Bloomberg BNA

Privacy and Security Law Report®

Privacy Class Actions: Current Trends and New Frontiers in 2013



BY DAVID F. MCDOWELL, D. REED FREEMAN JR., AND JACOB M. HARPER

I. Introduction: Tracking Class Actions Today.

As behavioral advertising, mobile device applications, and websites advance, so do general concerns over privacy, as expressed in the press and by regulators, advocates, academics, and the plaintiff's bar. While users flock to Google Maps to check local traffic jams, and social media to see friends' activities and interests, these groups repeatedly express unease about the vague idea that Big Brother is somehow watching. Increasingly, this unease is expressed through class action matters.

The problem for plaintiffs thus far has been articulating a harm that is sufficient to confer standing in federal court. Such lawsuits-in-search-of-an-injury began over a decade ago with *In re DoubleClick Privacy Litig.*, the seminal privacy class action in which desktop computer users sued DoubleClick Inc., a trailblazer in technology-using browser ''cookies'' to create tailored online advertising, for breaching alleged privacy rights on the theory that the users did not know websites could ''see'' users' visited web pages or create advertisements tailored based on those website visits.[1] *DoubleClick* ended quietly with a settlement, followed by years of relative silence on the litigation front as tech companies built the internet into the ubiquitous (and generally free) wealth of information it is today. In the last few years, though, as a burgeoning array of technologies has emerged, privacy concerns are again expressed through class action lawsuits.

Indeed, over one hundred new tracking lawsuits have been filed, all falling into one of a handful of factual situations. The *desktop ''zombie cookie'' class actions* followed largely the same fact pattern as *DoubleClick*, though the ''cookies'' in these cases come in the form of allegedly difficult-to-delete Flash local shared objects (LSOs or Flash cookies), HTML5 coding, and other proprietary coding.[2] *Mobile device tracking class actions* make similar claims about smartphones and mobile apps.[3] Yet other suits accuse technology companies of

David F. McDowell, a partner at Morrison & Foerster LLP's Los Angeles office, is a member and former co-chair of the firm's Consumer Litigation and Class Action Practice Group. D. Reed Freeman Jr., a partner in Morrison & Foerster's Washington office, is a member of the firm's Privacy and Data Security Practice Group. Jacob M. Harper, an associate with the firm's Los Angeles office, is a member of the firm's Class Action, Privacy, and Appellate and Supreme Court Practice Groups.

[1] *In re DoubleClick Privacy Litig.*, No. 00-0641 (S.D.N.Y. filed Jan. 31, 2000).

[2] *See, e.g., In re Specific Media Flash Cookie Litig.*, No. SACV 10-1256-GW (C.D. Cal. filed Apr. 18, 2010) (concerning Flash local stored objects, or ''Flash cookies''); *Bose v. Interclick, Inc.*, No. 10-cv-9183 (S.D.N.Y. filed Dec. 8, 2010) (same); *Low v. LinkedIn Corp.*, No. 11-CV-01468-LHK (C.D. Cal. filed Mar. 25, 2011) (referrer URLs or ''beacons''); *In re Hulu Privacy Litig.*, No. C 11-03764 LB (N.D. Cal. filed July 29, 2011) (alleging Hulu makes unauthorized use of ''KISSmetrics,'' which assign difficult-to-remove ''ETag'' unique user identifiers on users' computers without permission).

[3] *See, e.g., Aughenbaugh v. Ringleader Digital, Inc.*, No. 8:2010-cv-01407 (C.D. Cal. filed Sept. 16, 2010) (difficult-to-delete HTML5 ''cookies'' that are on mobile devices); *In re*

 ISSN 1538-3423

using *interactive online maps*,[4] and even *privacy policies*,[5] to misappropriate private information. One recently filed action—*N.J. v. Viacom Inc.*[6]—brings the cases full circle, alleging Viacom uses Google's ''doubleclick.net'' cookies to identify users—not the adults in *DoubleClick*, but minors subject to brand new and more stringent privacy standards established just three days earlier in the Federal Trade Commission's Dec. 18, 2012, update to the Children's Online Privacy Protection Act rule.[7]

While we have seen a new wave of privacy class actions, the issues facing the federal courts are the same: how to reconcile an inarticulable discomfort with data methods asserted in privacy class actions with their constitutional mandate to address only plaintiffs with standing: the requirement that courts remedy only ''concrete'' and ''particularized'' injuries.

