

Litigation

WWW.NYLJ.COM

MONDAY, JULY 15, 2013



Privacy: The Next Frontier In Consumer Class Actions?

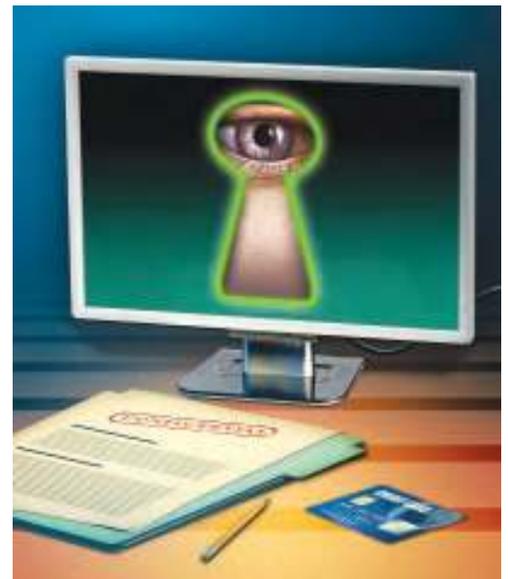
BY LAWRENCE T. GRESSER
AND KAREN H. BROMBERG

In one of the largest privacy class action suits ever filed, the U.S. Court of Appeals for the Seventh Circuit recently affirmed a federal district court decision allowing a class action to proceed against comScore, an online data research company, for alleged violations of federal privacy statutes.¹ The class, which is likely to total well over one million members, includes all individuals who have downloaded the company's software since 2005. At the heart of the complaint is plaintiff's claim that comScore's software collects more personal information about users than is disclosed in the

company's terms of service and that the company sells this information to third parties, who in turn use the data for marketing research.

Historically, plaintiffs have had a difficult time showing that they have sustained damages from alleged privacy violations, and this has frustrated most attempts to bring privacy class actions. However, in *comScore*, the lead plaintiffs were found to have standing, and the purported class was certified, based on statutory damages, not actual damages. The *comScore* decision and other recent decisions allowing privacy cases to proceed in the absence of actual damages suggest that the legal landscape may be changing, and that privacy could be the next significant frontier in consumer class action litigation.

This article provides an overview of privacy actions, reviews the defenses—injury and standing—that



have made it difficult for plaintiffs to prevail, and discusses recent case law and the future of privacy class action litigation.

Consumer Privacy Actions

Security breaches involving personal information are occurring more frequently and affecting many more people than in the

LAWRENCE T. GRESSER is the managing partner and cofounder of Cohen & Gresser. KAREN H. BROMBERG is a partner at the firm and heads its intellectual property and technology group. SOEUN (NIKOLE) LEE, an associate in the litigation and arbitration group, assisted in the preparation of this article.

past. According to a June 2013 report from the Privacy Rights Clearinghouse, “the total number of records containing sensitive personal information involved in security breaches in the United States is 608,087,870 in 3,763 data breaches since January 2005.”² The result, unsurprisingly, has been an increase in privacy litigation in general, and a rise in the frequency of privacy class actions in particular.

Consumer privacy actions are typically based on allegations of inappropriate collection of personal data resulting from: (i) human error, theft, or malicious attacks; or (ii) the affirmative acts of companies collecting personal data without appropriate notice and consent. These lawsuits have most often included common law claims of negligence, breach of contract, unjust enrichment, trespass to personal property/chattel, invasion of privacy, and/or breach of the implied covenant of good faith and fair dealing, as well as statutory claims under state consumer protections acts and state data breach notification laws. More recently, plaintiffs have sued under federal statutory causes of action such as the Computer Fraud and Abuse Act, an anti-hacking statute (the CFAA).³ But, as discussed *infra*, privacy plaintiffs asserting these claims have confronted significant obstacles.

