VENABLE® LLP

Class Action Alert

March 2013

The Impact Of The Supreme Court's Recent Decision In *Clapper v. Amnesty International USA* On Privacy and Data-Security Litigation

AUTHORS

Edward P. Boyle
Emilio W. Cividanes
Thomas E. Gilbertsen
Stuart P. Ingis
David N. Cinotti
Joeann E. Walker

RELATED PRACTICES

Litigation
Class Action Defense
Privacy Class Action Defense

ARCHIVES

2013 2009 2005
2012 2008 2004
2011 2007 2003
2010 2006

On February 26, 2013, the Supreme Court decided *Clapper v. Amnesty International USA*, which clarified the standard to establish Article III standing for claims based on impending or future harm. The Supreme Court, in a 5-4 decision by Justice Samuel A. Alito, Jr., held that plaintiffs must demonstrate harm that is "certainly impending," not speculative, to satisfy the injury-in-fact requirement of standing. The Court also held that plaintiffs may not "manufacture" standing "by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."

The decision has important implications for suits in federal court relating to Internet privacy and data security. Plaintiffs in such cases often rely on fear of future harm—that the defendant's conduct has left them susceptible to identity theft or future privacy breaches, for example—or that they have incurred costs in order to avoid future harm. Federal courts will lack jurisdiction over such claims unless plaintiffs can show that the harm or injury that they allege is certainly impending, rather than merely possible.

Issue Before the Court

The plaintiffs in *Clapper* were a group of attorneys and nonprofit organizations who alleged that their work requires them to engage in sensitive and sometimes privileged telephone and e-mail communications with people outside the United States. They sought to challenge the constitutionality of Section 702 of the Foreign Intelligence Surveillance Act of 1978, codified at 50 U.S.C. § 1881a ("Section 1881a"). That statute allows the Attorney General and the Director of National Intelligence, with the approval of the Foreign Intelligence Surveillance Court, to authorize the surveillance of non-U.S. persons located outside the United States. The issue in the case was whether the plaintiffs had standing to bring their challenge.

To establish standing to sue in federal court, a plaintiff must plead and then prove an injury that is:

. concrete, particularized, and actual or imminent;
. fairly traceable to the defendant's action; and
. redressable by a favorable court ruling.

The plaintiffs maintained that they met this standard, and, in particular, the "injury-in-fact" requirement that the injury be concrete, particularized, and actual or imminent, because some of the people abroad with whom they communicate were likely targets of FISA surveillance, and because the plaintiffs ceased engaging in some communications and undertook costly measures to protect the confidentiality of their communications.

The U.S. Court of Appeals for the Second Circuit held that the plaintiffs had standing due to an objectively reasonable likelihood that their communications would be intercepted in the future. The Second Circuit also held that the plaintiffs had suffered present injuries by avoiding certain communications and incurring costs such as traveling to meet in person rather than communicating by e-mail or telephone with people overseas who might be subject to surveillance.

A majority of the Supreme Court disagreed. Instead of speculative or reasonably likely harm, the Court held that the plaintiffs needed to allege injury that was certainly impending, which they failed to do. The plaintiffs also could not rely on self-inflicted "present" harm when the harm they sought to avoid was only speculative or hypothetical.

"Certainly Impending" Standard

Although the Court did not conclusively define what "certainly impending" means in the context of imminent harm, it explained what was *insufficient* to satisfy the standard: injury that depends on the

occurrence of a series of possibilities, none of which is certain to occur.

The Court noted its prior precedents holding that threatened or future injury must be certainly impending, not speculative or merely possible. It was not enough to show that the plaintiffs were objectively reasonable in believing that their communications would be subject to surveillance. The plaintiffs' alleged harm would only have occurred if:

. the Government decided to target the communications of non-U.S. persons located abroad;
. the Government chose to invoke its authority under Section 1881a rather than some other authority to do so;
. the Foreign Intelligence Surveillance Court approved the surveillance;
. the Government was successful in intercepting communications; and
. the plaintiffs were parties to the particular communications intercepted.

The plaintiffs' claims therefore amounted to a "highly attenuated chain of possibilities," not certainly impending harm.

Self-Inflicted Harm Not Enough

The Supreme Court also rejected the plaintiffs' second theory that they had suffered "present" harm because they avoided certain communications and incurred costs like travel expenses due to fear of surveillance under Section 1881a. The Court held that plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." Costs that plaintiffs incur because of their fear alone cannot create standing.

Application to Privacy and Data-Security Litigation

Article III standing is a recurring issue in litigation relating to Internet privacy and data security. For example, in putative class actions alleging that defendants used cookies or applications to collect information, defendants have argued that plaintiffs lacked standing because they did not suffer an injury-in-fact.[1] Standing has also been an issue in cases alleging that the defendant created an increased risk of identity theft in the future.[2] Similarly, plaintiffs seeking injunctive relief are often vulnerable to Article III standing challenges when they are not current customers of the defendant and therefore unable to demonstrate sufficiently imminent risk of future harm.

The *Clapper* decision can be a useful tool to oppose plaintiffs' standing in privacy and data-security litigation. *Clapper* emphasizes that injury for purposes of Article III standing must be actual or imminent, not speculative. In addition, plaintiffs will not be able to rest on allegations that a defendant's conduct exposed their data or personal information to a risk of future collection or unauthorized use, without pleading facts to show that such an injury is certainly impending. Defendants should seek to present plaintiffs' claims as depending on a series of speculative or hypothetical possibilities that are not certain to occur. Finally, incurring costs such as installing software or taking other measures to prevent a security breach or reduce the effects of one should not be sufficient to establish standing if the threat of the data breach due to the defendant's conduct is merely possible or even probable.

If you have any questions regarding this case or this alert, please contact one of our authors or any member of **Venable's Class Action Defense Group**.

---

1 *See, e.g., In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1054- 55 (N.D. Cal. 2012); *LaCourt v. Specific Media Inc.*, No. SACV 10-1256-GW, 2011 WL 1661532, at *3-6 (C.D. Cal. Apr. 28, 2011).

2 *See, e.g., Reilly v. Ceridian Corp.*, 664 F.3d 38, 41-46 (3d Cir. 2011), *cert. denied*, 132 S. Ct. 2395 (holding that plaintiffs whose personal data might have been released as a result of a security breach lacked standing to sue defendant); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1142-43 (9th Cir. 2010) (holding that plaintiffs had standing to sue defendant based on the possibility that their personal data would be misused after a laptop containing that information was stolen from the defendant, their employer).