This article addresses how federal courts are dealing with notions of privacy harm in the online tracking context. While courts have historically told privacy plaintiffs to seek redress elsewhere—Congress, agencies, the states—district judges have been increasingly open to new notions of harm that allow them, rather than other government bodies, to address the growing but amorphous conception that something about the way their gadgets work does not feel right. The U.S. Supreme Court's recent decision in *Clapper v. Amnesty Int'l USA*, which held that fear of injury in context of government surveillance does not constitute a cognizable injury,[8] may cause those courts to reverse once again and dismiss such suits.

II. The Most Common Result: No Harm, No Foul, No Case.

Standing has traditionally made it difficult for tracking suits to survive in federal court. To show standing, a plaintiff must allege (1) an ''injury-in-fact'' that is ''concrete and particularized,'' and ''actual or imminent''; (2) an injury that is ''fairly traceable to the challenged action of the defendant''; and (3) likelihood, ''as opposed to mere[ ] speculat[ion], that the injury will be redressed by a favorable decision.''[9] Many courts have dismissed these lawsuits, at least in their earlier iterations, under the first prong: lack of an injury in fact.

In the seminal *DoubleClick* litigation, plaintiffs sued for violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, which contains a statutory minimum of $5,000 in harm to raise a viable claim. Plaintiffs claimed they met the $5,000 threshold by alleging injuries under two theories: (1) the cost to remediate damage to computers and (2) the supposed lost value of the information sought.[10]

The court rejected these ideas. Regarding the first theory—loss to the computer—the *DoubleClick* court explained that ''users may easily and at no cost prevent DoubleClick from collecting information by simply selecting options on their browsers or downloading an 'opt-out' cookie from DoubleClick's Web site.''[11] Regarding the second—lost information value—the court explained that online advertising is no different from a television marketer or ad mailer sending ads or collecting information about its customers:

> We do not commonly believe that the economic value of our attention is unjustly taken from us when we choose to watch a television show or read a newspaper with advertisements and we are unaware of any statute or caselaw that holds it is. We see no reason why Web site advertising should be treated any differently. A person who chooses to visit a Web page and is confronted by a targeted advertisement is no more deprived of his attention's economic value than are his off-line peers. Similarly, although demographic information is valued highly (as DoubleClick undoubtedly believed when it paid over one billion dollars for Abacus), the value of its collection has never been considered an economic loss to the subject. Demographic information is constantly collected on all consumers by marketers, mail-order catalogues and retailers. However, we are unaware of any court that has held the value of this collected information constitutes damage to consumers or unjust enrichment to collectors.[12]

In other words, marketers, advertisers, and broadcasters have used data to tailor their services for decades; no harm arose from those methods, and their expansion to the internet—through ''cookies'' or otherwise—is no different. With no harm, plaintiffs did not suffer any injury, let alone one totaling $5,000.

In most of the recent tracking cases, *DoubleClick*'s skepticism about typical but valueless injury claims—harm to computers, or lost value of private information—have translated seamlessly to Article III standing-based dismissals. In *LaCourt v. Specific Media Inc.*, a Flash LSO case, the plaintiffs made no allegation about harm to their computers. Instead, they relied on the notion that deprivation of an amorphous conception of ''personal data'' constituted an injury. As in *DoubleClick*, the court did not buy it: ''Plaintiffs do not explain how they were 'deprived' of the economic value of their personal information simply because their unspecified personal information was purportedly collected by a

---

Google Android Consumer Privacy Litig., No. 3:2011-MD-02264 (N.D. Cal. filed May 2, 2011) (same, concerning Google's Android platform); *Cousineau v. Microsoft Corp.*, No. 2:11-CV-01438 (W.D. Wash. filed Aug. 31, 2011) (same, concerning mobile devices running Microsoft's Windows 7); *Goodman v. HTC Am., Inc.*, No. C11-1793 (W.D. Wash. filed Oct. 26, 2011) (same, concerning HTC mobile devices and software developers).

