by other branches of government.[56] Second, their suit challenged actions of those branches "in

[49] *Id.* at 1142.

[50] *Id.* at 1143.

[51] *Id.* at 1155.

[52] Amnesty Int'l U.S. v. Clapper, 638 F.3d 118, 134 (2d Cir. 2011).

[53] *Id.* at 138.

[54] *Clapper*, 133 S. Ct. at 1143.

[55] *Id.* at 1147.

[56] *Id.*

the fields of intelligence gathering and foreign affairs."[57] Though not expressly incorporating these aspects of the case into the majority opinion's subsequent standing analysis, Justice Alito noted that previous standing inquiries had been "especially rigorous" in the first category of cases,[58] and that the Court had "often found a lack of standing" in the latter category.[59]

[18] Turning first to the plaintiffs' claim that they had standing because of the reasonable likelihood that they would be subject to government surveillance, Justice Alito concluded that the Second Circuit's "objectively reasonable likelihood" standard was "too speculative to satisfy the well-established requirement that threatened injury must be 'certainly impending.'"[60] While the majority opinion, citing language from previous decisions, left open the possibility that a "substantial risk" of future harm could also constitute injury-in-fact,[61] Justice Alito concluded that the plaintiffs' "attenuated chain of possibilities" would fail even that standard.[62] According to Justice Alito, the plaintiffs' theory of harm depended on the occurrence of no less than five successive events: (1) that the Government would target the plaintiffs' clients or sources; (2) that this surveillance was authorized under § 1881a; (3) that the Foreign Intelligence Surveillance Court would approve such surveillance; (4) that the Government would succeed in carrying out the surveillance; and (5) that the Government would monitor plaintiffs' own communications with those clients or sources.[63]

---

[57] *Id.*

[58] *Id.* (quoting Raines v. Byrd, 521 U.S. 811, 819–20 (1997)) (internal quotation marks omitted).

[59] *Id.* at 1147.

[60] *Clapper*, 133 S. Ct. at 1143.

[61] *Id.* at 1150 n.5.

[62] *Id.* at 1148.

[63] *See id.* at 1148–50.

[19] Turning next to the plaintiffs' claim that they had and would continue to undertake burdensome measures to protect themselves from government surveillance, Justice Alito held that such measures were not traceable to § 1881a.[64] Justice Alito rejected the Second Circuit's conclusion that a litigant could establish standing by incurring costs to mitigate any fear of surveillance that was not "fanciful, paranoid, or otherwise unreasonable."[65] As Justice Alito explained, Article III did not allow the plaintiffs to "manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."[66] The plaintiffs similarly could not establish standing on the basis of their clients' reluctance to speak with them, because such behavior was "based on third parties' subjective fear of surveillance."[67]

[20] Finally, Justice Alito distinguished several previous decisions where the Court had found standing based on a risk of future harm.[68] First, the majority explained that the Court's prior decision in *Laidlaw* involved wrongdoing that all parties conceded was ongoing, whereas in the facts before it in *Clapper* the plaintiffs had not proven that the government was monitoring them under § 1881a.[69] Second, the majority distinguished a First Amendment case, *Meese v. Keene*,[70] which involved a plaintiff who desired to show three films labeled as "political propaganda," and who was, unlike the *Clapper* plaintiffs, "unquestionably

[64] *Id.* at 1151.

[65] *Id.*

[66] *Clapper*, 133 S. Ct. at 1151.

[67] *Id.* at 1152 n.7.

[68] *Id.* at 1153.

[69] *Id.* at 1153.

[70] Meese v. Keene, 481 U.S. 465 (1987).

regulated" by the statute that he wished to challenge.[71] Third, the majority noted that the plaintiffs in *Geertson Seed Farms* had demonstrated concrete facts showing that gene flow could occur between their alfalfa and genetically modified alfalfa, whereas the plaintiffs in *Clapper* "present no concrete evidence to substantiate their fears, but instead rest on mere conjecture about possible governmental actions."[72]

[21] The majority opinion concluded with a summary of its central holding: the plaintiffs lacked Article III standing "because they cannot demonstrate that the future injury they purportedly fear is certainly impending and because they cannot manufacture standing by incurring costs in anticipation of non-imminent harm."[73]

[22] Justice Breyer, joined by Justices Ginsburg, Sotomayor, and Kagan, dissented.[74] According to Justice Breyer, the majority opinion, and in particular its reliance on the phrase "certainty impending," set a stricter requirement for injury-in-fact based on a risk of future harm than had past cases.[75] As Justice Breyer explained, "*certainty* is not, and never has been, the touchstone of standing."[76] Rather, "what the Constitution requires is something more akin to 'reasonable probability' or 'high probability.'"[77] For support, Justice Breyer gathered previous decisions from the Court where injury-in-fact had been found on the basis of, among

[71] *Clapper*, 133 S. Ct. at 1153.

[72] *Id.* at 1154 (citing Monsanto Co. v. Geertson Seed Farms, 130 S. Ct. 2743, 2755 (2010)).

[73] *Id.* at 1155.

[74] *Id.*

[75] *Id.* at 1165.

[76] *Id.* at 1160. (Breyer, J., dissenting).

[77] *See Clapper*, 133 S. Ct. at 1165.

other things, "realistic," "substantial," and "reasonable" risks of harm.[78] His opinion further argued, citing to both Supreme Court and circuit court decisions, that "courts have often found *probabilistic* injuries sufficient to support standing."[79] Justice Breyer concluded that he would have found the plaintiffs in *Clapper* to possess Article III standing.[80]

III. INJURY-IN-FACT IN DATA BREACH AND DATA COLLECTION CASES

[23] Over half a decade before the Supreme Court addressed Article III standing to challenge government collection of private information in *Clapper*, lower courts began addressing a separate, though closely related, issue: Article III standing to challenge *private* collection, retention, and disclosure of private information. This section catalogs those cases and the different conclusions they have reached on the issue of standing; cases interpreting *Clapper*'s standing analysis are discussed in the following section.

[24] This Article uses the terms "data breach cases" and "data collection cases" to describe the two different types of data privacy lawsuits that have emerged in recent years. The term "data breach cases" refers to lawsuits arising from the defendant's inadvertent loss or disclosure of a plaintiff's PII. Data breach cases generally focus on the increased risk of identity theft following a breach, and plaintiffs "customarily seek to recover their expenditures on credit monitoring, credit and debit card cancellation fees, and repayment for unauthorized charges."[81]

[78] *See id.* at 1161–62.

[79] *Id.* at 1162.

[85] *Id.* at 1165.

[81] Holmes v. Countrywide Fin. Corp., No. 5:08-CV-00205-R, 2012 U.S. Dist. LEXIS 96587, at *10 (W.D. Ky. July 12, 2012).

[25] The term "data collection cases," meanwhile, refers to lawsuits that arise from a defendant's intentional collection, storage, or sharing of the plaintiff's PII. These cases most typically involve either information shared on social networking websites, information surreptitiously collected by Internet "cookies," or information collected by smartphones or similar devices. While some data collection cases also focus on the risk of identity theft, most are driven by more traditional privacy concerns; the PII at issue often includes the plaintiff's shopping habits, web-browsing history, or even physical location. The theories of liability in data collection lawsuits are more varied than in data breach lawsuits, with plaintiffs often seeking damages under breach-of-contract theories, state consumer protection laws, or federal statutes.

[26] While data breach and data collection cases have raised a number of different legal issues, this Article focuses only on the issue of Article III standing. Many of the decisions discussed below found plaintiffs to have standing but nonetheless dismissed their claims on substantive grounds. This includes decisions that concluded that, while the plaintiffs may have alleged an injury sufficient to satisfy Article III's injury-in-fact requirement, they had not alleged an injury sufficient to satisfy the damages requirement of a state-law negligence or breach-of-contract claim.[82]

A. Data Breach Cases

[27] Plaintiffs in data breach cases have advanced several different theories of injury-in-fact. Most commonly, plaintiffs have contended that they suffered injury-in-fact from an increased risk of identity theft after their personal information has been compromised in a breach. Most plaintiffs relatedly contend that expenses they have incurred to mitigate this risk—for example, credit monitoring or cancellation of credit cards—constitute a separate basis for injury-in-fact. A smaller number of

[82] *See, e.g.*, Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 640 (7th Cir. 2007) (holding that plaintiffs had standing but had not alleged damages that were compensable under Indiana law).

plaintiffs have argued that they have suffered injury-in-fact due to their anxiety and distress upon learning about the loss of their personal information. Finally, some plaintiffs have sought to establish injury-in-fact on the theory that the loss of their personal information breached an implied contract with the defendant. This section assesses each theory in turn.

1. Increased Risk of Identity Theft and Measures Taken to Mitigate that Risk

[28] Among plaintiffs' arguments for injury-in-fact in data breach lawsuits, by far the most common are the related arguments that: (1) the plaintiff has suffered injury-in-fact due to an increased risk of future identity theft; and (2) the plaintiff has suffered injury-in-fact due to the expenses required to mitigate such risk of future identity theft. Though they are distinct arguments, courts have generally treated these two theories of injury-in-fact as rising or falling with one another.

[29] These theories of standing have achieved mixed results in lower courts. While initial federal decisions were hostile to the idea that an increased risk of identity theft could constitute injury-in-fact, a shift occurred after the Seventh Circuit endorsed such a theory in *Pisciotta v. Old National Bancorp*.[83] Despite more success for plaintiffs after *Pisciotta*, other courts have continued to find that an increased risk of identity theft does not establish injury-in-fact, including the Third Circuit in *Reilly v. Ceridian Corp.*[84]

[30] Even though they have differed in their final conclusions, courts have been more consistent in identifying what factors are relevant to whether a plaintiff's risk of future identity theft is either "real and imminent" or "conjectural and hypothetical." These factors include: (1) whether a data breach has actually occurred; (2) whether the data was lost or stolen; and (3) whether a third-party has actually used plaintiff's

[83] *Id.* at 634.

[84] Reilly v. Ceridian Corp., 664 F.3d 38, 46 (3d Cir. 2011).

sensitive third-party information in a way that has caused the plaintiff harm.

a. Injury-in-Fact Where Breached Personal Information Has Been Used to Harm the Plaintiff

[31] Courts have understandably found injury-in-fact in data breach cases where third parties actually use a plaintiff's compromised personal information in a way that causes the plaintiff harm. In *Resnick v. AvMed, Inc.* for example, the plaintiffs alleged that the defendant, a health-services company, had two laptops stolen from it that contained unencrypted files with the plaintiffs' health information, Social Security numbers, names, addresses, and phone numbers.[85] Ten months after the theft, one plaintiff discovered that a third-party had used her name to open bank accounts, activate credit cards, and make an address change.[86] Another plaintiff's information was used to open a brokerage account.[87] The Eleventh Circuit held that the plaintiffs had established injury-in-fact by "alleg[ing] that they have become victims of identity theft and have suffered monetary damages as a result."[88] The Eleventh Circuit expressly reserved judgment on whether any increased risk of future identity theft would also establish injury-in-fact.[89]

[85] Resnick v. AvMed, Inc., 693 F.3d 1317, 1322 (11th Cir. 2012).

[86] *Id.*

[87] *Id.*

[88] *Id.* at 1323.

[89] *Id.* at 1323 n.1 (11th Cir. 2012); *see also* Burrows v. Purchasing Power, LLC, No. 1:12-CV-22800-UU, 2012 U.S. Dist. LEXIS 186556, at *6 (S.D. Fla. Oct. 18, 2012) (applying *Resnick* to conclude that plaintiff, who alleged that an unknown third-party used his personal information to file a federal tax return and obtain a tax refund, has alleged injury-in-fact).

[32] The Sixth Circuit reached a similar conclusion in *Lambert v. Hartman*.[90] The plaintiff in that case alleged that third parties had made purchases in her name after her personal information, including her Social Security number, was publicly posted on the Hamilton County, Ohio's Clerk of Courts website.[91] The Sixth Circuit concluded that the plaintiff had standing to pursue her 42 U.S.C. § 1983 claims against the county.[92] As the court explained, the plaintiff had alleged "that her identity was stolen and that her financial security and credit rating suffered as a result."[93] These "actual financial injuries" were "sufficient to meet the injury-in-fact requirement."[94] By contrast, the Sixth Circuit noted in dicta that the plaintiff's allegation of an increased future risk of identity theft was "somewhat 'hypothetical' and 'conjectural.'"[95]

[33] Mere allegations of fraudulent credit card charges, however, may not necessarily establish injury-in-fact, even if traceable to the data breach at issue. For example, in *Willingham v. Global Payments, Inc.*, two plaintiffs alleged that they had discovered hundreds of dollars in fraudulent charges on their credit and debit cards following a data breach at the defendant company.[96] Despite finding the charges "fairly traceable" to the data breach,[97] the district court concluded that neither plaintiff had

[90] Lambert v. Hartman, 517 F.3d 433, 437 (6th Cir. 2008).

[91] *Id.* at 435–36. The information had come from a traffic citation issued to the plaintiff. *Id.* at 435.

[92] *Id.* at 438–39.

[93] *Id.* at 437.

[94] *Id.*

[95] *Id.*

[96] Willingham v. Global Payments, Inc., No. 1:12-CV-01157-RWS-JFK, 2013 U.S. Dist. LEXIS 27764, at *6–8 (N.D. Ga. Feb. 5, 2013).

