CYBERLAW — DATA BREACH LITIGATION — D.C. CIRCUIT HOLDS THAT HEIGHTENED RISK OF FUTURE INJURY CAN CONSTITUTE AN INJURY IN FACT FOR ARTICLE III STANDING. — *In re U.S. Office of Personnel Management Data Security Breach Litigation*, 928 F.3d 42 (D.C. Cir. 2019).

In an overwhelmingly digital age, individuals are put at risk of serious injuries such as identity theft, fraud, and even personal embarrassment if their data is exposed to malicious third parties.[1] Victims of such data breaches have often turned to litigation to seek remedy against companies that allegedly failed to secure consumers' private data.[2] Courts seeking to provide legal recourse to these plaintiffs have grappled with the difficulty of applying established legal doctrines, such as standing to bring suit, to novel fact patterns created by new technologies.[3] For example, the circuit courts have split over one such legal issue: whether plaintiffs who have yet to actually suffer theft or fraud as a result of a data breach have standing to sue at all.[4] Recently, in *In re U.S. Office of Personnel Management Data Security Breach Litigation*[5] (*In re OPM*), the D.C. Circuit weighed in on the debate by allowing the plaintiffs to proceed on the theory that they had suffered an injury of exposure to increased risk of future harm.[6] *In re OPM* is the most recent case in a pattern of lower courts struggling to reconcile Supreme Court guidance with a theory of future injury, and it emphasizes the need for novel legal theories better suited to data breach litigation.

The U.S. Office of Personnel Management (OPM) maintains a large volume of sensitive private information about federal

---

[1] *See, e.g.*, Stacy Cowley, *Equifax to Pay at Least $650 Million in Largest-Ever Data Breach Settlement*, N.Y. TIMES (July 22, 2019), https://nyti.ms/2YgXFqJ [https://perma.cc/2GP4-BEC7] (describing historic monetary settlement following loss of millions of individuals' sensitive personal information by Equifax, a large credit bureau); Robert Hackett, *What to Know About the Ashley Madison Hack*, FORTUNE (Aug. 26, 2015), https://fortune.com/2015/08/26/ashley-madison-hack [https://perma.cc/8MUK-DGQG] (noting that data breach revealed embarrassing personal information about customers seeking extramarital affairs).

[2] *See* Megan Dowty, Note, *Life Is Short. Go to Court: Establishing Article III Standing in Data Breach Cases*, 90 S. CAL. L. REV. 683, 686 (2017). There are multiple avenues for the law to effect change in this arena, including regulatory enforcement and breach notification requirements, but these methods can prove unreliable and inadequate to empower affected individuals. *See* Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 781 (2018).

[3] *See* Dowty, *supra* note 2, at 686–87.

[4] *See* Ethan Kisch & Alejandro H. Cruz, *D.C. Circuit Breathes New Life into OPM Data Breach Litigation*, PATTERSON BELKNAP: DATA SECURITY LAW BLOG (July 15, 2019), https://www.pbwt.com/data-security-law-blog/d-c-circuit-breathes-new-life-into-opm-data-breach-litigation [https://perma.cc/D3X9-6NWT].

[5] 928 F.3d 42 (D.C. Cir. 2019).

[6] *See id.* at 49, 67, 75; *see also* Kisch & Cruz, *supra* note 4.

government employees.[7] OPM employs a private firm, KeyPoint Government Solutions, Inc. (KeyPoint), to help with internal investigations, which necessitates granting KeyPoint access to the OPM database.[8] As early as 2007, OPM's Inspector General had warned the agency about "major information security deficiencies" in its network, but OPM did not address these concerns.[9] Between November 2013 and November 2014, unidentified cyberattackers stole the sensitive data of over twenty-one million people from OPM's network using stolen KeyPoint credentials.[10] The impacted individuals brought suit against both OPM and KeyPoint for negligence and violation of federal statutes, including the Privacy Act of 1974.[11] A few of these plaintiffs alleged that they had already experienced fraud and identity theft since the data breach.[12] The suits were transferred to the U.S. District Court for the District of Columbia for pretrial proceedings.[13]