[4] *In re Google Inc. Street View Elecs. Commc'ns Litig.*, No. C-10-MD-02184 (N.D. Cal. filed Sept. 9, 2010), challenges Google's practice of allegedly intercepting data over Wi-Fi while its camera-equipped cars collect information for use on ''Street View.''

[5] *In re Google, Inc. Privacy Policy Litig.*, No. C 12-01382 PSG (N.D. Cal. filed Mar. 20, 2012) (alleging Google's conversion of 70-odd privacy policies into a single document violates users' privacy by allowing the company ''to cross-reference and use consumers' personal information across multiple Google products.'').

[6] *N.J. v. Viacom, Inc.*, No. 2:12-cv-04322-MJW (W.D. Mo. filed Dec. 21, 2012).

[7] Children's Online Privacy Protection Rule; Final Rule, 78 Fed. Reg. 3971 (Jan. 17, 2013) (to be codified at 16 C.F.R. pt. 312) (11 PVLR 1833, 12/24/12).

[8] *Clapper v. Amnesty Int'l, USA*, 133 S.Ct. 1138, 1143 (2013) (12 PVLR 350, 3/4/13).

[9] *Friends of the Earth, Inc. v. Laidlaw Envt'l. Servs. (TOC), Inc.*, 528 U.S. 167, 180–81 (2000).

[10] *In re DoubleClick Privacy Litig.*, 154 F. Supp. 2d 497, 524 (S.D.N.Y. 2001).

[11] *Id.* at 524–25.

[12] *Id.* at 525.

  PVLR ISSN 1538-3423

third party.''[13] Plaintiffs instead left the court with a ''quasi-philosophical debate about the possible value of consumers' 'personal information' on the Internet''—not enough for Article III standing.[14]

In *Low v. LinkedIn Corp.*, Plaintiffs sued LinkedIn for allegedly sharing browsing histories with third parties; the claimed injuries were the same as in *Specific Media*. Dismissing with leave to amend, the court observed that ''Plaintiff was unable to articulate a theory of what information had actually been transmitted to third parties, how it had been transferred to third parties, and how LinkedIn had actually caused him harm'' and ''failed to allege facts that demonstrate that he was economically harmed by LinkedIn's practices.''[15]

In *In re Google Privacy Policy Litig.*, plaintiffs complained of a new privacy policy provision allowing Google to combine Gmail account information with data gathered from YouTube, Picasa, and other Google products. In a decision issued in December 2012, the court dismissed the complaint for largely the same reasons as the other courts: Plaintiffs had not ''identified a concrete harm from the alleged combination of their personal information across Google's products and contrary to Google's previous policy sufficient to create an injury in fact.''[16]

For most cases, therefore, articulating a privacy injury has been the major hurdle in allowing these suits to go forward, though it is worth noting that a handful of cases have survived.[17] But even in these rare cases where a court finds harm was sufficiently alleged, the injury comes in the form of collateral damage—lost battery life, impaired computer performance—rather than an injury from the purported privacy violation itself.