[97] *Id.* at *14 (quoting Resnick v. AvMed, Inc., 693 F.3d 1317, 1324 (11th Cir. 2012)).

standing to sue.[98] According to the court, the plaintiffs' failure to plead that they either were not reimbursed for the charges or that they suffered other fees and expenses meant that they had not alleged identity theft in a way that created injury-in-fact.[99] The decisions in *Resnick* and *Lambert* are arguably consistent with *Willingham*, as both involved injuries that went beyond fraudulent credit card charges: changes of address and opened bank accounts in *Resnick*, and alleged damage to the plaintiff's credit score in *Lambert*.

b. Injury-in-Fact Where Data Has Been Stolen

[34] After situations where actual identity theft has occurred and caused the plaintiff harm, courts are next most likely to find injury-in-fact where a third-party has either stolen data or accessed it without authorization. Courts generally recognize these scenarios as presenting a more real threat of identity theft than where sensitive information is accidentally posted online or a computer containing sensitive information is simply lost or misplaced. Additionally, courts are even more likely to find injury-in-fact when circumstances suggest that a third-party specifically sought the plaintiffs' PII. This includes situations where an unknown third-party purposefully acquires information through computer hacking or credit card skimming, as well as situations where plaintiffs have traced subsequent fraudulent activity to the breach.

[35] These cases are also where the debate over Article III standing has most frequently arisen. Decisions from the Seventh and Ninth Circuit have held that the risk of future identity theft is sufficiently imminent in a data-theft context to establish injury-in-fact, while the Third Circuit has

[98] *Id.* at *23–26.

[99] *Id.* at *19–24. *But see* Burrows v. Purchasing Power, LLC, No. 1:12-CV-22800-UU, 2012 U.S. Dist. LEXIS 186556, at *7–9 (S.D. Fla. Oct. 18, 2012) (arguing that actual misuse of sensitive personal information even devoid of monetary loss is sufficient to confer standing). A possible distinction between *Willingham* and *Burrows* is that the latter case involved unauthorized use of the plaintiff's name and Social Security number, whereas the former appears to have only involved misuse of credit and debit card information.

held that it is not.[100] While the Seventh, Ninth, and Third Circuit's decisions are arguably factually distinguishable, they have contributed to a continuing split among district courts over whether standing exists in cases where a third-party purposefully compromises the plaintiff's PII.

[36] In *Pisciotta*, the Seventh Circuit held that an increased risk of future identity theft was sufficient to establish injury-in-fact for customers of a bank whose confidential records had been accessed by a third-party hacker.[101] The nature of the unauthorized access "suggest[ed] that the intrusion was sophisticated, intentional, and malicious."[102] While the customers did not allege to have experienced any direct financial loss or actual identity theft, they argued that they still had standing to pursue their claims for credit monitoring costs due to their increased risk of suffering future identity theft and the expenses they incurred to mitigate that risk.[103] The Seventh Circuit agreed, and stated that "the injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions."[104]

[37] To support its conclusion, the court in *Pisciotta* cited to previous Seventh Circuit decisions stating that a mere risk of future harm was sufficient for injury-in-fact.[105] The court also relied in part on decisions that endorsed Article III standing for medical monitoring claims in toxic

[100] *Compare* Reilly v. Ceridian Corp., 664 F.3d 38, 44 (3d Cir. 2011), *with* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007); *and* Krottner v. Starbucks Corp., 628 F.3d 1139, 1140 (9th Cir. 2010)).

[101] *Pisciotta*, 499 F.3d at 631.

[102] *Id.* at 632.

[103] *See id.*

[104] *Id.* at 634.

[105] *Id.* at 634 n.4 ("[E]ven a small probability of injury is sufficient to create a case or controversy . . . ." (quoting Elk Grove Vill. v. Evans, 997 F.2d 328, 329 (7th Cir. 1993)).

tort and medical device cases.[106] In discussing the separate issue of whether damages were available to the customers under Indiana law, the court described toxic tort medical monitoring cases as "somewhat analogous," though it ultimately noted that Indiana had yet to recognize such claims.[107]

[38] In *Krottner v. Starbucks Corp.*, the Ninth Circuit also found an allegedly increased risk of future identity theft to be sufficient to establish injury-in-fact.[108] The data breach in *Krottner* occurred when an unknown party stole a laptop with "unencrypted names, addresses, and social security numbers of approximately 97,000 Starbucks employees."[109] While the plaintiffs did not allege that they had experienced any financial harm, one plaintiff alleged that someone had attempted to open a bank account with his social security number.[110] The plaintiffs further alleged that they had and would continue to spend time and money monitoring their credit and finances for potential fraudulent activity.[111] The Ninth Circuit concluded that the plaintiffs had established injury-in-fact by alleging a "credible threat of harm."[112] The court noted that the risk of future harm had been sufficient to support standing in both the environmental[113] and toxic tort[114] contexts, as well as in the data breach

[106] *See id.* n.3 (citing Denney v. Deutsche Bank AG, 443 F.3d 253, 264–65 (2nd Cir. 2006); Sutton v. St. Jude Med. S.C., Inc., 419 F.3d 568, 574–75 (6th Cir. 2005)); *see also* Graves, *supra* note 12, at ¶ 12 (explaining that medical monitoring claims seek "recovery of the costs of medical tests designed to detect and prevent the onset of diseases resulting from [the] . . . defendant's actions.").

[107] *Pisciotta*, 499 F.3d at 638–39.

[108] Krottner v. Starbucks Corp., 628 F.3d 1139, 1140 (9th Cir. 2010).

[109] *Id.* at 1140.

[110] *Id.* at 1141.

[111] *Id.*

[112] *Id.* at 1143 (quoting Cent. Delta Water Agency v. United States, 306 F.3d 938, 950 (9th Cir. 2002) (internal quotation marks omitted)).

context with *Pisciotta*.[115] It observed by way of contrast that "[w]ere Plaintiffs-Appellants' allegations more conjectural or hypothetical—for example, if no laptop had been stolen, and Plaintiffs had sued based on the risk that it would be stolen at some point in the future—we would find the threat far less credible."[116]

[39] The Third Circuit, meanwhile, has held an increased risk of future identity theft to *not* be sufficient to support a finding of injury-in-fact in a data breach lawsuit. In *Reilly v. Ceridian Corp.*, it declined to find standing for customers of a payroll processing firm whose financial records had been accessed by a third-party. [117] According to the Third Circuit, the plaintiffs' increased risk of identity theft was "hypothetical" and "dependent on entirely speculative, future actions of an unknown third-party."[118] The Third Circuit distinguished both *Pisciotta* and *Krottner* as involving clearer indicia of potential identity theft: the intrusion in *Pisciotta* was "sophisticated, intentional and malicious," and someone had actually attempted to open a bank account with stolen personal information in *Krottner*.[119] The Third Circuit viewed these facts as demonstrating a more "imminent" and "certainly impending" harm than the present case, where there was "no evidence that the intrusion was intentional or malicious."[120]

---

[113] *Id.* at 1142 (citing Cent. Delta Water Agency, 306 F.3d 938, 948–50 (9th Cir. 2002)).

[114] *Krottner*, 628 F.3d at 1142 (citing Pritikin v. Dep't of Energy, 254 F.3d 791, 796–97 (9th Cir. 2001)).

[115] *Id.* (citing Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007)).

[116] *Id.* at 1143.

[117] Reilly v. Ceridian, 664 F.3d 38, 40–42 (3d Cir. 2011).

[118] *Id.* at 42.

[119] *Id.* at 43–44 (quoting Pisciotta, 499 F.3d at 632).

[120] *Id.* at 44.

[40] Although distinguishing *Pisciotta* and *Krottner*, the Third Circuit also expressed skepticism of both decisions' standing analyses, and particularly of their citation to toxic tort and medical device cases.[121] In the Third Circuit's view, an analogy to those cases was unfounded for at least two reasons. First, while in toxic tort and medical monitoring cases "an injury has undoubtedly occurred," in data breach cases "where no misuse is alleged," no such injury has occurred.[122] Second, medical device and toxic tort cases, as well as environmental cases, involved human health concerns often not redressable after the fact.[123] Finally, the court concluded that any expenditure by the plaintiffs to mitigate potential identity theft did not convert their hypothetical injury into an "actual or imminent" one.[124] According to the court, the plaintiffs had not spent money due to any actual injury, but rather "prophylactically spent money to ease fears of future third-party criminality."[125]

[41] District courts have likewise reached differing conclusions about injury-in-fact when a data breach occurs in a manner that suggests potential identity theft. An earlier Southern District of Ohio decision concluded that a risk of future identity theft was too conjectural to support standing[126] in a case where "unauthorized persons obtained access to and acquired the information of approximately 96,000 customers" of the retailer DSW, Inc.[127] In that case, the plaintiff alleged her "potential injury [was] contingent upon her information being obtained and then used by an unauthorized person for an unlawful purpose," but had "not alleged evidence that a third party intends to make unauthorized use of her

[121] *See id.*

[122] *Id.* at 4.

[123] *Reilly*, 664 F.3d. at 45–46.

[124] *Id.* at 46.

[125] *Id.*

[126] *See* Key v. DSW Inc., 454 F. Supp. 2d 684, 688–89 (S.D. Ohio 2006).

[127] *Id.* at 686.

financial information or of her identity."[128] The court also found medical monitoring cases inapposite, partially because they were "not inextricably linked to the possible criminal actions of unknown third parties at some unidentified point in the indefinite future."[129]

[42] An Eastern District of Missouri court reached a similar conclusion in *Amburgy v. Express Scripts, Inc.*[130] In that case, hackers had accessed confidential information in the defendant company's possession and attempted to extort the company with its threatened release.[131] The court nonetheless concluded that the plaintiff—who did not know for certain whether his personal data had been compromised and alleged only "an increased risk of identify [sic] theft at an unknown point in the future"—had not shown injury-in-fact.[132] According to the court, "many 'if's' would have to come to pass" for the plaintiff to suffer identity theft, including the compromise of his data, the obtaining of that data by a third-party, and the use of that data to commit identity theft.[133] These events were, in the court's view, all hypothetical and speculative.[134]

[43] Similarly, in *Willingham v. Global Payments, Inc.*, a case where plaintiffs alleged that they had actually experienced fraudulent credit and debit card charges following a security breach,[135] the Northern District of

[128] *Id.* at 690.

[129] *Id.* at 691.

[130] *See* Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046, 1053 (E.D. Mo. 2009) (citing Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992)).

[131] *Id.* at 1049.

[132] *Id.* at 1053 (citing Johnson v. Missouri, 142 F.3d 1087, 1089–90).

[133] *Id.* at 1053.

[134] *See id.*

[135] Willingham v. Global Payments, Inc., No. 1:12-CV-01157-RWS-JFK, 2013 U.S. Dist. LEXIS 27764, at *6–7 (N.D. Ga. Feb. 5, 2013).

Georgia concluded that the risk of future identity theft likely was not sufficiently "imminent" to establish injury-in-fact.[136] Citing to *Reilly*, the court noted that the plaintiffs' alleged risk of future identity theft was "dependent on entirely speculative, future actions of an unknown third-party."[137]

[44] By contrast, the Southern District of California found injury-in-fact to have been alleged when customers of Sony brought suit after hackers accessed Sony's computer networks and stole sensitive personal information from millions of accounts.[138] Following *Krottner* as binding authority, the court concluded that the plaintiffs had alleged injury-in-fact because they had alleged "that their sensitive Personal Information was wrongfully disseminated, thereby increasing the risk of future harm."[139] Similarly, the Western District of Kentucky found injury-in-fact when plaintiffs, customers of a bank whose former employee had stolen confidential information on 2.4 million individuals and "passed the data on to known and unknown third parties in exchange for payments of $70,000," alleged that automobile loans had been applied for in their names or that their home had been "bombarded" with telemarketing calls.[140] According to the court, the plaintiffs established injury by taking reasonable steps to mitigate the harms of the employee's actions, including purchasing credit monitoring and cancelling their home phone service.[141]

---

[136] *Id.* at *23–25 (recommending the plaintiffs' complaint be dismissed for failure to state a claim and the defendant's motion to dismiss for lack of jurisdiction be denied as moot).

[137] *Id.* at *20 (quoting Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011)) (internal quotation marks omitted).

[138] *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942, 950–51, 958 (S.D. Cal. 2012).

[139] *Id.* at 958 (citing Krottner v. Starbucks Corp., 628 F.3d 1139, 1142 (9th Cir. 2010)).

[140] Holmes v. Countrywide Fin. Corp., No. 5:08-CV-00205-R, 2012 U.S. Dist. LEXIS 96587, at *4–5, *12 (W.D. Ky. July 12, 2012).

[45] Courts have also reached differing conclusions when, like in *Reilly*, data has been stolen but nothing suggests that it was the thief's specific target.[142] A good example of the difference that the apparent motives and capabilities of a data hacker can have on a court's standing analysis is *Allison v. Aetna, Inc.*[143] In that case hackers managed to gain access to Aetna's job application data base, which contained the sensitive information of over 450,000 applicants, including the plaintiff's.[144] While Aetna confirmed that the hackers obtained the e-mail addresses of some applicants, it was unclear whether they obtained any other information; the hackers later sent "phishing" e-mails to job applicants asking them for more personal information.[145] The plaintiff could not confirm that his e-mail was among the ones stolen, and he had not received a phishing e-mail.[146] The district court concluded that his alleged increased risk of future identity theft, along with the steps he had taken to mitigate that risk, were "far too speculative" and could not establish injury-in-fact.[147] The court noted, among other things, that the hackers' phishing e-mails suggested that they in fact lacked the necessary information to commit identity theft, thus distinguishing the case from the more "sophisticated" hacking operation in *Pisciotta*.[148]

---

[141] *Id.* at *12 (citing Lambert v. Hartman, 517 F.3d 433, 437 (6th Cir. 2008); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007)).