In the district court, OPM and KeyPoint moved to dismiss the complaints.[14] The court granted their motions on two grounds. First, the plaintiffs failed to meet two out of three of the requirements for standing to litigate[15]: an injury in fact and causation linked to the defendants' misconduct.[16] Relying on *Spokeo, Inc. v. Robins*,[17] the district court rejected both of the plaintiffs' theories of injury — the loss of data itself and the heightened risk of future injury.[18] In addition, even those plaintiffs who had suffered actual injury failed to allege a substantial causal connection between OPM's negligence and any fraudulent activity.[19]

---

[7] *In re OPM*, 928 F.3d at 49–50. This information is collected for electronic personnel files, as well as "background checks and security clearance investigations." *Id.* at 50.

[8] *Id.* at 50.

[9] *Id.* at 51.

[10] *See id.* at 49–50.

[11] 5 U.S.C. § 552a (2018) (mandating that, absent certain exceptions not applicable here, "[n]o agency shall disclose any record which is contained in a system of records by any means of communication . . . except . . . with the prior written consent of[] the individual to whom the record pertains," *id.* at § 552a(b)).

[12] *See In re* U.S. Office of Pers. Mgmt. Data Sec. Breach Litig. (*OPM District Court*), 266 F. Supp. 3d 1, 8, 14 (D.D.C. 2017).

[13] *Id.* at 14.

[14] *See In re OPM*, 928 F.3d at 53.

[15] *See OPM District Court*, 266 F. Supp. 3d at 18–19, 38 & n.26. Article III standing is a prerequisite for justiciability in federal court. *See* Patrick J. Lorio, *Access Denied: Data Breach Litigation, Article III Standing, and a Proposed Statutory Solution*, 51 COLUM. J.L. & SOC. PROBS. 79, 82–83 (2017). Most data breach actions, particularly the large class actions, occur in federal court due to the broad jurisdiction granted to federal courts by the Class Action Fairness Act of 2005, Pub. L. No. 109-2, 119 Stat. 4 (2005) (codified in scattered sections of 28 U.S.C.). *See* Lorio, *supra*, at 82 n.16.

[16] *See In re OPM*, 928 F.3d at 54, 61. The court did not address the third standing requirement, redressability by a favorable court decision. *Id.*

[17] 136 S. Ct. 1540 (2016).

[18] *See OPM District Court*, 266 F. Supp. 3d at 20–26, 29.

[19] *See id.* at 36–38.

Furthermore, the plaintiffs' claims either were barred by sovereign immunity or failed to state a claim.[20]

The D.C. Circuit affirmed in part and reversed in part.[21] The panel's per curiam opinion found that the plaintiffs *had* alleged facts sufficient to meet the "low bar to establish . . . standing at the pleading stage."[22] The D.C. Circuit first analyzed the plaintiffs' theory of an injury in fact, which must be both "concrete and particularized[,] and actual or imminent."[23] According to the plaintiffs, the data breach had injured them by exposing them to increased risk of future harms such as identity theft.[24] To determine whether this injury was more than "merely conjectural,"[25] and therefore actual or imminent, the court considered whether the plaintiffs had plausibly alleged that the OPM hackers had "both the intent and the ability to use [the plaintiffs'] data for ill."[26] Here, the plaintiffs had alleged that some of them had "already experienced various types of identity theft," all of which could have been accomplished with the stolen information.[27] The nature of these previous attacks indicated both that the hackers were "sophisticated and apparently quite patient" and that the plaintiffs still faced "a substantial risk of future identity theft" arising from the breach.[28] Thus, the plaintiffs had successfully alleged an injury in fact.

