Bloomberg BNA

Privacy and Security Law Report®

Supreme Court's *Clapper* Decision Raises Bar For Standing in Data Security Breach Litigation



By Douglas H. Meal, David T. Cohen, and Daniel M. Routh

On Feb. 26, the U.S. Supreme Court in *Clapper v. Amnesty International USA* adopted a demanding standard for Article III standing in privacy cases.[1] Although the case addressed issues of constitutional privacy, the decision also will likely assist companies that have suffered data security breaches to obtain dismissal of ensuing lawsuits by consumers who claim that their data were compromised in the breach. The court held that, in order to satisfy Article III's standing requirement based on a threat of future harm, a plaintiff must show that the threatened injury is ''certainly impending.'' This holding has broad implications for data security breach litigation, where consumers often cannot plead, much less show, that any exposure of their data in the breach will certainly result in criminals committing identity theft or otherwise causing them actual injury, as *Clapper* now requires.

Article III Standing in Data Security Breach Litigation Prior to *Clapper*

A plaintiff seeking to invoke the jurisdiction of the federal courts must satisfy the standing requirements of Article III of the U.S. Constitution, which require that a plaintiff allege an ''injury in fact.'' Specifically, as explained in prior Supreme Court decisions such as *Lujan v. Defenders of Wildlife*, a plaintiff must show an injury that is ''(a) concrete and particularized'' and ''(b) actual or imminent, not conjectural or hypothetical.''[2] Constitutional standing also requires a causal connection between the injury alleged and the conduct complained of.[3]

Prior to *Clapper*, when plaintiffs attempted to meet the *Lujan* standard by pointing to a threat of future harm, the Supreme Court used varying phrases to describe the level of risk the plaintiff had to show. At times, the court stated that the threatened harm must be ''certainly impending.''[4] On other occasions (and sometimes in the same opinion) the court indicated that the plaintiff must face a ''realistic danger,''[5] ''reasonable probability,''[6] or ''substantial risk'' of harm.[7]

Perhaps in part because of this varying language, lower courts have inconsistently applied the *Lujan* standard in data security breach litigation. Some courts held that the standard was satisfied in cases where consumers claimed that a data security breach exposed them to an increased risk of future identity theft. In *Pisciotta v. Old National Bancorp*, for instance, a hacker was able to infiltrate a bank's website and thereby obtain access to the confidential information of tens of thousands of its customers, but the customers did not allege that they

[1] *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013), *available at* http://www.bloomberglaw.com/public/document/Clapper_v_Amnesty_Intl_USA_No_111025_2013_BL_50248_2013_ILRC_1311 (12 PVLR 350, 3/4/13).

[2] *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992).

[3] *Id.*

[4] *See, e.g.*, *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990); *Babbitt v. United Farm Workers Nat'l Union*, 442 U.S. 289, 298 (1979).

[5] *Babbitt*, 442 U.S. at 298.

[6] *Monsanto Co. v. Geertson Seed Farms*, 130 S. Ct. 2743, 2754 (2010).

[7] *Id.* at 2754–55.

 ISSN 1538-3423

had suffered identity theft or other financial harm as a result of the breach.[8] Instead, they claimed that the intrusion exposed them to an increased risk that such injury would eventually occur.[9] Despite their failure to allege actual misuse, the U.S. Court of Appeals for the Seventh Circuit concluded that the mere exposure of their information caused an ''injury in fact'' sufficient to confer Article III standing.[10] The court reasoned, without elaboration, 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.''[11]

Other courts, by contrast, have required plaintiffs to go further and allege that criminals actually used the data to commit identity theft or make fraudulent charges to their financial accounts. In *Reilly v. Ceridian Corporation*, for example, a hacker infiltrated a payroll processor's computer system and potentially gained access to the personal and financial information of thousands of employees of the processor's business customers. But the employees could only speculate as to whether the hacker actually copied their data or had the ability and intention to use it to commit fraud, and none claimed that the hacker had actually perpetuated any such fraud.[12] The U.S. Court of Appeals for the Third Circuit held that the employees' ''allegations of an increased risk of identity theft resulting from a security breach'' were ''insufficient to secure standing'' under Article III, and that allegations of actual misuse were required.[13] The court relied upon the ''certainly impending'' language found in several of the Supreme Court's opinions[14] and held that the plaintiffs failed to satisfy this standard because ''[a]ny damages that may occur'' from identity theft or other fraud were not ''certainly impending,'' but were ''entirely speculative and dependent on the skill and intent of the hacker.''[15] There had ''been no misuse of the information, and thus, no harm.''[16]