[142] *See* Reilly v. Ceridian Corp., 664 F.3d 38, 40, 44 (3d Cir. 2011).

[143] *See* Allison v. Aetna, Inc., No. 09-2560, 2010 U.S. Dist. LEXIS 22373, at *18–21 (E.D. Pa. Mar. 9, 2010).

[144] *See id.* at *1–3.

[145] *See id.* at *2–3.

[146] *See id.* at *3.

[147] *Id.* at *18–21.

[148] *See Allison*, 2010 U.S. Dist. LEXIS 22373, at *24 (citing Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 632).

[46] In *Randolph v. ING Life Insurance & Annuity Co.*, burglars stole a laptop containing the names, addresses, and Social Security numbers of 13,000 current and former employees of the District of Columbia.[149] The district court concluded that the risk of future identity theft was too speculative for a finding of injury-in-fact, based either on that risk alone or on the steps the plaintiffs had taken to mitigate the risk.[150] Since the plaintiffs had not alleged that the burglar was specifically after their personal information, this meant that their allegations were "mere speculation that at some unspecified point in the indefinite future they will be the victims of identity theft."[151] The district court remanded the case to state court, where it eventually reached the District of Columbia Court of Appeals.[152] The Court of Appeals issued its own opinion, which, while not squarely ruling on the standing issue (it dismissed the plaintiffs' complaint for failure to state a claim), criticized the district court's approach and suggested that injury-in-fact would be "fairly easily satisfied" by the plaintiffs' statutory and tort claims,[153] particularly in light of the Supreme Court's decision in *Doe v. Chao*.[154]

[47] Two other decisions, facing similar facts, reached the opposite conclusion and held that a threat of future identity theft did establish injury-in-fact. In *Caudle v. Towers, Perrin, Forster & Crosby, Inc.*, a

[149] *See* Randolph v. ING Life Ins. & Annuity Co., 486 F. Supp. 2d 1, 3 (D.D.C. 2007).

[150] *See id.* at 7–8.

[151] *Id.*; *see also* Hinton v. Heartland Payment Sys., Inc., No. 09-594 (MLC), 2009 U.S. Dist. LEXIS 20675, at *1, *3 (D.N.J. Mar. 16, 2009) (dismissing a "rambling" *pro se* complaint alleging that defendant had lost Plaintiff's sensitive personal information in a data breach where Plaintiff's "allegations of injuries amount to nothing more than mere speculation").

[152] *See Randolph*, 486 F. Supp. 2d at 11.

[153] *Randolph*, 973 A.2d at 707.

[154] *See id.* (citing Doe v. Chao, 540 U.S. 614 (2004)); *see also infra* section III.A.2 (discussing *Doe v. Chao*).

pension consulting company had several laptops containing sensitive personal information stolen from its office, but "[n]othing in the record shed[] light on whether the laptops were stolen for their intrinsic value, for the value of the data or for both."[155] The district court, citing *Pisciotta* and drawing an analogy to toxic tort cases, held that the threat of future identity theft faced by the plaintiffs was sufficient to establish standing.[156] In *Ruiz v. Gap Inc.*, two laptops containing the unencrypted sensitive personal information of over 800,000 Gap job applicants, including the plaintiff, were stolen from a Gap vendor. [157] The district court concluded that the plaintiff's allegation of an increased future risk of identity theft was sufficient to establish injury-in-fact at the motion-to-dismiss stage, though it suggested that more concrete allegations would be needed for the case to move forward.[158] When the defendants later brought motions for summary judgment, the court again found standing based on an increased risk of identity theft,[159] even though it was "less clear than it was in *Pisciotta* that the thief was targeting the plaintiff's personal information."[160] The court granted summary judgment, however, on the merits of the plaintiff's claims.[161] The Ninth Circuit affirmed both the district court's rulings on standing and on the merits.[162]

---

[155] Caudle v. Towers, Perrin, Forster & Crosby, Inc., 580 F. Supp. 2d 273, 276 (S.D.N.Y. 2008).

[156] *See id.* at 279–80 (citing Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007); LaFleur v. Whitman, 300 F.3d 256, 270 (2d Cir. 2002)).

[157] *See* Ruiz v. Gap, Inc., 540 F. Supp. 2d 1121, 1124–25 (N.D. Cal. 2008).

[158] *See id.* at 1125–26.

[159] *See* Ruiz v. Gap, Inc., 622 F. Supp. 2d 908, 911–13 (N.D. Cal. 2009).

[160] *Id.* at 912. The court noted, however, statistical evidence provided by the plaintiff that 19% of Americans notified of a data breach during the previous year had reported becoming victims of identity theft, while only 4.32% of Americans generally did so. *Id.* at 913.

[161] *Id.* at 918.

c. Injury-in-Fact Where Plaintiffs' Data Has Otherwise Been Exposed or Lost

[48] In contrast to cases where sensitive data has been stolen, courts have been less likely to find injury-in-fact due to an increased risk of identity theft where sensitive data has simply been lost or inadvertently exposed. Still, even in these factual situations, courts have reached differing conclusions about whether a risk of future identity theft is sufficiently imminent to establish injury-in-fact under Article III.

[49] Some courts have refused to find injury-in-fact where sensitive data has been exposed, but not necessarily exposed to criminal parties. In one of the first cases to consider data breach lawsuits and Article III standing, a district court held that an alleged increased risk of future identity theft did not support injury-in-fact where the plaintiff's personal information had been accessed by a company's client without authorization and sold to a marketing company.[163] The plaintiff did not plead that, in the three years since the breach, she had either received junk mail or suffered an identity theft.[164] Likewise, a bankruptcy court found no injury-in-fact where a creditor posted a proof of claim, which remained public for six days, containing the debtor's Social Security number, driver's license number, and date of birth.[165] The court concluded on summary judgment that the risk of identity theft was neither actual nor

[162] *See* Ruiz v. Gap, Inc., 380 F. App'x 689, 690–91 (9th Cir. 2010) ("Ruiz alleged, with support from an expert affidavit, that he was at greater risk of identity theft. As the district court properly concluded, this alleged prospective injury presents enough of a risk that the concerns of plaintiffs are real, and not merely speculative.").

[163] *See* Bell v. Acxiom Corp., No. 4:06CV00485-WRW, 2006 U.S. Dist. LEXIS 72477, at *1–3 (E.D. Ark. Oct. 3, 2006).

[164] *See id.* at *8.

[165] *See* Davis v. Eagle Legacy Credit Union, 430 B.R. 902, 905, 907 (Bankr. D. Colo. 2010).

imminent, as the debtor provided no proof that the information had been accessed by any unauthorized party.[166]

[50] Other district courts have similarly refused to find injury-in-fact established where files containing sensitive personal information were lost in transit. In *Giordano v. Wachovia Securities, LLC*, a package with financial information of tens of thousands of the defendant's customers was lost in the mail. [167] The district court concluded that plaintiffs' alleged increased risk of identity theft was "speculative and hypothetical" and did not establish injury-in-fact.[168] The court rejected the argument that the case was analogous to medical monitoring cases.[169] Likewise, in *Hammond v. The Bank of N.Y. Mellon Corp.*, the defendant company lost a metal box containing six to ten computer back-up tapes with the unencrypted sensitive personal information of over 12.5 million individuals.[170] Three plaintiffs alleged that they experienced "unauthorized credit transactions" after the tapes were lost.[171] The district court held that the plaintiffs' injury was speculative and conjectural, and noted that it found the Seventh Circuit's reasoning in *Pisciotta* unpersuasive.[172]

---

[166] *See id.* at 907.

[167] Giordano v. Wachovia Sec., LLC, No. 06-476 (JBS), 2006 U.S. Dist. LEXIS 52266, at *3–4 (D.N.J. July 31, 2006).

[168] *Id.* at *12.

[169] *Id.* at *11 n.4.

[170] Hammond v. Bank of N.Y. Mellon Corp., No. 08 Civ. 6060 (RMB) (RLE), 2010 U.S. Dist. LEXIS 71996, at *9–10, *14-15 (S.D.N.Y. June 25, 2010).

[171] *Id.* at *17.

[172] *See id.* at *23, *28; *see also* Whitaker v. Health Net of Cal. Inc., No. CIV S-11-0910 KJM-DAD, 2012 U.S. Dist. LEXIS 6545, at *5, *9 (E.D. Cal. Jan. 19, 2012) (declining to find standing where defendant lost several hard drives containing personal information of over 800,000 individuals, including plaintiffs, but plaintiffs had alleged no misuse of their information and distinguishing the Ninth Circuit's decisions in *Krottner* and *Ruiz* as involving "the theft of information, not its loss").

[51] By contrast, in another lawsuit stemming from the same data breach as *Hammond*, a district court found injury-in-fact to be present.[173] In *McLoughlin v. People's United Bank, Inc.*, which involved the same loss of back-up tapes as in *Hammond*, the court concluded that an increased risk of future identity theft was sufficient to confer Article III standing.[174] Unlike in *Hammond*, the court cited *Pisciotta*'s standing analysis favorably.[175]

d. Injury-in-Fact Where No Data Breach Has Occurred

[52] Finally, others decisions have considered—and rejected—Article III standing where plaintiffs have alleged not that their personal information had been compromised in a breach, but only that a defendant company's lax security practices created an intolerable likelihood that such a breach would occur.

[53] In *Katz v. Pershing, LLC*, a brokerage firm customer alleged that the defendant, a company that provided various back-office services to the brokerage firm, used inadequate privacy measures and had exposed her sensitive personal information to anyone with access to the defendant's computer network, including other customers.[176] The First Circuit concluded that without an actual identified unauthorized use of her data, the plaintiff could not establish injury-in-fact on the theory of an increased risk of identity theft or of expenses made to mitigate that risk.[177] More

[173] *See* McLoughlin v. People's United Bank, Inc., No. 3:08-CV-00944(VLB), 2009 U.S. Dist. LEXIS 78065, at *1–2, *13 (D. Conn. Aug. 31, 2009).

[174] *See id.* at *3, *7–13.

[175] *See id.* at *11–12 (citing Pisciotta v. Old Nat'l Bancorp., 499 F.3d 629 (7th Cir. 2007)).

[176] *See* Katz v. Pershing, LLC, 672 F.3d 64, 69–70 (1st Cir. 2012).

[177] *Id.* at 79.

recently, in *Hammer v. Sam's East, Inc.*, customers of the retail chain Sam's Club alleged that the company had made "numerous misrepresentations" about how it protects its customers' sensitive information.[178] The customers made "no allegation that their personal information has been stolen, compromised, or fraudulently used," nor did they "allege that a security breach has occurred."[179] The district court held that the customers' alleged injury was too speculative and noted that "no court has found that a mere increased risk of identity theft or fraud constitutes an injury in fact for standing purposes without some alleged theft of personal data or security breach."[180]

[54] Plaintiffs have brought similar claims in data collection cases: that a company's collection or transmittal of the plaintiffs' personal information, often without encryption, constitutes injury-in-fact due to the creation of an unreasonable risk of unauthorized use.[181] Courts have generally rejected this theory of standing.[182] As these cases involve allegations of either data collection by the Defendant itself or transfer of

[178] Hammer v. Sam's East, Inc., No. 12-CV-2618-CM, 2013 U.S. Dist. LEXIS 98707, at *2 (D. Kan. July 16, 2013).

[179] *Id.* at *3.

[180] *Id.* at *7–8 (citing Katz v. Pershing, 672 F.3d 64, 79 (1st Cir. 2012)).

[181] *See, e.g.*, Yunker v. Pandora Media, Inc., No. 11-CV-03113 JSW, 2013 U.S. Dist. LEXIS 42691, at *15 (N.D. Cal. Mar. 26, 2013) (allegation that Defendant's collection and storage of Plaintiff's personal identifying information, without anonymization, creates a substantive risk of future harm).

[182] *See id.* at *15–16; Hernandez v. Path, Inc., No. 12-CV-01515 YGR, 2012 U.S. Dist. LEXIS 151035, at *4 (N.D. Cal. Oct. 17, 2012) (citing Krottner v. Starbucks Corp., 628 F.3d 1139, 1141–43 (9th Cir. 2010)); Goodman v. HTC Am., Inc., No. C11-1793MJP, 2012 U.S. Dist. LEXIS 88496, at *19–20 (W.D. Wash. June 26, 2012) (citing Warth v. Seldin, 422 U.S. 490, 501 (1975)); Low v. Linkedin Corp., No. 11-CV-01468-LHK, 2011 U.S. Dist. LEXIS 130840, at *9 (N.D. Cal. Nov. 11, 2011). *But see In re* iPhone Application Litig., 844 F. Supp. 2d 1040, 1054 (N.D. Cal. 2012) (concluding, with little discussion, that the "increased, unexpected, and unreasonable risk to the security of sensitive personal information" allegedly surreptitiously transferred from Defendant to third-party advertisers created "actual injury").

information to third-party advertisers, courts have found that, even under *Krottner*, any fear of future identity theft is simply too speculative.[183] Perhaps equally importantly, courts have noted that the information at issue in these cases is often not sensitive financial information.[184]

2. Mental Distress About Identity Theft

[55] A few plaintiffs in data breach cases have argued that they suffered injury-in-fact due to anxiety and emotional distress caused by knowing that they are at an increased risk of future identity theft. Much like the theory that expenses incurred to mitigate the risk of identity theft can establish standing, this argument has risen or fallen with courts' assessments of the underlying likelihood of identity theft actually occurring. Thus, *Krottner*, which found an increased risk of future identity theft sufficient to establish injury-in-fact, also found that an allegation of "generalized anxiety and stress" resulting from the data breach constituted "present injury" that was "sufficient to confer standing."[185] But *Reilly*, which did not find an increased risk of identity theft to itself establish injury-in-fact, rejected the argument that the plaintiffs' emotional distress about identity theft established injury-in-fact.[186]

---

[183] *See, e.g.*, *Goodman*, 2012 U.S. Dist. LEXIS 88496, at *21–22 (finding Plaintiff's theory of harm too speculative to establish injury-in-fact and distinguishing *Krottner* because "Plaintiffs do not allege that their personal data has been stolen, only that is susceptible to theft").