According to the court, the plaintiffs' claims also satisfied the remaining standing requirements: causation and redressability.[29] The "relatively modest"[30] standard for proving causation at the pleading stage required only that the plaintiffs show the defendants' behavior was "fairly traceable" to the injury.[31] The plaintiffs had met this burden by alleging that OPM's and KeyPoint's data security practices were substantial contributing factors to the breach and that the information stolen was sufficient to enable identity theft.[32] Finally, money damages

---

[20] *See id.* at 38–39. OPM's sovereign immunity was not waived by the Privacy Act because the plaintiffs failed to plausibly allege "actual damages" under the statute. *Id.* at 40. The court also ruled the plaintiffs had failed to prove the existence of a constitutional right to informational privacy. *Id.* at 47.

[21] Judges Patel and Millett and Senior Judge Williams comprised the panel. The decision was issued per curiam, although Senior Judge Williams wrote a separate opinion concurring in part and dissenting in part.

[22] *In re OPM*, 928 F.3d at 61 (quoting Attias v. CareFirst, Inc., 865 F.3d 620, 622 (D.C. Cir. 2017)).

[23] *Id.* at 54 (quoting Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016)).

[24] *See id.* at 58–59.

[25] *Id.* at 58.

[26] *Id.* at 56 (quoting *Attias*, 865 F.3d at 628).

[27] *Id.*

[28] *Id.* at 59.

[29] *See id.* at 61.

[30] *Id.* (quoting Bennett v. Spear, 520 U.S. 154, 171 (1997)).

[31] *Id.* at 60.

[32] *See id.*

for expenses spent on protective services provided a clear way to redress the plaintiffs if they were to obtain a favorable decision.[33]

The court of appeals also held that sovereign immunity did not bar the court from taking jurisdiction.[34] By "plausibly alleg[ing]" the three elements of a Privacy Act claim, the plaintiffs had "unlock[ed]" the statute's waiver of sovereign immunity over OPM.[35] KeyPoint, OPM's private contractor, was also not immune because it could not acquire derivative sovereign immunity from an entity (OPM) that was itself not immune, and KeyPoint had failed to demonstrate that its problematic security practices were "authorized and directed by" a government agency.[36]

The opinion concluded by dismissing the plaintiffs' constitutional claims.[37] Although the court did not rule directly that a constitutional right to information privacy does not exist, it reasoned that, even assuming the existence of this right, only intentional disclosures — and not accidental breaches — would violate the right.[38] The court also rejected the plaintiffs' due process claim by denying any affirmative duty for the government to safeguard data where the affected parties (employees) voluntarily disclosed personal information.[39]

Judge Williams dissented from the majority's finding on standing and concurred with the remaining rulings.[40] On standing, Judge Williams found the plaintiffs had not met the *Twombly* and *Iqbal* standard for pleadings, which requires plaintiffs to allege facts that could negate "obvious alternative explanation[s]."[41] Judge Williams emphasized the fact that "a *government* system" was hacked to steal information about "*government* employees," so the "obvious" alternate explanation for the hack — espionage — nullified any likelihood of future identity

---

[33] *See id.* at 61.

[34] *See id.* at 61–62.

[35] *Id.* OPM had allegedly willfully violated the Privacy Act by ignoring repeated warnings about its security systems, *id.* at 62–64; the plaintiffs had collectively alleged actual damages, including the cost of credit protection, *id.* at 65–66; and proximate causation was satisfied by the identity theft that some of the plaintiffs had already experienced, *id.* at 67.

[36] *Id.* at 69 (quoting Campbell-Ewald Co. v. Gomez, 136 S. Ct. 663, 673 (2016)); *see id.* at 69–71.

[37] *Id.* at 74–75. The court did note, however, that the plaintiffs who claimed a constitutional injury would have had standing if a constitutional right did exist. *See id.* at 55.

[38] *See id.* at 74. More specifically, the court was extremely hesitant to establish such a constitutional right due to the government's role in this case as an "employer" rather than a "sovereign" and the existence of a pre-existing legislative means of regulating information privacy (the Privacy Act). *Id.* at 73.

[39] *See id.* at 75.