Common Obstacles: Standing and Injury

To bring a private action in federal court,⁴ a plaintiff must show that he or she has suffered “inju-

ry in fact” sufficient to meet the case or controversy requirement of Article III of the U.S. Constitution. This injury must be “concrete and particularized” and “actual or imminent,” not merely speculative.⁵ Absent concrete allegations that a privacy plaintiff has suffered actual economic losses from the disclosure or mishandling of personal information, a number of courts have rejected allegations that plaintiffs suffered injury in fact and have dismissed privacy class actions on standing grounds. Such was the case for the plaintiffs in *In re Google Street View Elec. Commc’ns Litig.*⁶ There, the court dismissed plaintiffs’ claims under California’s consumer protection statute because plaintiffs failed to plead facts showing that Google’s alleged collection of their Wi-Fi usage data caused plaintiffs to lose or expend money.⁷

A similar inability to allege actual damages resulted in the dismissal of a \$5 million class action lawsuit against the social networking site LinkedIn, involving the alleged compromise of 6.5 million users’ passwords.⁸ Here, the plaintiffs pled a total of nine causes of action including breach of contract, unjust enrichment, breach of the implied covenant of good faith and fair dealing, breach of an implied contract to reasonably safeguard user information, negligence and negligence *per se*. Holding that any damage to LinkedIn users was abstract and that plaintiffs failed to pro-

vide evidence of injury that was concrete and particularized, the court dismissed the complaint.

‘comScore’ and other recent decisions allowing privacy cases to proceed in the **absence of actual damages** suggest that the legal landscape may be changing, and that **privacy** could be the **next significant frontier in consumer class action litigation**.

In *LaCourt v. Specific Media*,⁹ plaintiffs alleged that Specific Media, an online third-party ad network, used flash cookies, which cannot be deleted and never expire, to track users across websites and to circumvent the privacy and security controls of users who had set their browsers to block third-party cookies. The plaintiffs asserted state law claims for invasion of privacy, consumer protection violations, unfair competition, trespass, and unjust enrichment, and a federal claim for violation of the CFAA. The federal district court in California found that plaintiffs, who did not articulate how they were deprived of the economic value of their personal information, failed to allege harm or economic injury sufficient to demonstrate standing.¹⁰

Changing Landscape?

Recent cases however, suggest that the legal landscape may be

changing. In 2010, the U.S. Court of Appeals for the Ninth Circuit held in *Edwards v. First Am.*¹¹ that a plaintiff who had suffered no monetary loss nonetheless had standing to challenge a violation of the Real Estate Settlement Procedures Act (RESPA). RESPA prohibits the payment of “any fee, kickback, or thing of value” in exchange for business referrals.¹² The statute provides that when a violation occurs, the defendant can be held liable in an “amount equal to three times the amount of any charge paid for such settlement service.”¹³ The court held that because RESPA gave the plaintiff a statutory cause of action, the plaintiff had standing to pursue claims against the defendants despite its failure to allege any actual or concrete injury from the RESPA violation.

Although *Edwards* arose in the narrow context of an alleged RESPA violation, the implications of the decision for privacy litigation have not been lost on plaintiffs’ lawyers: They are increasingly filing purported privacy class actions based upon alleged violations of federal privacy laws with statutory damages provisions, including the Electronic Communications Privacy Act (ECPA), also known as the Wiretap Act (18 U.S.C. §§2510, et seq.), and the Stored Communications Act (SCA) (18 U.S.C. §§2701, et seq.).¹⁴ In addition to providing a potential avenue for avoiding standing problems, the relatively modest statutory damages available under these statutes can be enormous when aggregated over a class.¹⁵

Privacy Class Actions After ‘com-Score’