Still, even for the vast majority that did not survive after amendment, dismissal is not inevitable. Indeed, courts have stated that '''[i]t is not obvious that Plaintiffs cannot articulate some actual or imminent injury in fact. It is just that at this point they haven't offered a coherent and factually supported theory of what that injury might be.' ''[18]

III. Harm Redefined: Two Emerging Injury Theories.

Specific Media and *Google Privacy Policy* rightly noted that plaintiffs have thus far generally failed to offer a ''coherent and factually supported theory,''[19] but two emerging theories of privacy harm that have been making their way through the courts: statutory injury, and fear as injury. Neither theory contemplates injury in the traditional sense; rather, they look to recharacterizing the notion of harm in a privacy case. These will be key theories to watch.

A. Statutory Injury.

The U.S. Court of Appeals for the Ninth Circuit recently opened up federal courts to any cases in which the plaintiff alleges a statutory injury: the violation of statute for which the plaintiff qualifies for protection—regardless of whether the plaintiff has suffered an actual injury from the alleged privacy violation.

In *Jewel v. Nat'l Sec. Agency*, the plaintiff alleged that the federal government used surveillance devices attached to AT&T's network to intercept the communications of class members, thereby violating three federal surveillance statutes, all of which explicitly create private rights of action for claims of unlawful surveillance: the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801, the Electronic Communications Privacy Act (ECPA, also known as the Federal Wiretap Act), 18 U.S.C. § 2510, and the Stored Communications Act, 18 U.S.C. § 2710.[20] Although the plaintiff claimed no particular injury from the use of surveillance, the court concluded that the plaintiff alleged concrete injury sufficiently because ''a concrete 'injury required by Art. III may exist solely by virtue of statutes creating legal rights, the invasion of which creates standing.' ''[21]

Likewise, in *Edwards v. First Am. Corp.*, a home purchaser alleged that her agent unlawfully referred her title insurance business to First American pursuant to an exclusive agency agreement in violation of anti-kickback provisions of the Real Estate Settlement Procedures Act, 12 U.S.C. § 2607.[22] Finding standing, *Edwards* relied again on the principle that ''[t]he injury required by Article III can exist solely by virtue of statutes creating legal rights, the invasion of which creates standing''—even though (1) the plaintiff did not suffer a concrete injury; and (2) the statute does not itself require injury.[23]

Jewel and *Edwards* are not traditional tracking class actions, nor are they controlling outside the Ninth Circuit. But as one case put it in refusing to dismiss a tracking case against Pandora Media Inc., these cases portend an opening up of tracking suits to federal litigation ''without a showing of actual damages.''[24] Two reasons suggest *Jewel* and *Edwards* will have broad implications for privacy class actions.

First, after initially granting *certiorari* in *Edwards* (and thereby raising hope within the defense bar that the U.S. Supreme Court would reaffirm the requirement of actual harm to state a claim), the U.S. Supreme

---

[13] *LaCourt v. Specific Media, Inc.*, No. SACV 10-1256-GW, 2011 BL 333087, at *5 (C.D. Cal. Apr. 28, 2011).

[14] *Id.* at *4.

[15] *Low v. LinkedIn Corp.*, No. 11-CV-01468-LHK, 2011 BL 292771, at *4, 5 (N.D. Cal. Nov. 11, 2011) (10 PVLR 1681, 11/21/11).

[16] *In re Google Inc. Privacy Policy Litig.*, No. C 12-01382 PSG, 2012 BL 341343, at *5 (N.D. Cal. Dec. 28, 2012) (12 PVLR 40, 1/7/13).

[17] *See, e.g.*, *Goodman v. HTC Am., Inc.*, 2012 BL 180872, at *6–7 (W.D. Wash. June 26, 2012) (finding plaintiff sufficiently alleged harm through ''diminution in value of their phones due to lost battery utility and lifespan'' and because advertisements ''affected Plaintiffs' and Class Members' decisions to purchase and willingness to pay'') (11 PVLR 1106, 7/9/12); *Cousineau v. Microsoft Corp.*, No. 2:11-CV-01438, 2012 BL 344133, at * 6 (W.D. Wash. June 22, 2012) (finding the plaintiff ''demonstrate[d], with significant detail, how [the purported defect in the Microsoft camera she operated] led to the loss of her location data''; comparing *LinkedIn* and *Specific Media*).

