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

On February 26, 2013, the United States Supreme Court in *Clapper v. Amnesty International* adopted a demanding standard for Article III standing in privacy cases. Although the case addressed issues of Constitutional privacy, the decision also will likely assist companies that have suffered data security breaches in obtaining dismissal of ensuing lawsuits by consumers claiming that their data was 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 has resulted or will imminently result in criminals committing identity theft or otherwise causing them financial injury.

A plaintiff seeking to invoke the jurisdiction of the federal courts must satisfy the standing requirements of Article III of the 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 "invasion of a legally protected interest which is (a) concrete and particularized" and "(b) actual or imminent, not conjectural or hypothetical." Constitutional standing also requires a causal connection between the injury alleged and the conduct complained of.

To date, courts have inconsistently applied this 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. Other courts 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. Courts also have disagreed as to whether steps consumers take to preemptively "mitigate" potential harm from a data security breach, such as by enrolling in credit monitoring services, constitute a sufficiently concrete injury to confer standing.

The likely resolution to these conflicts 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 located outside the United States, but the government may only do so after obtaining approval from a Foreign Intelligence Surveillance Court ("FISC"). 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 whom they believed were likely targets of surveillance. The district court dismissed the case on the ground that plaintiffs had failed to show "injury in fact" sufficient to confer Article III standing, but the Second Circuit reversed, holding that the plaintiffs' claimed injuries were sufficiently concrete and imminent.

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 Alito, the Court rejected both of these theories and held that the plaintiffs lacked standing. The Court held that to be sufficiently concrete and imminent for purposes of Article III, a

threatened injury must be "certainly impending," as opposed to merely "possible." The plaintiffs' first theory did not meet this standard because it relied on a "speculative chain of possibilities." Specifically, the claimed injury would only occur *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* 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."

Plaintiffs' second theory fared no better. The Court viewed 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." 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."

Clapper has important implications for data security and privacy litigation, particularly suits over data security breaches. The case 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. If the possibility of government surveillance was too speculative to support standing in *Clapper*, companies will have a strong argument that, likewise, the possibility that a criminal *may* use exposed information to commit fraud is likewise speculative – in other words, the misuse is not "certainly impending." 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 – he may not have the ability to commit fraud using the information, and even if he does, he may not decide to do so. 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 the breach.

For more information regarding the *Clapper* decision and its potential impact, please contact a member of our leading privacy and data security team, including Doug Meal, Mark Szpak, Jim DeGraw, and David McIntosh.