The *Clapper* Decision

The likely resolution to this conflict in *Clapper* began when several attorneys and human rights, labor, legal, and media organizations sued to challenge a 2008 amendment to the Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. § 1881a. Section 1881a allows the federal government to conduct surveillance on the electronic communications of non-U.S. persons reasonably believed to be located outside the United States, but the government may do so only after obtaining approval from a Foreign Intelligence Surveillance Court (FISC).[17] The plaintiffs sued to obtain a declaration that the law is unconstitutional and an injunction against the surveillance, claiming that their work required them to engage in sensitive international communications with individuals who they believed were likely targets of surveillance. The district court dismissed the case on the ground that the plaintiffs had failed to show ''injury in fact'' sufficient to confer Article III standing,[18] but the U.S. Court of Appeals for the Second Circuit reversed, holding that the plaintiffs' claimed injuries were sufficiently concrete and imminent.[19]

In the Supreme Court, the plaintiffs presented two theories to buttress their argument that they had suffered sufficient injury to assert their claims. First, they argued that there was an objectively reasonable likelihood that their communications would be monitored under § 1881a at some point in the future, thus causing them injury. Second, they claimed that as a result of § 1881a, they suffered present injury in the form of costly and burdensome measures they were forced to take to protect the confidentiality of their international communications (such as travel to hold meetings in person).

In a 5-4 decision by Justice Samuel A. Alito Jr., the court rejected both of these theories and held that the plaintiffs lacked standing. Removing much of the ambiguity that had been created by the court's prior articulations of the *Lujan* standard, the court held that to be sufficiently concrete and imminent for purposes of Article III, a threatened injury must be ''certainly impending.''[20] The plaintiffs' first theory did not meet this standard because it relied on a ''speculative chain of possibilities.''[21] Specifically, the claimed injury would occur only *if* the government actually decided to target plaintiffs' non-U.S. contacts, did so under § 1881a, obtained approval from the FISC, succeeded in intercepting the communications, *and* the plaintiffs were parties to those particular communications. Importantly, the court emphasized that the FISC was an independent third party whose actions could not be predicted, and refused to ''endorse standing theories that rest on speculation about the decisions of independent actors.''[22]

The plaintiffs' second theory fared no better. The court viewed the plaintiffs' reliance on steps they took to avoid monitoring as an impermissible attempt to ''manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.''[23] Were the court to accept that theory, Justice Alito noted, ''an enterprising plaintiff would be able to secure a lower standard for Article III standing simply by making an expenditure based on a nonparanoid fear.''[24]

Dissenting from the court's opinion, Justice Stephen G. Breyer criticized the court's application of the ''certainly impending'' standard. ''[W]hat the Constitution requires,'' Justice Breyer contended, ''is something more akin to 'reasonable probability' or 'high probabil-

[8] *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 631–32 (7th Cir. 2007) (6 PVLR 1374, 9/3/07).
[9] *Id.* at 632.
[10] *Id.* at 634.
[11] *Id.*
[12] *Reilly v. Ceridian Corp.*, 664 F.3d 38, 43 (3d Cir. 2011) (10 PVLR 1859, 12/19/11).
[13] *Id.*
[14] *Id.* at 42 (citing *Whitmore*, 495 U.S. at 158).
[15] *Id.* at 45.
[16] *Id.* at 42.
[17] 50 U.S.C. § 1881a.
[18] *Amnesty Int'l USA v. McConnell*, 646 F. Supp. 2d 633, 658 (S.D.N.Y. 2009).
[19] *Amnesty Int'l USA v. Clapper*, 638 F.3d 118, 150 (2d Cir. 2011) (10 PVLR 486, 3/28/11).
[20] *Clapper*, 133 S. Ct. at 1147.
[21] *Id.* at 1150.
[22] *Id.* at 1148–50.
[23] *Id.* at 1151.
[24] *Id.*