The *comScore* decision shows that if plaintiffs are found to have standing to bring privacy claims based solely on statutory damages, with no need to make “concrete and particularized” allegations of actual damages, the resulting class actions can be enormous. In *comScore*, the U.S. District Court for the Northern District of Illinois certified a putative privacy class based on the statutory damages available under the ECPA and the SCA and the superiority of the class action mechanism for resolving plaintiffs’ CFAA claims, notwithstanding uncertainty about the existence and amount of plaintiffs’ actual damages. Plaintiffs in *comScore* brought claims for unjust enrichment and for violations of the SCA, the ECPA, and the CFAA, alleging that defendants improperly obtained and used personal information after consumers downloaded and installed the company’s software. The crux of plaintiffs’ claims was that comScore’s data collection violated the terms of the User License Agreement and the Downloading Statement. The court denied class certification on the unjust enrichment claim, but granted certification for the federal statutory claims, rejecting comScore’s argument that the issue of whether each individual plaintiff suffered damage or loss from the alleged privacy violations precluded class certification. The court ruled that the SCA and the ECPA provided

statutory damages for which only a violation must be established, and noted that although the CFAA required proof of loss aggregating to at least \$5,000 in value, “individual factual damages issues do not provide a reason to deny class certification when the harm to each plaintiff is too small to justify resolving the suits individually.”¹⁶

Courts in the Ninth Circuit have likewise permitted privacy class actions to go forward based solely on claimed violations of federal statutes with statutory damages provisions. In *Gaos v. Google*,¹⁷ the U.S. District Court for the Northern District of California dismissed the named plaintiff’s common law claims but allowed her claims under the SCA to survive, holding that “the SCA provides a right to judicial relief based only on a violation of the statute without additional injury.” See also *In re Facebook Privacy Litig.*¹⁸ (plaintiffs established standing when they alleged a violation of the ECPA); *In re Zynga Privacy Litig.*¹⁹ (holding that “a violation of one’s statutory rights under the SCA is a concrete injury”); *Cousineau v. Microsoft*²⁰ (denying motion to dismiss for lack of Article III standing where plaintiff alleged an SCA violation).

However, the Fourth Circuit has reached the opposite conclusion. In *Van Alstyne v. Elec. Scriptorium*²¹ the Fourth Circuit ruled that a plaintiff must prove actual damages to recover a statutory award under the SCA. See also *Sterk v. Best Buy Stores*,²² (claim for violation of Video Privacy Protection Act based

on alleged disclosure of plaintiff's movie purchase history was insufficient to confer Article III standing).

It is not too soon to wonder whether the emerging split between courts permitting privacy cases to go forward based solely on statutory damages and those requiring actual damages will eventually be resolved by the U.S. Supreme Court—and to wonder what might happen there. The implications of this seemingly narrow question for class action jurisprudence and for online businesses are enormous: *comScore* suggests that if a lead plaintiff in a purported privacy class action can overcome the standing hurdle by citing statutory damages, then the class certification hurdle may also be manageable. The stakes are high.

.....●●.....

1. *Harris v. comScore*, No. 11 C 5807, 2013 WL 1339262 (N.D. Ill. April 2, 2013). The U.S. Court of Appeals for the Seventh

Circuit, without opinion, denied the petition for leave to appeal class certification.

2. See Chronology of Data Breaches: Security Breaches 2005—Present, Privacy Rights Clearinghouse (April 20, 2005; updated June 29, 2013), <http://www.privacyrights.org/data-breach>.

3. 18 U.S.C. §1030 (2008)

4. Privacy class actions are typically brought in federal court either because a violation of a federal law is alleged, 28 USC §1331, or because removal is appropriate under the Class Action Fairness Act (CAFA). CAFA provides federal district courts with original jurisdiction to hear a class action if the class has more than 100 members, the parties are minimally diverse, and the "matter in controversy exceeds the sum or value of \$5,000,000." 28 U.S.C. §1332(d)(2), (d)(5)(B).

5. *Friends of the Earth v. Laidlaw Env'tl. Servs. (TOC)*, 528 U.S. 167, 180-81 (2000) (citations and internal quotation marks omitted).

6. 794 F. Supp. 2d 1067 (N.D. Cal. 2011).

7. Plaintiffs also pled claims for violation of the federal and state wiretap statutes. The court declined to dismiss the federal statutory claim, and dismissed the state Wiretap Act claim on preemption grounds.