[18] *In re Google Inc. Privacy Policy Litig.*, 2012 BL 341343, at *5 (quoting *Specific Media*, 2011 BL 333087, at *5).

[19] *Id.* at *5.

[20] *Jewel v. NSA*, 673 F.3d 902, 905–06, 908 (9th Cir. 2011) (11 PVLR 53, 1/9/12).

[21] *Id.* at 908–09 (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 578 (1992)).

[22] *Edwards v. First Am. Corp.*, 610 F.3d 514, 515–16 (9th Cir. 2010).

[23] *Id.* at 517.

[24] *Deacon v. Pandora Media, Inc.*, 901 F. Supp. 2d 1166, 1171–76 (N.D. Cal. 2012) (declining to dismiss privacy claim brought under state video rental privacy statutes) (11 PVLR 1498, 10/8/12).

Court withdrew *certiorari* as improvidently granted following oral argument.[25] Since then, district courts appear to have read the *certiorari* withdrawal as implicit affirmation that actual injury is no longer required. It will obviously be important to watch how this plays out in other cases.

Second, some district courts are applying the standing-through-statute theory to tracking actions (which, given their technology-oriented defendants, tend to arise more frequently in California than elsewhere). Thus, Judge Lucy H. Koh in the U.S. District Court for the Northern District of California refused to dismiss the amended complaints in the *LinkedIn* case based in part on *Edwards* and *Jewel*—notwithstanding that cases do not articulate an independent tangible harm.[26]

Limits do exist, however; *Jewel* and *Edwards*, even read broadly, do not provide a free ticket to federal court for just any no-injury complaint.

Injury Requirement in Underlying Statute. Defendants should be on the lookout for underlying statutes that require a showing of injury—a common requirement where plaintiffs depend on a private right of action provision. For example, in *Boorstein v. Men's Journal LLC*, no-injury plaintiffs sued Men's Journal for allegedly disclosing personal information to third parties in alleged violation of California's Unfair Competition Law (UCL), Cal. Bus. & Prof. Code § 17200, and ''Shine the Light'' Law, Cal. Civ. Code § 1798.83; plaintiffs premised standing on private right of action provisions under these statutes.[27] The court dismissed the action for lack of standing because private rights of action under the Shine the Light Law and UCL ''expressly require[ ] an injury resulting from a violation. Thus, a violation of the statute[ ], without more, is insufficient'' to establish standing, and plaintiffs failed to establish such an injury.[28]

Likewise, in *Sterk v. Best Buy Stores LP*, a case decided after *certiorari* was withdrawn in *Edwards*, a no-injury plaintiff sued Best Buy for allegedly disclosing his DVD purchase history to a corporate affiliate in purported violation of the Video Privacy Protection Act (VPPA), 18 U.S.C. § 2710, which prohibits such disclosures.[29] To assert a private right of action under the VPPA, however, the plaintiff must have been '' 'aggrieved,' meaning the individual has suffered an Article III injury-in-fact.''[30] Thus, ruled the court:

> [A] plaintiff must plead an injury beyond a statutory violation to meet the standing requirement of Article III. Plaintiff argues that a statutory violation is adequate to meet this requirement. However, while Congress is permitted to expand standing to the extent permitted under Article III, Congress cannot abrogate the basic standing requirement that an individual suffer an actual redressable injury in fact.[31]

Here, because the plaintiff did not allege any damage as a result of the alleged disclosure, he was not ''aggrieved,'' could not satisfy the underlying statutory requirements for the VPPA, and lacked standing.