[184] *See Yunker*, 2013 U.S. Dist. LEXIS 42691, at *16 (noting that Plaintiff "does not allege that he disclosed sensitive financial information, such as a social security number or a credit card number"); *see also In re* Linkedin User Privacy Litig., 932 F. Supp. 2d 1089, 1094–95 (N.D. Cal. 2013) (holding that public posting of Plaintiff's LinkedIn password did not amount "to a legally cognizable injury, such as, for example, identify [sic] theft or the theft of her personally identifiable information").

[185] Krottner v. Starbucks Corp., 628 F.3d 1139, 1142 (9th Cir. 2010); *see also* McLoughlin v. People's United Bank, Inc., No. 3:08-cv-00944(VLB), 2009 U.S. Dist. LEXIS 78065, at *9 (D. Conn. Aug. 31, 2009) (citing Denney v. Deutsche Bank AG, 443 F.3d 253, 264 (2d Cir. 2006)) (noting that "the fear or anxiety of future harm" can constitute injury-in-fact).

[56] While these cases may suggest that an emotional distress argument is unlikely to succeed as a standalone basis for injury-in-fact, potentially complicating the matter is the Supreme Court's decision in *Doe v. Chao*. The plaintiff in *Doe* had filed for benefits under the Black Lung Benefits Act and later learned that the Department of Labor had inadvertently disclosed his Social Security number in hearing notices sent to multiple parties.[187] The plaintiff brought suit against the federal government under the Privacy Act,[188] but did not provide any proof of injury other than allegations that he was "torn . . . all to pieces" and "greatly concerned and worried" about the disclosure of his Social Security number.[189] The Supreme Court did not address Article III standing, but clearly assumed that such standing was present: its opinion focused instead on whether the plaintiff had stated a claim under the Privacy Act.[190] In her dissenting opinion, Justice Ginsburg characterized the majority as having found that "Doe has standing to sue" based on his alleged emotional injury.[191]

[57] This issue of standing and emotional harm came up in a subsequent Privacy Act case, *American Federation of Government Employees v. Hawley*. The claims in *Hawley* were brought by Transportation Security Administration ("TSA") employees after the TSA lost a hard drive containing sensitive personal information on over 100,000 current and former employees.[192] Bringing suit under the Privacy Act, the employees alleged to have suffered injury in the form of, among other things, "embarrassment, inconvenience, mental distress, concern for

[186] *See* Reilly v. Ceridian Corp., 664 F.3d 38, 44–45 (3d Cir. 2011).

[187] *See Doe v. Chao*, 540 U.S. 614, 616–17 (2004).

[188] 5 U.S.C. § 552a(b) (2012).

[189] *Chao*, 540 U.S. at 617–18 (internal quotation marks omitted).

[190] *See id.* at 616.

[191] *Id.* at 641 (Ginsburg, J., dissenting).

[192] *See* AFGE v. Hawley, 543 F. Supp. 2d 44, 45 (D.D.C. 2008).

identity theft, concern for damage to credit report . . . [and] mental distress due to the possibility of security breach at airports."[193] The district court agreed that these allegations of mental distress "alleged injury . . . not speculative nor dependent on any future event, such as a third party's misuse of the data."[194] While the court did not cite to *Chao* in its standing analysis, it did cite to another Privacy Act case.[195]

[58] Yet in *In re Science Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litigation*, another judge on the same court reached a different conclusion. The litigation in *SAIC* arose from the theft of several data tapes that contained personal information and medical records of 4.7 million U.S. military members and their families.[196] But the tapes did not appear to be the target of the theft (they were stolen from a car along with a GPS system and a stereo), and accessing their information required specialized computer equipment.[197] The district court held that the plaintiffs could not bring a Privacy Act claim because they could not allege "that their information has been exposed in a way that would facilitate easy, imminent access."[198] The court distinguished *Chao* on the ground that the plaintiff's information in that case had actually been published on documents that were sent to third-parties.[199]

[59] Courts have also cited to *Chao* in cases not involving the Privacy Act. Despite *Doe*'s lack of discussion on the issue of standing, the Ninth

[193] *Id.* at 50–51 (internal quotation marks omitted).

[194] *Id.* at 51.

[195] *Id.* n.12 (quoting Krieger v. Dep't of Justice, 529 F. Supp. 2d 29, 53 (D.D.C. 2008)).

[196] *See In re*. Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., No. 12-347 (JEB), 2014 U.S. Dist. LEXIS 64125, at *5–6 (D.D.C. May 9, 2014).

[197] *Id.* at *5, *10.

[198] *Id.* at *35.

[199] *See id.* at *36 (citing Doe v. Chao, 540 U.S. 614, 617 (2004)).

Circuit in *Krottner* cited it in support of its own holding and characterized the decision as "suggesting" that the plaintiff's alleged emotional distress had established Article III standing.[200] The District of Columbia Court of Appeals also cited to *Doe* in its discussion of injury-in-fact in *Randolph*, albeit not in connection to claims of emotional distress.[201]

3. Breach of an Implied Contract

[60] Finally, some plaintiffs in data breach cases have attempted to establish injury-in-fact under the theory that the data breach was itself a breach of an implied contract between them and the defendant, whereby the defendant, in return for some sort of consideration, had agreed to take reasonable measures to protect the plaintiffs' sensitive personal information. Most commonly, plaintiffs have argued that they believed reasonable protection of their sensitive personal information was included in the price they paid for the defendant's goods or services.

[61] Some courts have recognized that this theory of injury, if pled correctly, can establish injury-in-fact. The First Circuit, for example, has twice recognized implied contract claims in data breach cases.[202] It held in *Katz* that a breach-of-contract claim could establish injury-in-fact, although the court quickly dismissed the contract claim in *Katz* on substantive grounds.[203] The court held in another case, *Anderson v. Hannaford Bros. Co.*, that under Maine law a jury could reasonably find the existence of an implied contract between a grocery store and its customers that the store "would not use the credit card data for other people's purchases, would not sell the data to others, and would take

[200] *See* Krottner v. Starbucks Corp., 628 F.3d 1139, 1142 (9th Cir. 2010) (citing *Chao*, 540 U.S. at 617–18, 624–25).

[201] *See* Randolph v. ING Life Ins. & Annuity Co., 973 A.2d 702, 706–07 (D.C. 2009) (citing *Doe*, 540 U.S. at 621).

[202] *See infra* notes 215–16.

[203] *See* Katz v. Pershing, 672 F.3d 64, 72 (1st Cir. 2012).

reasonable measures to protect the information."[204] *Anderson* did not discuss Article III standing.[205]

[62] By contrast, in *Remijas v. Neiman Marcus Group*, the Northern District of Illinois rejected the notion that an implied breach-of-contract claim could establish injury-in-fact for data breach plaintiffs.[206] The plaintiffs in *Remijas* had argued that the prices they paid for goods at the defendant's department store included a "premium" for proper data security measures.[207] The court dismissed this theory on the ground that, unlike in other implied contract cases, the alleged deficiency in data security measures was "extrinsic" to the products purchased by defendants.[208]

[63] While establishing injury-in-fact from a breach of contract may be possible for data breach plaintiffs, successfully pleading such a theory has proven much more difficult. In *In re Linkedin User Privacy Litigation*, the plaintiffs, paying members of LinkedIn's services, alleged that LinkedIn had breached an implied contract to adequately protect their sensitive information.[209] Dismissing this claim, the court noted that LinkedIn's

[204] Anderson v. Hannaford Bros. Co., 659 F.3d 151, 159 (1st Cir. 2011).

[205] *See also* Doe 1 v. AOL, LLC, 719 F. Supp. 2d 1102, 1109 (N.D. Cal. 2010) (holding that plaintiffs had Article III standing to pursue a consumer protection claim against AOL, which had publically posted their Internet search histories). Though the rationale for *Doe 1*'s finding of injury-in-fact was not entirely clear, the court did agree with plaintiffs' claim that "AOL's collection and disclosure of members' undeniably sensitive information is not something that members bargained for when they signed up and paid fees for AOL's service." *Id.* at 1111.

[206] *See* Remijas v. Neiman Marcus Grp., LLC, No. 14 C 1735, 2014 U.S. Dist. Lexis 129574, at *13–14 (N.D. Ill. Sep. 16, 2014).

[207] *See id.* at *4.

[208] *See id.* at *5; *see also infra* section II.B.2 (cataloguing some disagreement between data collection cases over whether a breach-of-contract theory supports injury-in-fact).

[209] *In re* Linkedin User Privacy Litig., 932 F. Supp. 2d 1089, 1092 (N.D. Cal. 2013).

privacy policy and user agreement were the same for both paying and non-paying members, thus precluding any argument that the policies went to the basis of the parties' bargain.[210] Likewise, in *In re Barnes & Noble Pin Pad Litigation*, the district court held that plaintiffs, whose credit card numbers had been skimmed from Barnes & Noble pin pad machines, had failed to plead injury-in-fact premised on the theory that the prices they paid for Barnes & Noble goods implicitly included a promise to adequately protect their financial information.[211] As the court noted, Barnes & Noble charged the same price for its products whether payment was made with a credit card or in cash.[212]

B. Data Collection Cases

[64] Unlike data breach cases, data collection cases do not focus on the occurrence or possibility of unauthorized third-party access to sensitive personal data in the defendant's possession. Rather, they focus on allegedly unauthorized collection or transmittal of personal information conducted by the defendant itself. In the most common data collection cases, plaintiffs allege that the defendant, typically a social-media website or other Internet business, has surreptitiously transmitted their personally identifiable information to third-party advertisers seeking to exploit it for marketing purposes.

[210] *See id.* at 1093. The court also noted that the Plaintiffs had failed to allege in their complaint that they had actually read LinkedIn's privacy policy. *Id.*

[211] *See In re* Barnes & Noble Pin Pad Litig., No. 12-CV-8617, 2013 U.S. Dist. LEXIS 125730, at *14–15 (N.D. Ill. Sept. 3, 2013).

[212] *See id.* at *15; *cf.* Hammer v. Sam's East, Inc., No. 12-CV-2618-CM, 2013 U.S. Dist. LEXIS 98707, at *8 n.5 (D. Kan. July 16, 2013) (dismissing plaintiff's argument of standing based on payment of excessive fees where complaint failed to allege that such fees were actually paid or that Defendant's actions reduced the value of the services received for the fees); McLoughlin v. People's United Bank, Inc., No. 3:08-CV-00944 (VLB), 2009 U.S. Dist. LEXIS 78065, at *24 (D. Conn. Aug. 31, 2009) (dismissing plaintiff's argument of standing based on payment of excessive fees to defendant due to the complaint's failure to mention any such fees).

[65] Data collection cases differ from data breaches in significant ways, many of which impact courts' standing analyses. First, data collection and data breach cases often involve different types of parties. Data collection cases generally do not involve the transfer of data to criminal third parties or other entities that are likely to use it to commit identity theft, but rather involve the transfer of PII to businesses seeking to use it for advertising and marketing purposes. Second, data collection and data breach cases often involve different types of information. Plaintiffs in data collection cases rarely allege that sensitive financial information—Social Security numbers, credit card numbers—have been illegally used by the Defendant. Rather, they more typically allege the illegal use of information such as names, addresses, Internet browsing history, and physical location. This information's disclosure poses much less of a threat of identity theft, but much more of a threat of embarrassment or violation of other traditional privacy notions.

[66] Plaintiffs in data collection cases have advanced several different theories of injury-in-fact, including: (1) that the unauthorized use of their PII deprived them of that information's economic value; (2) that the unauthorized use of their PII constituted a breach of contract; (3) that the unauthorized collection or transmittal of PII from their phones negatively impacted the phones' performance; (4) that the unauthorized use of PII caused emotional harm; (5) that the unauthorized use of PII required expenditures to prevent that use; and (6) that injury-in-fact is established by various computer and privacy statutes. As explained below, these theories have achieved varying levels of success.

[67] Also worth noting is that data collection cases have an even more recent history than data breach cases. The vast majority of data collection cases have taken place in district courts in the Ninth Circuit, most notably the Northern District of California (home of Silicon Valley and many of the country's largest technology firms). Consequently, a decision from the Ninth Circuit could abruptly and dramatically shift the current landscape of Article III standing in these cases.

1. Economic Value of PII

[68] One of the most common, but least successful, arguments for injury-in-fact made by data collection plaintiffs is that the unauthorized collection or transmittal of their PII deprives them of that information's inherent economic value. This argument is premised on the idea that the type of information collected by defendants in these cases—names, e-mail addresses, demographic information, Internet browsing and shopping history—has economic value that advertising and marketing companies are willing to pay for, at least in the aggregate. Plaintiffs argue that by taking this information without authorization, defendants have deprived them of the opportunity to exploit the economic value of this information themselves.