  PVLR ISSN 1538-3423

ity' '' of harm.[25] Such a test, Justice Breyer contended, was ''readily met in this case.''[26]

Implications of *Clapper* for Data Security Breach Litigation

Clapper has important implications for data security and privacy litigation, particularly suits over data security breaches. By applying a ''certainly impending'' standard to deny standing on the facts before it, *Clapper* likely resolves the conflict that had developed among federal courts as to the application of standing principles where data security breach plaintiffs rely merely upon a risk of future injury from the breach or steps they took to mitigate that risk. In short, such data security breach plaintiffs rely upon the very ''speculative chain of possibilities'' that *Clapper* held insufficient to constitute ''injury in fact.'' Their claims to Article III standing are unlikely to succeed in future litigation.

Specifically, if the possibility of government surveillance was too speculative to support standing in *Clapper*, companies will have a strong argument that the possibility that a criminal *may* use exposed information to commit fraud is likewise speculative—in other words, the misuse is not ''certainly impending.'' Data security breach plaintiffs often do not specifically allege (much less show) that an intruder has even obtained their consumer data.

More importantly, however, even *if* such plaintiffs sufficiently plead and prove that the hacker has stolen *their* data, any allegation of misuse of that data to commit fraud would impermissibly rely on speculation as to the ability or intentions of third parties. Critically, just as the possible approval of surveillance by the third-party FISC in *Clapper* was too unpredictable to allow standing, breached companies can argue that the actions of a third-party hacker or other criminal are likewise unpredictable. A hacker may not have the ability to commit fraud using stolen information, whether because of the type of information, the form in which it was found, or other circumstances. And even if he has the ability, he may not have the intent to commit fraud, for any number of reasons. In fact, hackers' avowed purpose often is *not* to commit identity theft or harm consumers, but rather to embarrass or harm the hacked corporation, steal trade secrets, or make a political statement. To use the words of Justice Alito in *Clapper*, plaintiffs ''cannot rely on speculation about 'the unfettered choices made by independent actors not before the court.' ''[27] Indeed, it would be hard to find an actor more ''independent'' from the control of defendants and plaintiffs in litigation than a third-party hacker.

Moreover, just as the *Clapper* plaintiffs could not rely on steps they took to avoid surveillance, breached companies can argue that consumers should not be permitted to manufacture standing by incurring costs to monitor their credit or otherwise mitigate an as-yet unrealized risk of fraud stemming from a data security breach. As *Clapper* held, allowing plaintiffs to bring an ''action based on costs they incurred in response to a speculative threat'' would ''improperly water[ ] down the fundamental requirements of Article III.''[28]

In short, *Clapper* demonstrates that *Reilly* and similar cases were right, while decisions like *Pisciotta* were wrong. As the *Reilly* line of cases held, the *Lujan* injury-in-fact standard is too demanding to permit standing in cases where data security breach plaintiffs rely merely upon a risk of future identity theft or other harm. Going forward, then, lower federal courts should follow *Reilly*'s analysis to deny standing in such cases. Those that instead follow *Pisciotta* will face a significant risk of reversal or petitions for certiorari to the Supreme Court—and, though we of course hesitate to speculate ''as to how independent decisionmakers will exercise their judgment,''[29] we suspect the Supreme Court may welcome the opportunity to adopt *Reilly* as the law of the land.

Douglas H. Meal is a partner and David T. Cohen and Daniel M. Routh are associates at Ropes & Gray LLP. Meal has played a leading role in the firm's privacy and data security practice, specializing in representing clients targeted by litigation and government investigations stemming from highly publicized data security breaches. Cohen, whose practice focuses on complex business and commercial disputes, has extensive experience working with corporate clients that have suffered data breaches or have been accused of privacy violations. Routh, who works within the firm's litigation department, has significant experience representing large companies in consumer class actions relating to data security breaches. Meal and Routh practice in the firm's Boston office; Cohen practices in its Washington office.

[25] *Id.* at 1165 (Breyer, J., dissenting).
[26] *Id.*
[27] *Id.* at 1150 n.5.
[28] *Id.* at 1151.
[29] *Id.* at 1150.