Other Requirements in Underlying Statute. In addition, a court will dismiss a statutory standing case if the plaintiffs do not meet other underlying requirements, even if an injury is not one of them. In *In re Google Privacy Policy Litig.*, another set of plaintiffs made conclusory allegations that disclosure of personal data violated the ECPA, California Consumer Legal Remedies Act (Cal. Civ. Code § 1750), California Right to Privacy Statute (Cal. Civ. Code. § 3344), and the UCL. Rejecting that theory and declining to apply the statutory injury theory, the court observed that ''nothing in the precedent of the Ninth Circuit or other appellate courts confers standing on a party that has brought statutory or common law claims based on nothing more than the unauthorized disclosure of personal information''—in other words, *Edwards* and *Jewel* require valid allegations establishing all elements of a statutory violation to satisfy standing.[32] The court dismissed the case.

Application of Statute to Defendants. Defendants should also pay attention to whether the underlying statute applies to *them* as opposed to the plaintiffs. The ECPA is a common statute plaintiffs assert in tracking actions, but a growing line of cases holds that it does not apply to internet service providers accessing data in the ordinary course of business, including by making data available to ''trackers.''[33] If an ISP finds itself on the defensive end of a tracking suit, and plaintiffs premise standing on an ECPA violation, that claim should therefore fail.

Overall, although *Edwards* and *Jewel* may be interpreted by at least some courts to permit some privacy suits without injury where an independent statute creates a private right of action without injury, some valid allegation of harm is still necessary, at least when the underlying statutes require it. And even when the statute does not require an injury, statutory limitations will also undermine dubious standing claims. Those limits aside, *Jewel* and *Edwards* offer new tools for privacy plaintiffs to use in trying to bypass, in some cases, the injury in fact requirement that traditionally undermined such lawsuits.

---

[25] *First Am. Fin. Corp. v. Edwards*, 132 S. Ct. 2536, 2537 (2012) (11 PVLR 1060, 7/2/12).

[26] *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1020–22 (N.D. Cal. 2012) (declining to dismiss amended complaint; finding alleged violations of SCA sufficed for standing) (applying *Edwards* and *Jewel*) (11 PVLR 1159, 7/23/12).

[27] *Boorstein v. Men's Journal LLC*, No. CV 12-771 DSF (Ex), 2012 BL 168984, at *3–5 (C.D. Cal. June 14, 2012) (11 PVLR 1142, 7/16/12).

[28] *Id.*

[29] *See Sterk v. Best Buy Stores, L.P.*, No. 11 C 1894, 2012 BL 275176, at *1 (N.D. Ill. Oct. 17, 2012) (11 PVLR 1589, 10/29/12).

[30] *Id.* at *6 (quoting 18 U.S.C. § 2710(c)(1)).

[31] *Sterk*, 2012 BL 275176, at *6.

[32] *In re Google Inc. Privacy Policy Litig.*, 2012 BL 341343, at *5.

[33] *See, e.g., Kirch v. Embarq Mgmt. Co.*, 702 F.3d 1245, 1250 (10th Cir. 2012) (affirming dismissal of tracking suit against ISP where it had ''access to no more of its users' electronic communications than it had in the ordinary course of its business as an ISP,'' which ''is therefore protected from liability by the statutory exemption for activities conducted in the ordinary course of a service provider's business'') (12 PVLR 47, 1/7/13); *Hall v. Earthlink Network, Inc.*, 396 F.3d 500, 504–505 (2d Cir. 2005) (noting that because defendant email provider ''acquired the contents of electronic communications but did so in the ordinary course of business,'' there was no '' 'interception' '' within the statutory definition) (4 PVLR 111, 1/31/05).

  PVLR ISSN 1538-3423

B. Fear as Injury.

Another emerging theory is that mere fear of privacy harm, however indescribable or amorphous, by itself may constitute sufficient injury for Article III standing.