[69] While courts have not completely ruled out the idea that an individual's PII may have value, they have been reluctant to hold that this value translates into injury-in-fact in data collection cases.[213] One of the first data collection decisions, *LaCourt v. Specific Media, Inc.*, contains an influential analysis of this issue. The plaintiffs in *LaCourt* alleged that the defendants had placed "cookies" on their Internet browsers to track, without consent, their Internet usage.[214] The plaintiffs alleged that this

[213] Courts have also rejected arguments of injury-in-fact based on loss of PII value in data breach cases. *See In re* Science Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.,No. 12-347 (JEB), 2014 U.S. Dist. LEXIS 64125, at *7 (D.D.C. May 9, 2014); Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 657 (S.D. Ohio 2014*); In re* Barnes & Noble Pin Pad, No. 12-CV-8617, 2013 U.S. Dist. LEXIS 125730, at *12–13 (N.D. Ill. Sept. 3, 2013); Willingham v. Global Payments, Inc., No. 1:12-CV-01157-RWS-JFK, 2013 U.S. Dist. LEXIS 27764, at *20 (N.D. Ga. Feb. 5, 2013). *But see* Claridge v. RockYou, Inc., 785 F. Supp. 2d 855, 861, 866 (N.D. Cal. 2011) ("declin[ing] to hold . . . as a matter of law" that plaintiff had not alleged Article III standing where plaintiff alleged (1) that it had "paid" Defendant, an Internet application producer, with the value of his PII in exchange, in part, for a promise to reasonably safeguard that PII, and (2) a data breach "caused plaintiff to lose the 'value' of their PII, in the form of their breached personal data").

[214] LaCourt v. Specific Media, Inc., No. SACV 10-1256-GW(JCGx), 2011 U.S. Dist. LEXIS 50543, at *1 (C.D. Cal. Apr. 28, 2011).

conduct injured them by collecting information about their browsing habits without permission or compensation.[215] The district court, while declining "to say that it is categorically impossible for Plaintiffs to allege some property interest that was compromised by Defendant's alleged practices," held that the plaintiffs had not adequately pled injury under this theory.[216] As the court explained, even if the plaintiffs' PII has value, the plaintiffs could not explain how defendants' collection of this information denied them some other opportunity to exploit it.[217]

[70] Subsequent decisions have followed *LaCourt*'s approach: while not denying that PII may have economic value, they have dismissed complaints that fail to explain how plaintiffs could actually exploit the value of their own PII themselves.[218] Other courts have reached similar conclusions when evaluating the theory not as a basis for standing, but rather as a part of a plaintiff's substantive legal claim (for example, meeting a statutory claim's damages requirement).[219] As a recent decision

[215] *See id.* at *3–4.

[216] *Id.* at *11–12.

[217] *See id.* at *12 (stating that Plaintiffs had failed to allege how Defendant's conduct foreclosed them from entering a "value-for-value exchange" with their own data).

[218] *See In re* Google, Inc. Privacy Policy Litig., No. C-12-01382-PSG, 2013 U.S. Dist. LEXIS 171124, at *15–16 (N.D. Cal. Dec. 3, 2013); *In re* Google Android Consumer Privacy Litig., No. 11-MD-02264 JSW, 2013 U.S. Dist. LEXIS 42724, at *14 (N.D. Cal. Mar. 26, 2013); *In re* Google Inc. Cookie Placement Consumer Privacy Litig., 988 F. Supp. 2d 434, 442 (D. Del. 2013); Yunker v. Pandora Media, Inc., No. 11-CV-03113 JSW, 2013 U.S. Dist. LEXIS 42691, at *10, *12 (N.D. Cal. Mar. 26, 2013); Goodman v. HTC Am., Inc., No. C11-1793MJP, 2012 U.S. Dist. LEXIS 88496, at *20–21 (W.D. Wash. June 26, 2012); Low v. Linkedin Corp., No. 11-CV-01468-LHK, 2011 U.S. Dist. LEXIS 130840, at *12–13 (N.D. Cal. Nov. 11, 2011).

[219] *See* Vecchio v. Amazon.com, LLC, No. C11-366RSL, 2012 U.S. Dist. LEXIS 76536, at *12–13 (W.D. Wash. June 1, 2012) ("*Del Vecchio II*"); Del Vecchio v. Amazon.com Inc., No. C11-366-RSL, 2011 U.S. Dist. LEXIS 138314, at *9–10 (W.D. Wash. Nov. 30, 2011) ("*Del Vecchio I*"); *see also In re* JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 327 (E.D.N.Y. 2005); *In re* Doubleclick Privacy Litig., 154 F. Supp. 2d 497, 525 (S.D.N.Y. 2001). The court in *Del Vecchio II* did, with little discussion, find the

described, plaintiffs will not have standing if they cannot explain how "the ability to monetize their PII has been diminished or lost by virtue of" the defendant's actions.[220]

[71] An example of a Plaintiff successfully articulating such financial harm is in *Fraley v. Facebook, Inc*. The personal information at issue in *Fraley* was different than in other cases: the plaintiffs had alleged that Facebook had used, without authorization, images of them for "sponsored stories" that announced on the website that the plaintiffs had endorsed (or, in Facebook parlance, had "liked") a particular business or brand.[221] The district court concluded that the Plaintiffs had standing, in part because they had alleged a violation of a California statutory right against misappropriation of likeness.[222] Additionally, however, the court noted that the precise harm alleged by the plaintiffs was much more "concrete and particularized" than other PII cases, since the plaintiffs could plausibly allege exploitable economic value in "an individual's commercial endorsement of a product or brand to his friends."[223]

2. Breach of Contract

[72] Plaintiffs in data collection cases have also argued that the unauthorized collection or transmittal of their PII breached a contract with the defendant, thus establishing injury-in-fact. Similar to data breach

Plaintiff to have Article III standing, although it appeared to do so either because: (1) the Plaintiff had alleged the dissemination of sensitive financial information, or (2) the Plaintiff alleged unauthorized use of her computer. *See Del Vecchio II*, 2012 U.S. Dist. LEXIS 76536, at *5–6; *see also In re* Google Inc. Cookie Placement Consumer Privacy Litig., 988 F. Supp. 2d 434, 441 (D. Del. 2013) (noting that standing was found in *Del Vecchio II* because Plaintiff alleged dissemination of financial information).

[220] *In re Google Inc. Cookie Placement*, 988 F. Supp. 2d at 442.

[221] *See* Fraley v. Facebook, Inc., 830 F. Supp. 2d 785, 790 (N.D. Cal. 2011).

[222] *See id.* at 796–97.

[223] *Id.* at 796–798 (citing Lujan v. Defenders of Wildlife, 504 U.S. 555, 560–61 (1991)).

cases, plaintiffs have argued that unauthorized collection or transmittal of their PII either (1) breached an express promise by the defendant not to collect or transmit such information or (2) made the defendant's services less valuable than the price that the plaintiff originally paid.

[73] While plaintiffs have had success with this argument, uncertainty remains about what must precisely be alleged. One decision has suggested that a "contract breach by itself" does not constitute injury-in-fact.[224] This statement has yet to be truly tested, however, since any plaintiff to advance a breach-of-contract theory in a data collection case has also alleged some type of injury, even if it is only that they paid more for a product or service than they would have had they known the defendant was exploiting their PII. But whether even *that* establishes injury-in-fact is also unclear. In *In re Linkedin User Privacy Litigation*, the court declined to find injury-in-fact based on the theory that a LinkedIn data breach denied them the "benefit of the bargain" paid for by their membership dues.[225] The court explained that "in cases where the alleged wrong stems from allegations about insufficient performance or how a product functions, courts have required plaintiffs to allege 'something more' than 'overpaying for a 'defective' product.'"[226]

[74] Other courts, meanwhile, appear to have taken the view that an allegation of overpayment can establish injury-in-fact in data collection cases. In *Pirozzi v. Apple*, which also involved transmission of PII to third-parties, the court stated that "[o]verpaying for goods or purchasing goods a person otherwise would not have purchased based upon alleged misrepresentations by the manufacturer would satisfy the injury-in-fact and causation requirements for Article III standing."[227] Two other courts

[224] *See In re* Google, Inc. Privacy Policy Litig., No. C-12-01382-PSG, 2013 U.S. Dist. LEXIS 171124, at *19 (N.D. Cal. Dec. 3, 2013).

[225] *In re* Linkedin User Privacy Litig., 932 F. Supp. 2d 1089, 1092–93 (N.D. Cal. 2013).

[226] *Id.* at 1094 (quoting *In re* Toyota Motor Corp., 790 F. Supp. 2d 1152, 1165 n.11 (C.D. Cal. 2011).

[227] Pirozzi v. Apple, 913 F. Supp. 2d 840, 846–47 (N.D. Cal. 2012).

have reached similar conclusions.[228] These courts have also been strict, however, in requiring plaintiffs to properly plead that a material misrepresentation occurred.[229]

[75] This theory of injury-in-fact remains unsettled for other reasons. For example, *In re Linkedin User Privacy Litigation* cited to decisions from "no-injury" product liability suits—cases where plaintiffs allege that a defect in a line of products, though not occurring to them, has nonetheless harmed them by reducing the value of their particular product.[230] Courts are split generally over how to analyze standing in such lawsuits,[231] and no court has yet considered whether they provide a proper analogy for the breach-of-contract claims asserted in data collection suits. Considering also that most decisions on this topic come from one jurisdiction—the Ninth Circuit—future decisions may remain unpredictable.

3. Impact on Product Performance

[76] In cases where plaintiffs have alleged that defendants collected or transmitted PII from their smartphones, courts have been willing to find

[228] *See In re Google, Inc. Privacy Policy Litig.*, 2013 U.S. Dist. LEXIS 171124, at *24–25; Goodman v. HTC Am., Inc., No. C11-1793MJP, 2012 U.S. Dist. LEXIS 88496, at *14–15 (W.D. Wash. June 26, 2012) ("Plaintiffs' assertion that they overpaid for their smartphones meets the threshold for injury in fact because Defendants allege they would have paid less for the phones had Defendants not misrepresented the relevant features of the phones.").

[229] *Compare Pirozzi*, 913 F. Supp. 2d at 847 (dismissing complaint for lack of standing because "Plaintiff fails to allege specifically which statements she found material to her decision to purchase an Apple Device or App"), *with* Pirozzi v. Apple, Inc., 966 F. Supp. 2d 909, 917–18 (N.D. Cal. 2013) (finding standing based on Plaintiff's amended complaint).

[230] *See Linkedin*, 932 F. Supp. 2d at 1094.

[231] *See* Sheila B. Scheuerman, *Against Liability for Private Risk-Exposure*, 35 HARV. J. L. & PUB. POL'Y 681, 693–709 (2012).

injury-in-fact on the theory that such collection or transmittal adversely impacted the performance of the plaintiffs' phones, typically through shortened battery life. The success of these claims depends on how plausibly the plaintiff can allege that the defendant's conduct has a real, rather than simply *de minimis*, effect on phone performance.[232] Plaintiffs have not succeeded with this theory outside the smartphone context.[233]

4. Emotional Harm

[77] Whether plaintiffs in data collection cases may establish injury-in-fact through emotional harm caused by the collection of potentially embarrassing personal information remains relatively untested. In *Low v. Linkedin Corp.*, the plaintiff alleged that defendant LinkedIn permitted third parties to view its members' personally identifiable browsing history, and that he was "embarrassed and humiliated by the disclosure" of his history.[234] The court declined to find injury-in-fact on this ground, though primarily due to the vagueness of the plaintiff's allegations; as the court

[232] *Compare In re* iPhone Application Litig., 844 F. Supp. 2d 1040,1054 (N.D. Cal. 2012) (finding standing where Defendant's practices allegedly "diminished and consumed iDevice resources, such as storage, battery life, and bandwidth"), *and In re* Google Android Consumer Privacy Litig., No. 11-MD-02264 JSW, 2013 U.S. Dist. LEXIS 42724, at *17 (finding standing where Plaintiffs allege "that their batteries discharged more quickly and that their services were interrupted"), *and Goodman*, 2012 U.S. Dist. LEXIS 88496, at *19 (finding standing where Defendant's alleged practices reduce battery life and "diminish[] the battery's storage capacity"), *with* Yunker v. Pandora Media, Inc., No. 11-CV-03113 JSW, 2013 U.S. Dist. LEXIS 42691, at *14 (denying standing where Plaintiff "does not allege that he noticed any performance problems or that he had problems with his phone because of the diminished memory space"), *and* Hernandez v. Path, Inc., No. 12-CV-01515 YGR, 2012 U.S. Dist. LEXIS 151035, at *4 (N.D. Cal. Oct. 17, 2012) (declining to find standing where Plaintiffs alleged "depletion of two to three seconds of battery capacity").

[233] *See* LaCourt v. Specific Media, Inc., No. SACV 10-1256-GW(JCGx), 2011 U.S. Dist. LEXIS 50543, at *12–13 (concluding that impact of Defendant's cookies on Plaintiff's computer was "*de minimis*" and insufficient to create injury-in-fact).