[40] *Id.* at 75–76, 81 (Williams, J., concurring in part and dissenting in part). Judge Williams also wrote on two topics the majority did not address: a potential federal-state preemption issue in the question of KeyPoint's immunity, *see id.* at 80–81, and the district court's willingness to allow five plaintiffs to proceed anonymously, *see id.* at 81–84.

[41] *Id.* at 76 (quoting Ashcroft v. Iqbal, 556 U.S. 662, 682 (2009)).

theft caused by the breach.[42] He also suggested that the allegations were made even less plausible by the passage of two years since the original attacks without widespread identity theft among the plaintiffs.[43] According to Judge Williams, only those plaintiffs who actually suffered theft prior to the litigation could have standing.[44]

In *In re OPM*, the D.C. Circuit validated the plaintiffs' legal theory that exposure to an increased risk of future harm constitutes the "injury" necessary to confer standing on data breach victims. But the court's recognition of this injury stretched existing Supreme Court standing doctrine. Two important Supreme Court cases fleshed out the two injury-in-fact requirements that plaintiffs must meet to bring suit: *Clapper v. Amnesty International USA*[45] on imminence, and *Spokeo* on concreteness. The *In re OPM* opinion improperly applied this guidance when analyzing both requirements, however, revealing the incompatibility of the Court's injury-in-fact precedent with a "future injury" theory in the data breach context. This analytical difficulty has stymied other lower courts as well, and the ensuing incoherence of standing doctrine in the data breach context illustrates the need for novel, more fitting legal theories.

By relying on speculation about the hackers' future actions to find imminent injury, the D.C. Circuit did not faithfully apply *Clapper*'s imminence test. In *Clapper*, the Supreme Court held that a "substantial risk" of injury could render it imminent,[46] but severely cabined this theory by disfavoring speculation about a "chain of possibilities" that rested on "the decisions of independent actors."[47] The *Clapper* plaintiffs had claimed that a statute authorizing government surveillance of certain foreigners created a risk of future injury, namely that the government might overhear the plaintiffs' sensitive communications with those foreigners.[48] The *Clapper* Court dismissed this claim, refusing to assess the likelihood that the government would make particular choices — the choice to surveil a specific individual, for example — in future, hypothetical surveillance decisions.[49] In *In re OPM*, however, the court *did* speculate about the decisionmaking of independent, third-party actors — the cyberattackers.[50] More specifically, to evaluate imminence, the majority made multiple inferences about what was likely to be true

---

[42] *Id.* at 77.
[43] *See id.* at 79.
[44] *See id.*
[45] 568 U.S. 398 (2013).
[46] *Id.* at 414 n.5 (quoting Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 153 (2010)); *see id.* ("Our cases do not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about.").
[47] *Id.* at 414.
[48] *See id.* at 401.
[49] *See id.* at 411–14.
[50] *See In re OPM*, 928 F.3d at 57–58.

about the hackers: they did not conduct the attack for espionage purposes, and they had both the ability and intent to use the stolen data for future identity theft and fraud.[51] This chain of speculative inferences about independent actors resembled the *Clapper* dissent's musings on the history of government surveillance[52] far more closely than it did the *Clapper* majority's desire to *reduce* judicial guessing.[53] The D.C. Circuit's imminence analysis thus did not comply with the Supreme Court's holding in *Clapper*.

The D.C. Circuit also did not adequately evaluate whether the plaintiffs' theory of injury — *risk* of future injury — was concrete under the Supreme Court's *Spokeo* analysis. Instead, the court relied on its own precedent that identity theft itself is a concrete injury. In *Spokeo*, the Supreme Court acknowledged that "risk of real harm" *could* satisfy the concreteness requirement if the alleged injury (1) paralleled injuries rooted in the common law, or (2) violated a right expressly protected by statute.[54] In explicitly delineating how risk of harm might satisfy its test,[55] *Spokeo* implied that the concreteness of the *risk* should be analyzed when risk stands in for the actual injury. Although this analysis extends to all cases that involve injury in fact, the *In re OPM* opinion referenced *Spokeo* in just one paragraph, and only cursorily to quote blanket statements about the three basic elements of Article III standing.[56] The resolution of the concreteness requirement consisted of a conclusory citation to the D.C. Circuit's previous ruling in *Attias v. CareFirst, Inc.*,[57] where it established that "identity theft . . . constitute[s] a concrete . . . injury,"[58] but the court did not engage further with *Spokeo*'s concreteness requirement. This analytical move elided the actual question that *Spokeo* suggested should be answered here: whether the plaintiff's theory of injury — substituting *risk* of future injury for