As an initial matter, the fear-as-injury theory had been rejected repeatedly since the U.S. Supreme Court initially addressed that notion in *Laird v. Tatum*.[34] In *Laird*, plaintiffs challenged a government surveillance system that, by secretly collecting and analyzing personal information about plaintiffs, allegedly injured them by so offending their sensibilities that it had a ''chilling effect'' on their First Amendment expressive activities.[35] The court dismissed the claim for lack of an injury in fact: ''[T]heir claim, simply stated, is that they disagree'' with the ''very existence'' of the data-gathering system, as well as the ''the type and amount of information'' gathered.[36] The plaintiffs' vague notions of discomfort and claims that their speech activities were ''chilled'' were not an ''adequate substitute for a claim of specific present objective harm or a threat of specific future harm.''[37]

Circuit courts have followed *Laird* for decades. In *Vernon v. City of Los Angeles*, the Ninth Circuit dismissed a similar claim in which the plaintiff, a police officer, lamented an ''investigation'' into whether his religious views affected his policing duties.[38] The court held that the plaintiff lacked standing because any perceived harm did not amount to a ''substantial'' injury.[39]

More recently in *Am. Civil Liberties Union v. Nat'l Sec. Agency*, plaintiffs sued to enjoin the NSA from listening to phone calls based on perceived fear of privacy violations.[40] Again, the court held that fear of privacy violation is not a viable injury. ''[T]he plaintiffs do not want the NSA listening to their phone calls or reading their emails. That is really all there is to it. . . . The problem with asserting only a breach-of-privacy claim is that, because the plaintiffs cannot show that they have been or will be subjected to surveillance personally, they clearly cannot establish standing.''[41]

Laird and its progeny were revisited in 2011, however, at least in the U.S. Court of Appeals for the Second Circuit. In *Amnesty Int'l USA v. Clapper*, plaintiffs, on behalf of lawyers, journalists, and researchers in routine communications with foreign individuals identified as terrorists, sued the U.S. government for invasions of privacy resulting from secret surveillance activity over communications with foreign terrorism suspects.[42] In 2011, against precedent, the Second Circuit held that a ''reasonable fear of future injury'' *does* meet Article III's standing requirements, and the plaintiffs may therefore go forward with their suit against the United States. Held the court:

> Because standing may be based on a reasonable fear of future injury and costs incurred to avoid that injury, and the plaintiffs have established that they have a reasonable fear of injury and have incurred costs to avoid it, we agree that they have standing.[43]

After a fractured Second Circuit denied *en banc* review,[44] the U.S. Supreme Court granted *certiorari* earlier in 2012.

Clapper does not address tracking suits directly, but its impact on standing certainly has implications for them. As Amnesty International's brief put it, plaintiffs believed they had standing because of a ''substantial risk that their communications will be monitored'' under the act and because this substantial risk has effectively ''compelled them to take costly and burdensome measures to protect sensitive and privileged information from the risk of inception.''[45] In other words, the plaintiffs hoped the court would interpret privacy ''harm'' as any action that carries a ''substantial risk'' of requiring plaintiffs to change their behavior so as to avoid the threat—whether actual or merely perceived.

On March 9, the Supreme Court rejected plaintiff's claim for harm and reversed the Second Circuit.[46] In a majority opinion by Justice Samuel Alito (and joined by Justices Anthony Kennedy, John G. Roberts, Antonin Scalia, and Clarence Thomas), the court issued two primary holdings that promise to dampen the plaintiffs' bar's enthusiasm for no-injury privacy suits.

Holding 1: Fear of Future Privacy Injury Insufficient. The court reaffirmed prior precedent to hold that Article III requires a tangible injury, not a speculative threat of one. While a possible future injury could, in some cases, pass muster under Article III, the plaintiff must allege facts showing such an injury was ''certainly impending.''[47] Without the possibility of only speculative injury satisfying the injury in fact requirement, most of the privacy class actions still making their way around the country face a new hurdle.