[234] Low v. Linkedin Corp., No. 11-CV-01468-LHK, 2011 U.S. Dist. LEXIS 130840, at *8 (N.D. Cal. Nov. 11, 2011).

explained, he had "not alleged *how* third party advertisers would be able to infer [his] personal identity" from LinkedIn.[235]

5. Expenditures to Prevent Unauthorized Use of PII

[78] Courts have found injury-in-fact to exist where data collection plaintiffs have plausibly alleged that they have or will spend money to remedy the defendant's allegedly unlawful use of their PII. In *In re Google, Inc. Privacy Policy Litigation*, a plaintiff established injury-in-fact by alleging that Google's change in privacy policy motivated him to purchase a new phone.[236] In *Hernandez v. Path, Inc.*, the plaintiff established injury-in-fact by alleging that he wanted to remove the defendant's tracking software from his phone and doing so would cost him up to $12,250.00.[237]

6. Invasion of Statutory and Constitutional Rights

[79] Finally, multiple courts have found standing in data collection cases under the theory that the plaintiff had alleged the invasion of a statutory or constitutional right. These decisions almost universally cite to the Supreme Court's statement in *Warth v. Seldin* that injury-in-fact "may exist solely by virtue of 'statutes creating legal rights, the invasion of which creates standing.'"[238] Cases from the Ninth Circuit also frequently cite to *Jewel v. National Security Agency*, in which the Ninth Circuit held a plaintiff could establish injury-in-fact by alleging violations of the Electronic Communications Privacy Act ("ECPA"), Foreign Intelligence

[235] *Id.* at *8–9.

[236] *See In re* Google, Inc. Privacy Policy Litig., No. C-12-01382-PSG, 2013 U.S. Dist. LEXIS 171124, at *19–23 (N.D. Cal. Dec. 3, 2013).

[237] *See* Hernandez v. Path, Inc., No. 12-CV-01515 YGR, 2012 U.S. Dist. LEXIS 151035, at *4 (N.D. Cal. Oct. 17, 2012).

[238] Warth v. Seldin, 422 U.S. 490, 500 (1975) (quoting Linda R. S. v. Richard D., 410 U.S. 614, 617 n.3 (1973)).

Surveillance Act ("FISA"), and Stored Communications Act ("SCA").[239] Within the Ninth Circuit, courts have found injury-in-fact established through alleged violations of the Stored Communications Act,[240] the Wiretap Act,[241] and the Video Privacy Protection Act.[242] Courts have likewise found injury-in-fact established through alleged violations of state statutory rights,[243] as well as state constitutional rights to privacy.[244] Courts have found plaintiffs to satisfy any additional requirement that their statutory injury be "particularized" (as opposed to a generalized statutory

[239] Jewel v. Nat'l Sec. Agency, 673 F.3d 902, 906, 912–13 (9th Cir. 2011) (quoting Fec v. Akins, 524 U.S. 11, 20 (1998)).

[240] *See* Low v. Linkedin Corp., 900 F. Supp. 2d 1010, 1021 (N.D. Cal. 2012); *In re* iPhone Application Litig., 844 F. Supp. 2d 1040, 1054–55; Cousineau v. Microsoft Corp., 992 F. Supp. 2d 1116, 1121–23 (W.D. Wash. 2012); Gaos v. Google Inc., No. 5:10-CV-4809 EJD, 2012 U.S. Dist. LEXIS 44062, at *12–13 (N.D. Cal. Mar. 29, 2012).

[241] *See In re iPhone Application Litig.*, 844 F. Supp. 2d at 1055; *In re* Facebook Privacy Litig., 791 F. Supp. 2d 705, 712 (N.D. Cal. 2011); *In re* Zynga Privacy Litig., No. C 10-04680 JW, 2011 U.S. Dist. LEXIS 154237, at *7–8 (N.D. Cal. June 15, 2011), *aff'd* 750 F.3d 1098 (9th Cir. 2014).

[242] *See In re* Hulu Privacy Litig., No. C 11-03764 LB, 2012 U.S. Dist. LEXIS 80601, at *16 (N.D. Cal. June 11, 2012).

[243] *See* Fraley v. Facebook, 830 F. Supp. 2d 785, 797 (N.D. Cal. 2011); *In re* Google, Inc. Gmail Litig., No. 13-MD-02430-LHK, 2013 U.S. Dist. LEXIS 172784, at *65 (N.D. Cal. Sept. 26, 2013); Goodman v. HTC Am., Inc., No. C11-1793MJP, 2012 U.S. Dist. LEXIS 88496, at *23 (W.D. Wash. June 26, 2012).

[244] *See Low*, 900 F. Supp. 2d at 1021; Yunker v. Pandora Media, Inc., No. 11-CV-03113 JSW, 2013 U.S. Dist. LEXIS 42691, at *16–17 (N.D. Cal. Mar. 26, 2013); *Goodman*, 2012 U.S. Dist. LEXIS 88496, at *38–41. These decisions have apparently viewed state constitutional rights as equivalent to statutory rights for purposes of Article III standing. *See, e.g.*, *Goodman*, 2012 U.S. Dist. LEXIS 88496, at *38–39 ("A state constitutional or statutory provision conferring standing does not replace the requirements of Article III, but it serves to expand standing in federal court 'to the full extent permitted under Article III.'") (quoting Bennett v. Spear, 520 U.S. 154, 165 (1997)).

grievance), so long as their specific PII has been affected by the alleged statutory violation.[245]

[80] Parties relying on decisions from the Ninth Circuit should be aware that the outer parameters of *Warth* remain unsettled,[246] and thus not every circuit is guaranteed to agree with *Jewel*'s holding. For example, one of the few data breach cases to consider statutory injury, *In re Barnes & Noble Pin Pad Litigation*, rejected injury-in-fact on the alleged basis of defendant's violation of state breach notification laws and explained that "[p]laintiffs must plead an injury beyond a statutory violation to meet the standing requirement of Article III."[247]

IV. INJURY-IN-FACT IN DATA BREACH AND DATA COLLECTION CASES AFTER *CLAPPER*

[81] As the above cases show, federal courts remain fractured in their approach to injury-in-fact in data breach and data collection cases. While courts have reached consistent conclusions with respect to some theories of standing, they have sharply disagreed over others. *Clapper*, which discusses both the collection of data and the ability of plaintiffs to prove injury-in-fact through the risk of future harm, presents an opportunity to resolve some of these differences of opinion. Yet *Clapper*'s precise effect on data privacy cases remains unsettled. Data collection cases have not addressed Justice Alito's majority opinion in any significant detail, while the few data breach decisions to do so have drawn different conclusions

[245] *See, e.g.*, *Low*, 900 F. Supp. 2d at 1021 ("Because Plaintiffs have alleged that *their information* has been disclosed to third parties by LinkedIn's policies, Plaintiffs have sufficiently articulated, with particularity, injury as to themselves for the purposes of Article III standing.").

[246] The Supreme Court recently granted, and then dismissed as improvidently granted, certiorari in a case that contributed to an existing split over the ability of litigants to establish standing *solely* on the invasion of statutory rights (that is, without any proof of real-world injury). *See* First Am. Fin. Corp. v. Edwards, 132 S. Ct. 2536 (2012).

[247] *In re* Barnes & Noble Pin Pad Litig., No. 12-cv-8617, 2013 U.S. Dist. LEXIS 125730,at *8–9 (N.D. Ill. Sept. 3, 2013) (citing Kyles v. J.K. Guardian Sec. Servs., 222 F.3d 289, 295 (7th Cir. 2000)).

about *Clapper*'s effect on existing standing law. Still, these cases do suggest, at the very least, that lower courts are inclined to interpret *Clapper* as rejecting the idea that *any* increase in a risk of future harm may support injury-in-fact. While not a sweeping, across-the-board adoption of *Clapper*'s "certainly impending" language, this development would still have significant consequences for data privacy litigation.

A. *Clapper*'s Impact in Lower Courts So Far

1. Data Breach Cases

[82] To date, *Clapper* has received extended analysis in seven data breach cases: *In re Sony Gaming Networks and Customer Data Security Breach Litigation*,[248] *In re Barnes & Noble Pin Pad Litigation*,[249] *Galaria v. Nationwide Mutual Insurance Co.*,[250] *Strautins v. Trustwave Holdings, Inc.*,[251] *In re Science Applications International Corp. (SAIC) Backup Tape Data Theft Litigation*,[252] *Moyer v. Michaels Stores, Inc*,[253] and *In re Adobe Systems, Inc. Privacy Litigation*.[254] These decisions have reached different conclusions about *Clapper*'s impact on standing law. The courts in *In re Sony*, *Moyer*, and *In re Adobe* expressly disavowed that *Clapper*

[248] *See In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F.Supp.2d 942, 960–63 (S.D. Cal. 2014).

[249] *See In re Barnes & Noble*, 2013 U.S. Dist. LEXIS 125730, at *7–12.

[250] *See* Galaria v. Nationwide Mutual Ins. Co., 998 F. Supp. 2d 646, 651–57 (S.D. Ohio 2014).

[251] *See* Strautins v. Trustwave Holdings, Inc., No. 12 C 09115, 2014 U.S. Dist. LEXIS 32118, at *11–14, *17–23 (N.D. Ill. Mar. 12, 2014).

[252] *See In re* SAIC Backup Tape Data Theft Litig., No. 12–347 (JEB), 2014 U.S. Dist. LEXIS 64125, at *19–33 (D.D.C. May 9, 2014).

[253] *See* Moyer v. Michaels Stores, Inc., No. 14 C 561, 2014 U.S. Dist. LEXIS 96588, at *14–16 (N.D. Ill. July 14, 2014).

[254] *See In re* Adobe Sys., Inc. Privacy Litig., No 13-CV-05226-LHK, 2014 U.S. Dist. LEXIS 124126, at *16–32 (N.D. Cal. Sep. 4, 2014).

constituted any sort of substantial reworking of standing doctrine.[255] The other decisions, meanwhile, relied, at least in part, on *Clapper*'s "certainly impending" language to dismiss claims of injury premised on an increased future risk of identity theft.[256]

[83] *In re Sony* followed a previous decision of the Southern District of California, which had held that customers of Sony who had their personal information compromised in a massive data breach could establish injury-in-fact on the basis of an increased risk of future identity theft, even without allegations that any information had actually been used by third parties.[257] Sony asked the court to revisit that holding in light of *Clapper*.[258] The court did so, and concluded that *Clapper* did not change its earlier conclusion that the plaintiffs had standing to sue.[259] While the court noted *Clapper*'s "certainly impending" language differed from the "real and immediate" language used by the Ninth Circuit in *Krottner*, it concluded that "*Clapper* did not set forth a new Article III framework, nor did the Supreme Court's decision overrule previous precedent requiring that the harm be 'real and immediate.'"[260] The *Clapper* plaintiffs' "speculative chain of possibilities," the *Sony* court appeared to believe, would have been insufficient to establish injury-in-fact even under

[255] *See In re Sony*, 996 F. Supp. 2d at 961; *In re Adobe*, 2014 U.S. Dist. LEXIS 124126 *24–27; *Moyer*, 2014 U.S. Dist. LEXIS 96588, at *12, *15.

[256] *See In re* Barnes & Noble Pin Pad Litig., No.12-cv-8617, 2013 U.S. Dist. LEXIS 125730, at *7–12 (N.D. Ill. Sep. 3, 2013); *Galaria*, 998 F. Supp. 2d at 657; *Strautins*, 2014 U.S. Dist. LEXIS 32118, at *13; *In re SAIC*, 2014 U.S. Dist. LEXIS 64125, at *50–51.

[257] *See In re Sony*, 996 F. Supp. 2d at 962–63.

[258] *See id.* at 960.

[259] *See id.* at 961.

[260] *Id.*

Krottner, thus suggesting that *Clapper* had simply "reiterated an already well-established framework" for assessing injury-in-fact.[261]

[84] *In re Barnes & Noble*, meanwhile, involved a "skimming" security breach at the book retailer through which criminals succeeded in collecting credit and debit card numbers used by customers on the store's pin pad machines.[262] At the time the plaintiffs sued Barnes & Noble, only one had suffered a fraudulent charge, which had been previously reimbursed.[263] The district court dismissed the plaintiffs' various theories for standing.[264] Most notably, the court rejected as too speculative the plaintiffs' claims of an increased risk of future identity theft, explaining that "[a]s the Supreme Court held in *Clapper*, 'threatened injury must be *certainly impending* to constitute injury-in-fact, and . . . [a]llegations of *possible* future injury are not sufficient.'"[265] The court likewise rejected the plaintiffs' theory of standing based on their mitigating expenses, noting that "such expenses would not qualify as actual injuries under *Clapper*" and that "Plaintiffs 'cannot manufacture standing by incurring costs in anticipation of non-imminent harm.'"[266] The court also rejected the plaintiffs' theory of standing based on anxiety and emotional distress, as "there is no indication there is an imminent threat" of identity theft.[267]

[261] *Id.*

[262] *See In re* Barnes & Noble Pin Pad Litig., No.12-CV-8617, 2013 U.S. Dist. LEXIS 125730, at *2–3 (N.D. Ill. Sep. 3, 2013).

[263] *See id.* at *4–5.

[264] *See id.* at *16–17.

[265] *Id.* at *8 (alteration in original) (quoting *Clapper*, 133 S. Ct. at 1147).

[266] *Id.* at *11 (quoting *Clapper*, 133 S. Ct. at 1155).

[267] *Id*. at *13–14.