8. *In re LinkedIn User Privacy Litigation*, No. 5:12-CV-03088 EJD (N.D. Cal. March 6, 2013) (order granting motion to dismiss).

9. No. SACV 10-1256-GW (JCGx), 2011 WL 1661532 (C.D. Cal. April 28, 2011).

10. The pertinent provision of the CFAA requires a showing of economic damages of \$5,000 in a one-year period. 18 U.S.C. §1030(c)(4)(A)(i)(I). The CFAA defines damage as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. §1030(e)(8).

11. 610 F.3d 514 (9th Cir. 2010), cert. granted in part sub nom. *First Am. Fin. v. Edwards*, 131 S. Ct. 3022 (2011), and cert. dismissed as improvidently granted sub nom. *First Am. Fin. v. Edwards*, 132 S. Ct. 2536 (2012).

12. 12 U.S.C. §2607(a), (b)

13. 12 U.S.C. §2607(d)(2)

14. The ECPA prohibits the intentional interception, use, or disclosure of wire and electronic communication and provides for damages in the greater amount of \$100 per day of violation or a total of \$10,000, and the SCA prohibits unauthorized access to stored electronic communications, and minimum damages of \$1000 per plaintiff. For alleged privacy violations involving video content, plaintiffs also have brought claims under the Video Privacy Protection Act (VPPA) (18 U.S.C. §2710), a statute enacted by Congress after Robert Bork's video rental history was published during his Supreme Court nomination process. The VPPA makes any

"video tape service provider" that discloses rental or sales information outside the ordinary course of business liable for up to \$2,500 per plaintiff. Other statutes that sometimes come into play in privacy cases are the Telephone Consumer Protection Act (47 U.S.C. §227), which regulates telemarketing and provides for statutory damages of at least \$500 per violation, trebled to \$1500 for willful violations, and the Driver's Privacy Protection Act (18 U.S.C. §§2721, et seq.), which protects the confidentiality of driver's license records and provides for \$2,500 in minimum damages per person.

15. In *Leysoto v. Mama Mia I*, 255 F.R.D. 693, 697-98 (S.D. Fla. Feb. 17, 2009), plaintiffs filed a class action against a local restaurant with approximately \$40,000 in net assets alleging violations under the Fair and Accurate Credit Transactions Act (FACTA) which requires that merchants truncate credit card and debit card numbers on electronically-printed customer receipts. FACTA provides for statutory damages between \$100 and \$1,000 per violation of the law. 15 U.S.C. §1681n(a)(1)(A). Because the putative class in *Leysoto* involved an estimated class size of 46,000, the claimed damages were between \$4.6 million and \$46 million despite the lack of evidence that no member of the class suffered actual economic injury. Given the disproportionately large class damages, in contrast to plaintiffs' lack of injury, the district court concluded that "a class action is not the superior method for fair adjudication of a FACTA dispute under Rule 23(b)(3)."

16. *Id.*, 2013 WL 1339262 at *10.

17. No. 5:10-CV-4809 EJD, 2012 WL 1094646, at *3 (N.D. Cal. March 29, 2012).

18. 791 F. Supp. 2d 705, 711-13 (N.D. Cal. 2011) (but finding that although the injury component was met under the ECPA, plaintiffs failed to plead the elements to state a claim for a violation of that act).

19. No. C 10-04680 JWW, 2011 WL 7479170, at *2 (N.D. Cal. June 15, 2011).

20. No. C11-01438-JCC (W.D. Wash. June 22, 2012) (order denying in part, and granting in part, motion to dismiss)

21. 560 F.3d 199, 203-08 (4th Cir. 2009).

22. No. 11 C 1894, 2012 WL 5197901 (N.D. Ill. Oct. 17, 2012).

Reprinted with permission from the July 15, 2013 edition of the NEW YORK LAW JOURNAL © 2013 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-257-3382 or reprints@alm.com. # 070-07-13-20



COHEN & GRESSER LLP