Holding 2: Spending Money to Prevent Future Privacy Injury Insufficient. To the extent plaintiffs would claim an injury based on money spent avoiding such an injury, the court foreclosed that possibility as well.[48] As noted above, tracking plaintiffs often premise standing on the expenditure of money on a product in reliance on a given statement, and have therefore suffered an economic injury sufficient to confer standing. *Clapper* holds, however, that such a notion would ''improperly water[ ] down the fundamental requirements of Article III.''[49] Such a theory of injury:

> improperly allow[s] respondents to establish standing by asserting that they suffer present costs and burdens that are based on a fear of surveillance, so long as that fear is not ''fanciful, paranoid, or otherwise unreasonable.'' This improperly waters down the fundamental requirements of Article III. Respondents' contention that they have standing because they incurred certain costs as a reasonable reaction to a risk of harm is unavailing—because the harm respondents seek to avoid is not certainly impending. In other words, ***respondents cannot manufacture standing merely by inflict-***

[34] *Laird v. Tatum*, 408 U.S. 1 (1972).
[35] *Id.* at 6–8.
[36] *Id.* at 13.
[37] *Id.* at 14.
[38] *Vernon v. City of Los Angeles*, 27 F.3d 1385, 1388–89 (9th Cir. 1994).
[39] *Id.* at 1395.
[40] *ACLU v. NSA*,, 493 F.3d 644, 657 (6th Cir. 2007) (6 PVLR 1081, 7/9/07).
[41] *Id.*
[42] *Amnesty Int'l USA v. Clapper*, 638 F.3d 118, 122 (2d Cir. 2011) (10 PVLR 486, 3/28/11).
[43] *Id.* at 122.
[44] *Amnesty Int'l USA v. Clapper*, 667 F.3d 163, 164 (2d Cir. 2011).
[45] Brief for Respondents at 21, 24, *Clapper v. Amnesty Int'l, USA*, 133 S.Ct. 1138, 1143 (2013) (No. 11-1025).
[46] *Clapper*, 133 S.Ct. at 1155.
[47] *Id.* at 1147–50.
[48] *Id.* at 1150–52.
[49] *Id.* at 1151.

ing harm on themselves based on their fears of hypothetical future harm that is not certainly impending.[50]

The *Clapper* plaintiffs' attempts to ''manufacture standing'' by spending money to prevent future privacy injuries is remarkably similar to efforts in tracking lawsuits.

Notwithstanding the court's clear stance on these issues, it is not clear district courts will apply it to all tracking matters. After all, 24-hour government surveillance of attorney communications with foreign clients is a far cry from the social-media-might-have-been-tracking-my-browser-history civil lawsuits that defendants are facing today.

IV. Conclusion: The Next Frontier in Standing—Causation and Redressability.

Establishing standing in tracking class actions could be on the way to becoming a lower impediment for plaintiffs, though we are only in the early stages of emerging trends that allow plaintiffs' counsel new room to argue for standing. Even if courts are ultimately more willing in some cases to recognize a privacy harm without actual injury, the other two standing prongs—causation (prong two, requiring an injury that is ''fairly traceable to the challenged action of the defendant'') and redressability (prong three, requiring a likelihood, ''as opposed to mere[ ] speculat[ion], that the injury will be redressed by a favorable decision'')—prove formidable threats to privacy suits.[51]

Thus, plaintiffs will need to allege specific facts showing the defendant's actions *caused* the plaintiffs' particular harm (whatever that may be), a difficult proposition in light of the cookie-cutter complaints frequently making broad accusations without allegations specific to the plaintiffs. And they will need to show that the court can *redress* whatever harm occurs—a particularly difficult feat because, once the data have been shared (as typically alleged), nothing a court can do can take the data back.

We will see how the rest of 2013 plays out on standing, but the current uncertainty makes clear that the cases will keep coming. Even if decisions out of the federal courts continue an emerging trend toward loosening of the standing requirements, however, defense counsel still have strong tools to fight back. All we know for sure right now is that 2013 will be an important year for the direction of privacy class actions in the United States.

[50] *Id.* at 1151 (emphasis added).

[51] *Friends of the Earth, Inc.*, 528 U.S. at 180–81.