[85] The Northern District of Illinois again addressed *Clapper*'s impact on data breach litigation in *Strautins v. Trustwave Holdings, Inc.*[268] At issue in *Strautins* was a breach at the South Carolina Department of Revenue, whereby hackers were able to obtain the Social Security numbers of millions of individuals, as well as hundreds of thousands of tax records and credit and debit card numbers.[269] Plaintiff, a South Carolina taxpayer, brought suit against the data security company responsible for protecting the Department of Revenue, alleging the company's negligence had caused her injury in the form of an increased risk of identity theft.[270] The district court, however, concluded that "*Clapper* compels rejection of [Plaintiff's] claim that an increased risk of identity theft is sufficient to satisfy the injury-in-fact requirement for standing."[271] According to the court, any risk of identity theft raised by the plaintiff did not rise to *Clapper*'s "certainly impending" standard.[272] Likewise, *Clapper* required rejection of plaintiff's argument that she had standing based on present expenses to mitigate the risk of future identity theft.[273]

[86] Unlike in *In re Barnes & Noble*, the court in *Strautins* attempted to reconcile *Clapper* with the Seventh Circuit's earlier standing decision in *Pisciotta*.[274] The district court expressed skepticism that *Pisciotta*'s statement about injury-in-fact—that it could arise from a mere increase in

[268] *See* Struatins v. Trustwave Holdings, Inc., No. 12 C 09115, 2014 U.S. Dist. LEXIS 32118 (N.D. Ill. Mar. 12, 2014).

[269] *See id.* at *1.

[270] *See id.* at *2.

[271] *See id.* at *11.

[272] *See id.* at *13.

[273] *See id.* at *13–14 n.9.

[274] *See Strautins*, 2014 U.S. Dist. LEXIS 32118, at *18, *20–22.

the risk of future harm—had any continuing validity after *Clapper*.[275] In the court's view, "*Clapper* seems rather plainly to reject the premise, implicit in *Pisciotta* and fairly explicit in *Elk Grove Village*, that any marginal increase in risk is sufficient to confer standing."[276] The court noted that *Clapper* had "expressly rejected the Second Circuit's 'objectively reasonable likelihood' standard."[277] The court ultimately hedged its rejection of *Pisciotta*, however, by dismissing the plaintiff's complaint on the alternative ground that she had not plausibly alleged the theft of her own PII and thus had failed to state a claim.[278]

[87] In *Galaria v. Nationwide Mutual Insurance Co.*, the Southern District of Ohio similarly relied on *Clapper* to reject a claim of injury-in-fact premised on an increased risk of future identity theft.[279] Like in *Strautins*, the plaintiffs in *Galaria* sued after hackers gained entry into the defendant's computer network, although neither plaintiff alleged that their specific information had been misused.[280] The district court held the

[275] *See id.* at *17–19.

[276] *Id.* at *18.

[277] *Id.* at *18–19.

[278] *See id.* at *28–29. A subsequent decision from the Northern District of Illinois, *Remijas v. Neiman Marcus Group*, No. 14 C 1735, 2014 WL 4627893 (N.D. Ill. Sep. 16, 2014), likewise found *Clapper* to preclude standing for a group of data breach plaintiffs, though without expressly finding *Pisciotta* to be abrogated. The court in *Remijas* suggested both that *Pisciotta* was factually reconcilable with *Clapper*'s "certainly impending" standard (a premise that seems to be rejected in cases such as *Strautins*) and that *Clapper*'s "certainly impending" requirement was less rigorous outside the contexts of national security and constitutional law. *See id.* at *3; *see also Tierney v. Advocate Health & Hosp. Corp.*, No. 13 CV 6237, at *2 (N.D. Ill. Sep. 4, 2014) (holding that only those data breach plaintiffs who had been notified of fraudulent activity had alleged injury-in-fact, though not analyzing the impact of *Clapper* on prior Seventh Circuit standing law).

[279] *See* Galaria v. Nationwide Mut. Ins. Co., No. 2:13-CV-118, 2014 U.S. Dist. LEXIS 23798, at *22–24 (S.D. Ohio Feb. 10, 2014).

[280] *See id.* at *2–4.

plaintiffs could not establish injury-in-fact based on an alleged increased risk of identity theft, as such risk was not, as *Clapper* required, "certainly impending."[281] The court also relied on *Clapper* in rejecting the plaintiffs' theory of standing based on their present expenditures to mitigate against the risk of future identity theft, and quoted *Clapper*'s statement that litigants "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."[282] The court also rejected the plaintiffs' arguments for injury-in-fact based on "loss of privacy" and on the alleged deprivation of value of their PII.[283]

[88] The district court in *Galaria*, like the court in *Strautins*, also considered *Clapper*'s impact on previous decisions about data breach litigation and Article III standing.[284] The court noted that other data breach cases where plaintiffs were found to have standing—including both *Krottner* and *Pisciotta*—had been decided prior to *Clapper*.[285] The court further noted, as did the court in *Strautins*, that *Clapper* had "specifically rejected the idea that an injury is certainly impending if there is an 'objectively reasonable likelihood' it will occur."[286]

[89] In *SAIC*, the district court reached conclusions similar to those of *Strautins* and *Galaria*. However, unlike those cases, *SAIC* arose from a theft of data tapes where it was unclear that the thief was even aware that

[281] *See id.* at *23–24.

[282] *Id.* at *24–25 (citing Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1143 (2013)).

[283] *See id.* at *28–29 (concluding that the plaintiffs would have standing to pursue a tort claim for invasion of privacy, but finding that their complaint failed to state such a claim).

[284] *See id.* at *22.

[285] *See Galaria*, 2014 U.S. Dist. LEXIS 23798, at *20–22.

[286] *Id.* at *22 (citing *Clapper*, 133 S. Ct. at 1147).

she procured sensitive personal data.[287] The district court held that the plaintiffs could not establish standing based on an increased risk of future identity theft.[288] Even if that risk was, as the plaintiffs alleged, 9.5 times higher after the breach occurred, *Clapper* established that "[t]he degree by which the harm has increased is irrelevant—instead, the question is whether the harm is certainly impending."[289] The court further noted that the plaintiff's alleged risk of identity theft failed to meet even *Clapper*'s "substantial risk" language.[290]

[90] *SAIC* also considered the effect that *Clapper* had on previous data privacy decisions.[291] Like *Strautins* and *Galaria*, it viewed *Clapper* as calling into question decisions such as *Krottner* and *Pisciotta*.[292] It described decisions finding standing based on an increased risk of identity theft as "decided pre-*Clapper* or rel[iant] on pre-*Clapper* precedent and are, at best, thinly reasoned."[293] The court rejected the continued viability of an "increased risk" theory of standing: "After all, an *increased risk* or *credible threat* of impending harm is plainly different from *certainly impending* harm, and certainly impending harm is what the Constitution and *Clapper* require."[294]

[287] *See In re* SAIC Backup Tape Data Theft Litig., No. 12-347 (JEB), 2014 U.S. Dist. LEXIS 64125, at *1 (D.D.C. May 9, 2014).

[288] *See id.* at *7.

[289] *Id.* at *22.

[290] *See id.* at *26–27.

[291] *See id.* at *31–32.

[292] *See id.* at *31–32.

[293] *In re* SAIC, 2014 U.S. Dist. LEXIS 64125, at *31–32.

[294] *Id.* at *32–34.

[91] In *Moyer*, by contrast, another judge from the Northern District of Illinois disagreed that *Clapper* had abrogated the Seventh Circuit's decision in *Pisciotta*.[295] The plaintiffs in *Moyer* alleged that they were at an increased risk of identity theft after using their credit and debit cards at Michaels Stores within a time period during which Michaels may have experienced a data security attack.[296] Though the district court ultimately dismissed the plaintiffs' complaint for failure to state a claim, it first concluded that the plaintiffs had alleged Article III injury-in-fact due to an elevated risk of identity theft.[297]

[92] Notably, the court in *Moyer* disagreed with any suggestion from *Strautins* and *Barnes & Noble* that *Clapper* had abrogated the Seventh Circuit's decision in *Pisciotta*.[298] According to the court, *Pisciotta* remained good law for two reasons.[299] First, *Clapper* involved a constitutional challenge to a federal national security law, and the extent to which its standing analysis applied outside that specific context was "an open question."[300] Second, the court noted that other Supreme Court decisions, such as *Susan B. Anthony List v. Driehaus*[301] and *Geertson Seed Farms*,[302] demonstrate that the Supreme Court has also applied a less rigorous standing analysis than *Clapper*'s for allegations of future

[295] *See* Moyer v. Michaels Stores, Inc., No. 14 C 561, 2014 U.S. Dist. LEXIS 96588, at *15 (N.D. Ill. July 14, 2014).

[296] *See id.* at *2.

[297] *See id.* at *19, *24.

[298] *See id.* at *14–15.

[299] *See id.* at *15–16, *19.

[300] *Id.* at *15.

[301] Susan B. Anthony List v. Driehaus, 134 S. Ct. 2334, 2343 (2014) (permitting pre-enforcement challenge to state statute criminalizing false statements about candidates during political campaigns).

[302] Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 155 (2010).

injury.[303] The court further observed that *Clapper* was factually distinguishable from the plaintiffs' claims because while at least one customer of Michaels had reported identity theft after the security breach, in *Clapper*, there was "no evidence that the relevant risk of harm had ever materialized in similar circumstances."[304]

[93] Most recently, in *In re Adobe*, the Northern District of California agreed with *In re Sony* that, despite *Clapper*, the Ninth Circuit's decision in *Krottner* remained good law.[305] The claims in *In re Adobe* arose from a sophisticated, weeks-long hacking operation through which hackers obtained and decrypted the personal information and credit card numbers of over 38 million Adobe customers.[306] Citing to *SAIC*, *Strautins*, and *Galaria*, among other cases, Adobe argued that the plaintiffs could not establish injury-in-fact through an alleged increased risk of identity theft.[307] The court disagreed, and noted that "*Clapper* did not change the law governing Article III standing."[308] As the court explained, *Krottner* was already "closer to *Clapper*'s 'certainly impending' language" than it was to the Second Circuit's rejected "objective reasonable likelihood" standard.[309] Regardless, the court found the plaintiffs' allegations, which involved an elaborate crime clearly designed to obtain personal information, some of which had already had been misused, to plausibly allege "certainly impending" harm.[310]

---

[303] *See Moyer*, 2014 U.S. Dist. LEXIS 96588, at *16–18.

[304] *Id.* at *19.

[305] *See In re* Adobe Sys., Inc. Privacy Litig., No. 13-CV-05226-LHK, 2014 U.S. Dist. LEXIS 124126, at *32 (N.D. Cal. Sep. 4, 2014).

[306] *See id.* at *6–7.

[307] *Id.* at *21.

[308] *Id.* at *24

[309] *Id.* at *26.

[310] *See id.* at *28.

[94] Other data breach decisions have mentioned *Clapper*, albeit with less analysis. The District of Kansas cited *Clapper* in a decision finding no standing where no data breach had been alleged to have occurred—a position courts consistently reached even before *Clapper*.[311] Likewise, the District of New Jersey cited *Clapper* in *Polanco v. Omnicell, Inc.*,[312] which dismissed for lack of standing a plaintiff who claimed that she suffered injury-in-fact because she avoided treatment at hospitals served by the defendant company, which had previously experienced a data breach and which the plaintiff believed to employ inadequate data security measures.[313] The district court cited to *Clapper* in dismissing this claim, though its analysis suggested that it did not view *Clapper* as changing in any substantive way the Third Circuit's binding analysis in *Reilly*.[314]

[95] These opinions demonstrate different perspectives on how *Clapper* impacts existing standing law. On one side, decisions such as *Strautins*, *Galaria*, and *SAIC* view *Clapper* as abrogating appellate decisions like *Pisciotta*. On the other side, *In re Sony*, *Moyer*, and *In re Adobe* assert that *Clapper* did not effect any sort of substantial change in standing law.[315] These opinions also demonstrate the *Clapper* majority opinion's

[311] *See* Hammer v. Sam's East, Inc., No. 12-CV-2618-CM, 2013 U.S. Dist. LEXIS 98707, at *4–8 (D. Kan. July 16, 2013).

[312] *See* Polanco v. Omnicell, Inc., 988 F. Supp. 2d 451, 466 (D.N.J. 2013).

[313] *See id.* at 468–71.

[314] *See id.* at 466–67.

[315] Another example of courts' taking fundamentally different views on *Clapper* is a comparison of *In re Sony* with *Polanco*. While both decisions found *Clapper* not to have disrupted existing standing law, *In re Sony* viewed *Clapper* as consistent with the Ninth Circuit's decision in *Krottner*, while *Polanco* viewed it as consistent with the Third Circuit's decision in *Reilly*. *Compare In re* Sony, 996 F. Supp. 942, 961–63 ("the Court finds both *Clapper* and *Krottner* controlling"), *with Polanco* 988 F. Supp. 2d at 466 (noting the similarity between the holdings in *Reilly* and *Clapper*).

open-ended nature.[316] Though *Strautins*, *Galaria*, and *SAIC* recite *Clapper*'s "certainly impending" language, no decision conclusively endorses such language as the governing standard for assessing all claims of injury-in-fact premised on future harm. Rather, all three opinions follow *Clapper*'s approach and decline to decide whether a "substantial risk" standard might apply in other circumstances.[317]

[96] Still, the courts in *Barnes & Noble*, *Strautins*, *Galaria*, *SAIC*, and *Polanco* all interpreted *Clapper* as imposing *some* sort of objective imminence threshold that an increased risk of harm must meet before it constitutes injury-in-fact. That is, all five decisions do appear to agree that, under *Clapper*, injury-in-fact requires something more than just a slight risk of future harm. Even *In re Sony* and *In re Adobe*, which take more limited views of *Clapper*'s effect on standing law, reached arguably consistent results. Though *In re Sony* admittedly cites with approval decisions such as *Pisciotta*, [318] the district courts in both cases held only that *Clapper* did not change the Ninth Circuit's "real and immediate" requirement for future harm—an arguably more rigorous standard than the "increased risk" language rejected in *Strautins*, *Galaria*, and *SAIC*.[319]

[316] *See* Strautins v. Trustwave Holdings Inc., No. 12 C 09115, 2014 U.S. Dist. LEXIS 32118, at *5 n.11 (N.D. Ill. Mar. 12, 2014) (noting that "the import of *Clapper* for standing analysis in the Seventh Circuit a question on which reasonable minds may differ").