---

[51] *See id.* Indeed, the primary point of contention between the majority and Judge Williams on the issue of standing was about whether the hackers intended to conduct espionage or financial thievery. *Compare id.* at 57, *with id.* at 77–78 (Williams, J., concurring in part and dissenting in part).

[52] *See Clapper*, 568 U.S. at 427–31 (Breyer, J., dissenting) (claiming that the Court "need only assume that the Government is doing its job . . . in order to conclude," *id.* at 431, that "the Government will intercept at least some of the plaintiffs' communications," *id.* at 430).

[53] *See id.* at 414 (majority opinion).

[54] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016) (noting that "it is instructive to consider whether an alleged tangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts" and that "Congress is well positioned to identify intangible harms that meet minimum Article III requirements").

[55] *See id.* ("This does not mean, however, that the risk of real harm cannot satisfy the requirement of concreteness.").

[56] *See In re OPM*, 928 F.3d at 54 (citing *Spokeo* for the proposition that Article III standing has three elements, including an injury in fact and causation). This passing reference is especially notable because the district court extensively analyzed *Spokeo*, but the court of appeals did not respond directly to this reasoning in overruling the district court. *See OPM District Court*, 266 F. Supp. 3d 1, 21–26 (D.D.C. 2017).

[57] 865 F.3d 620 (D.C. Cir. 2017).

[58] *In re OPM*, 928 F.3d at 55 (first and second alterations in original) (quoting *Attias*, 865 F.3d at 627).

actual injury (identity theft) — was sufficiently concrete. The court thus sidestepped the more contentious question of whether the risk of future injury alleged by these plaintiffs was sufficiently concrete.

These inconsistencies between the reasoning of the D.C. Circuit and that of the Supreme Court demonstrate the difficulty of wrestling the square peg of risk of future injury into the round hole of injury-in-fact analysis. As previously acknowledged, both *Clapper* and *Spokeo* did suggest that "substantial risk" *could* theoretically meet the requirements for injury in fact. However, the imminence and concreteness tests actually articulated by the Supreme Court have created a tricky conundrum for lower courts. Analyzing a theory of future injury forces courts to speculate about the future: after all, any activity, no matter how innocuous, will always create *some* risk of future injury, so courts must have some way to evaluate how imminent a risk actually is. This challenge is especially acute in the context of a data breach where no plaintiffs have yet suffered actual injury, as the motives and future actions of independent actors are always difficult to know with certainty. *Clapper* thus seems to actually prohibit a "substantial risk" from constituting an injury in fact in data breach cases, because assessing the gravity of the risk necessarily involves conjecture about the actions of third-party hackers. Similarly, to engage properly with *Spokeo*, lower courts would have to answer an oddly abstract question: What does it mean for *risk* of future injury to be "concrete"? Although both the common law[59] and statutes[60] have protected against the loss of privacy itself, it is less clear that either has expressly classified the exposure of individuals to the possibility of identity theft as a concrete injury. Supreme Court precedent thus placed the *In re OPM* court in the unenviable position of attempting to vindicate plaintiffs' claims by reference to a restrictive injury-in-fact doctrine.

This doctrinal difficulty has helped fuel the circuit split[61] — and general lack of coherence among federal courts — over what data breach plaintiffs are required to prove to have standing to bring suit. The D.C. Circuit's *In re OPM* opinion thus continued the pattern of lower court confusion over how *Clapper* and *Spokeo* apply to data breaches. In the absence of clear guidance on how much speculation is really allowed in the imminence analysis, lower courts have interpreted *Clapper* with varying

---

[59] Scholars, including the reporters of the Restatement of Torts, have argued that the history of privacy torts evinces an independent right to privacy rooted in common law. *See, e.g.*, Jordan Elias, *Course Correction — Data Breach as Invasion of Privacy*, 69 BAYLOR L. REV. 574, 587–89 (2017).