[317] *See Strautins*, 2014 U.S. Dist. LEXIS 32118 at *8–9; *Galaria*, 2014 U.S. Dist. LEXIS 23798 at *14–15; *In re SAIC*, 2014 U.S. Dist. LEXIS 64125 at *25–26.

[318] *See In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 961–62 n.8 (citing favorably to *Pisciotta* and other decisions stating that a mere increased risk of harm can support standing).

[319] *See id.* at 961. *In re* Adobe Sys., Inc. Privacy Litig., No. 13-CV-05226-LHK, 2014 U.S. Dist. LEXIS 124126, at *25–26 (N.D. Cal. Sep. 4, 2014).

[97] *Moyer*, by contrast, appears to have taken a position less reconcilable with an objective imminence requirement.[320] Unlike in *In re Sony*, the court in *Moyer* did rely on *Pisciotta* for its standing analysis.[321] And the court concluded that plaintiffs had established standing by alleging "a credible, non-speculative risk of future harm"—a standard that would appear to be less rigorous than even the Ninth Circuit's "real and immediate" standard.[322] Still, *Moyer*'s more expansive view of standing remains the minority among the post-*Clapper* data breach cases.

[98] In short, while lower courts may have reached different conclusions about the extent of *Clapper*'s effect on data privacy litigation, they have been more consistent in viewing *Clapper* as rejecting the proposition that *any* increase risk of future harm can support Article III standing. Though this conclusion is consistent with much of the standing law to come before *Clapper*, it is in tension with some decisions, such as the Seventh Circuit's in *Pisciotta*. Whether *Clapper* will ultimately result, as *Strautins*, *Galaria*, and *SAIC* suggest, in the abrogation of decisions like *Pisciotta* remains to be seen.

2. Data Collection Cases

[99] With respect to data collection lawsuits, *Clapper* has been more notable in its absence than in its presence. To date, *Clapper* has appeared as a brief citation in three data collection cases: *Yunker*, *In re Google Android Consumer Privacy Litigation*, and *In re iPhone Application Litigation*.[323] While both *Yunker* and *In re Google Android* quote

[320] *See* Moyer v. Michaels Stores, Inc., No. 14 C 561, 2014 U.S. Dist. LEXIS 96588 at *19 (N.D. Ill. July 14, 2014).

[321] *See id.* (noting that holding on standing "follows from *Pisciotta*").

[322] *See id.* at *17.

[323] Yunker v. Pandora Media, Inc., No. 11-CV-03113 JSW, 2013 U.S. Dist. LEXIS 42691, at *8 (N.D. Cal. Mar. 26, 2013); *In re* Google Android Consumer Privacy Litig., No. 11-MD-02264 JSW, 2013 U.S. Dist. LEXIS 42724, at *11 (N.D. Cal. Mar. 26,

Clapper's "certainly impending" language as part of their general recitation of standing requirements,[324] neither case suggests that *Clapper* affects previous standing doctrine. And other courts, whether cognizant of *Clapper* or not, have continued to find injury-in-fact established for data collection plaintiffs under theories of overpayment for goods and services,[325] impact on device performance,[326] and invasion of statutory rights.[327]

A. *Clapper* and Data Privacy Cases Going Forward

[100] An analysis of *Clapper* itself supports the conclusions reached by most of the lower courts that have considered its effect on standing law. While the majority opinion's "certainly impending" language suggests a high hurdle for plaintiffs seeking to prove injury-in-fact premised on an increased risk of future harm, the opinion also leaves open the possibility that such a requirement may not apply in all cases.[328] The majority's rejection of the Second Circuit's "objectively reasonable likelihood"[329]standard, meanwhile, is much more unequivocal, and thus much more likely to affect standing cases going forward. Still, a far-reaching impact is not guaranteed: *Clapper* is unclear enough about the

2013); *In re* iPhone Application Litig., No. 11-MD-02250-LHK, 2013 U.S. Dist. LEXIS 169220, at *24 (N.D. Cal. Nov. 25, 2013).

[324] *See Yunker*, 2013 U.S. Dist. LEXIS 42691 at *8; *In re Google*, 2013 U.S. Dist. LEXIS 42724 at *11–12.

[325] *See, e.g.*, *In re* Google, Inc. Privacy Policy Litig., No. C-12-01382-PSG, 2013 U.S. Dist. LEXIS 171124, at *23–24 (N.D. Cal. Dec. 3, 2013).

[326] *See, e.g.*, *id.* at *19–20.

[327] *See, e.g.*, *In re* Google Inc. Cookie Placement Consumer Privacy Litig., 988 F. Supp. 2d 434, 442 (D. Del. 2013).

[328] Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1150 n.5 (2013).

[329] *Id.* at 1147.

scope of cases to which it applies that lower courts could, as *Moyer* suggests, effectively limit it to the national security context.[330] Moreover, even if courts do generally adopt a broad reading of *Clapper*, it may simply have the effect of pushing data privacy litigants toward other theories of standing that do not depend on future injury.

[101] As mentioned above, viewed in light of the issues germane to data breach and data collection cases, *Clapper*'s most notable aspect is its statement that threatened harm must be "certainly impending"[331] in order to constitute injury-in-fact. Indeed, this language from *Clapper* has been its most widely quoted among lower courts, and has obvious relevance for cases where injury is alleged in the form of either an increased risk of future identity theft or present expenses incurred to mitigate that risk.[332] But as explained earlier, the *Clapper* majority opinion reserves decision on whether "certainly impending " is the only applicable standard for assessing threatened injuries.[333] In a footnote it concedes that "[o]ur cases do not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about,"[334] and recognizes that a separate "substantial risk" standard may also exist for injury-in-fact premised on the risk of future harm.[335] Thus, and as the decisions discussed above demonstrate, while courts may choose to adopt *Clapper*'s

[330] *See* Moyer v. Michaels Stores, No. 14 C 561, 2014 U.S. Dist. LEXIS 96588, at *19 (N.D. Ill. July 14, 2014); *see also In re* Adobe Sys., Inc. Privacy Litig., No. 13-CV-05226-LHK, 2014 U.S. Dist. LEXIS 124126, at *25 (N.D. Cal. Sep. 4, 2014) (observing that "*Clapper*'s discussion of standing arose in the sensitive context of a claim that other branches of government were violating the Constitution, and the U.S. Supreme Court noted that its standing analysis was unusually rigorous as a result").

[331] *Clapper*, 133 S. Ct. at 1155.

[332] *See supra* section III.A.

[333] *See Clapper*, 133 S. Ct. at 1150 n.5.

[334] *Id*.

[335] *Id*.

"certainly impending" language as the substantive requirement for alleging injury-in-fact in future data breach cases, *Clapper* itself does not necessarily compel them to do so.[336]

[102] *Clapper* is much more unequivocal, however, in its rejection of the Second Circuit's "objectively reasonable likelihood" standard for assessing future injury.[337] This aspect of the majority opinion may be more likely to alter the existing legal landscape on data litigation and injury-in-fact. Indeed, it is the rejection of the Second Circuit's standard, rather than the endorsement of a "certainly impending" standing, that *Strautins* and *Galaria* view as abrogating or potentially abrogating previous circuit court opinions.[338] This does not mean, of course, that *Clapper* necessarily abrogates the *holdings* of decisions like *Pisciotta* or *Krottner*; lower courts may still conclude, like in *In re Sony* and *In re Adobe*, that the risk of injury in those cases satisfied whatever minimum threshold of probability that *Clapper* imposed. Still, if *Clapper* makes clear that an "objectively reasonable likelihood" standard is inappropriate for assessing injury-in-fact based on a risk of future harm, it becomes difficult to see how establishing injury-in-fact based on only a "small" or "increased" risk of harm is not also inappropriate.

[103] Aside from the scope of *Clapper*'s holding, courts in data privacy cases may also be able to distinguish the decision on factual grounds.

---

[336] In its most recent statement about standing and future harm, the Court continued to leave this issue open. *See* Susan B. Anthony List v. Driehaus, 134 S. Ct. 2334, 2341 (2014) ("An allegation of future injury may suffice if the threatened injury is 'certainly impending,' or there is a ''substantial risk' that the harm will occur.") (quoting *Clapper*, 133 S. Ct. at 1150 n.5).

[337] *See Clapper*, 133 S. Ct. at 1147 ("As an initial matter, the Second Circuit's 'objectively reasonable likelihood' standard is inconsistent with our requirement that 'threatened injury must be certainly impending to constitute injury in fact.'") (quoting Whitmore v. Arkansas, 495 U.S. 149, 158 (1990)).

[338] *See* Strautins v. Trustwave Holdings, Inc., No. 12 C 09115, 2014 U.S. Dist. LEXIS 32118, at *18–19 (N.D. Ill. Mar. 12, 2014); Galaria v. Nationwide Mut. Ins. Co., No. 2:13-CV-118, 2014 U.S. Dist. LEXIS 23798, at *22 (S.D. Ohio Feb. 10, 2014).

Justice Alito began *Clapper*'s standing analysis by noting the presence of two factors that, in his view, called for a conservative standing analysis: (1) that the plaintiffs' claims would "force [the Court] to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional";[339] and (2) that the plaintiffs' claims would require the Court "to review actions of the political branches in the fields of intelligence gathering and foreign affairs."[340] Neither of these factors is typically present in a data breach case. Still, most courts so far have not construed this potion of *Clapper* as precluding its application to data breach cases.

[104] *Clapper*'s impact on other theories of standing used in data privacy cases is not obvious. Most of these other theories allege the existence of a present, rather than future, injury.[341] Perhaps most notably, *Clapper* would seemingly have little effect on plaintiffs who allege injury from an invasion of statutory rights—a theory of standing that may become increasingly available to data privacy plaintiffs if legislatures enact additional statutory causes of action.[342] If lower courts decide to read

[339] *Clapper*, 133 S. Ct. at 1147.

[340] *Id.*; *see also LEADING CASE: II. Federal Jurisdiction and Procedure: C. Standing-Challenges to Government Surveillance*-Clapper v. Amnesty International USA, 127 HARV. L. REV. 298, 298 (2013) (arguing that *Clapper*'s "certainly impending" language "should only be applied to litigants challenging governmental action in foreign affairs or national security").

[341] A possible exception may be standing premised on anxiety and emotional distress due to the perceived risk of future identity theft, which some courts have tied to the reasonableness of the threat causing the anxiety. The plaintiffs in *Clapper* did not make any sort of emotional-distress claim, however.

[342] *See* Patricia Cove, Note, *Giving Consumers a Leg to Stand On: Finding Plaintiffs a Legislative Solution to the Barrier from Federal Courts in Data Security Breach Suits*, 62 CATH. U. L. REV. 765, 769 (2013) (advocating for legislation to give plaintiffs a data breach suits a statutory cause of action, thereby overcoming previous decisions denying such plaintiffs standing). The plaintiffs in both *Strautins* and *Galaria*, for example, alleged violations of the Fair Credit Reporting Act in addition to their other claims and failed. *See Strautins*, 2014 U.S. Dist. LEXIS 32118, at *7; *Galaria*, 2014 U.S. Dist. LEXIS 23798, at *2. *But see In re* Adobe Sys., Inc. Privacy Litig., 13-CV-05226-LK,

Clapper broadly, more plaintiffs may plead these alternative theories of standing in place of theories premised on the risk of future harm.

[105] *Clapper* accordingly has the potential to change how injury-in-fact is alleged in data privacy cases, particularly if courts continue to find that its rejection of the Second Circuit's "objectively reasonable likelihood" standard requires abandonment of similarly lax language about injury-in-fact found in other circuits' case law. But given the other potential avenues for plaintiffs to assert injury-in-fact in data breach cases, it is less certain that *Clapper* will significantly reduce the number of data privacy plaintiffs who manage to proceed forward with their claims.

V. CONCLUSION

[106] Even after *Clapper*, federal courts continue to differ in their conclusions about the Article III standing of plaintiffs in data breach and data collection lawsuits. Despite this lack of consensus, the data privacy decisions issued in the wake of *Clapper* do suggest that lower courts, while not likely to all impose *Clapper*'s "certainly impending" language as an across-the-board standing requirement for plaintiffs, are nonetheless generally inclined to view *Clapper* as a rejection of the laxer standing requirements of decisions such as the Seventh Circuit's in *Pisciotta* and even the Ninth Circuit's in *Krottner*. Such a view, if widely adopted, could have a significant impact on data privacy litigation. Plaintiffs alleging injury-in-fact due to an increased risk of future harm will more likely encounter a rigorous, objective judicial analysis of how imminent the alleged risk of harm actually is. This in turn may push data privacy plaintiffs to other theories of standing, such as invasion of statutory rights, which do not depend on future harm. In sum, while *Clapper*'s exact impact on data privacy litigation still remains undetermined, it has already demonstrated its potential to shift the current standing debate in such cases

2014 U.S. Dist. LEXIS 124126, at *34 (N.D. Cal. Sept. 4, 2014) (holding that plaintiffs had not alleged independent injury to support a claim for violation of the California Customer Records Act, Cal. Civ. Code § 1798.2, which requires prompt notification about data breaches).

away from the risk of future harm and toward allegations of presently suffered injury.