[60] Congress has recognized the right to privacy of data given to government agencies by forbidding, through the Privacy Act, agency disclosure of this information without consent. *See* 5 U.S.C. § 552a (2012).

[61] The Sixth, Seventh, and Ninth Circuits favor a future-harm theory of injury, whereas the First, Third, and Fourth Circuits have been more hesitant to allow plaintiffs to proceed on this theory. *See* Beck v. McDonald, 848 F.3d 262, 273 (4th Cir. 2017) (collecting cases).

degrees of strictness.[62] Some, like the D.C. Circuit in *In re OPM*, have used inferences about the intentions and abilities of the hackers as proxies for imminence,[63] whereas others have rejected the future injury theory entirely because "future injuries stem from conjectural conduct of a third party . . . and are therefore inadequate to confer standing."[64] Similarly, many lower courts have struggled with *Spokeo*. Like the D.C. Circuit, most have essentially ignored the *Spokeo* test in data breach litigation, instead focusing only on imminence and engaging in a cursory concreteness analysis.[65] The *In re OPM* opinion — while ultimately plaintiff-friendly — did not help clarify how lower courts should evaluate whether data breach plaintiffs have standing in the future.

The inconsistency of the D.C. Circuit's *In re OPM* analysis with Supreme Court guidance reflects the difficulty of adapting older legal standards to the newer data breach context, especially where plaintiffs allege injury in the form of risk of future harm, a theory that inherently clashes with Supreme Court guidance on standing. Scholars have proposed at least one other theory for injury that might better meet the Court's standards and thereby alleviate the difficulties faced by lower courts: framing the loss of privacy itself at the moment of the data breach as an injury.[66] Although this theory may not be the best or only one that could remedy the analytical deficiencies displayed in *In re OPM*, it is increasingly important to think more critically about the theories courts adopt to evaluate individuals' rights and data collectors' obligations in data privacy.

---

[62] *See* Kassi Burns, *Data Breach Lawsuit Highlights: Standing & the Fading Impact of* Clapper, DRIVEN (Sept. 1, 2015), http://www.driven-inc.com/data-breach-lawsuit-highlights-standing-the-fading-impact-of-clapper [https://perma.cc/D2FK-U3FE].

[63] *See, e.g.*, Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015) ("Why else would hackers break into a store's database and steal consumers' private information?").

[64] *In re* Horizon Healthcare Servs. Inc. Data Breach Litig., No. 13-7418, 2015 WL 1472483, at *6 (D.N.J. Mar. 31, 2015); *see also In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 25 (D.D.C. 2014) (refusing to find imminence where "speculative" chain of future events would have to happen before plaintiffs experienced harm).

[65] *See* Lorio, *supra* note 15, at 91–103 (finding few meaningful concreteness inquiries, as required by *Spokeo*, in the circuit courts).

[66] *See, e.g.*, Elias, *supra* note 59, at 581–86 (framing immediate harms caused to data breach victims at moment of breach as an injury in fact). This theory has proved viable in lower courts already. In *Rowe v. Unicare Life & Health Insurance Co.*, No. 09 C 2286, 2010 WL 86391 (N.D. Ill. Jan. 5, 2010), for example, a federal district court found that invasion of privacy due to the data breach itself could be considered an injury and confer standing to sue. *Id.* at *9. The *In re OPM* plaintiffs did raise this legal theory in the district court, but the lower court disclaimed any ability to reach beyond Supreme Court and D.C. Circuit precedent to adopt this novel theory, and the issue was not brought up on appeal. *See OPM District Court*, 266 F. Supp. 3d 1, 19–20 (D.D.C. 2017).