ROPES & GRAY

ALERT

Privacy & Data Security

November 10, 2016

Recent Decisions Highlight Legal Risks Associated with Product Cybersecurity Vulnerabilities

Attorneys
Douglas H. Meal
Heather Egan Sussman
James S. DeGraw
Seth C. Harrington
Mark P. Szpak
Michelle Visser
Paul D. Rubin
Laura G. Hoey
Marc P. Berger
David T. Cohen
Joseph Santiesteban

Last month, plaintiffs in two product cybersecurity class actions were partially successful in surviving motions to dismiss, continuing the recent trend by plaintiffs and regulatory agencies to expand the pool of defendants in data security litigation. The cases, both from the Northern District of California, illustrate a growing trend in which public and private plaintiffs seek to hold companies responsible for alleged security defects in their *products*, as distinct from defects in the security of personal information held by companies on their own computer networks. Claims of this sort, which often are premised on a contention that the company misled consumers about the security vulnerability in question, underscore the need for caution and diligence when deciding whether and how to disclose potential product cybersecurity issues. Companies should also carefully consider whether and how to implement what the Federal Trade Commission has called "security by design," or building security into new products at the outset of the planning process.

In re Lenovo Adware Litigation

In *In re Lenovo Adware Litigation*, the court considered whether to dismiss various statutory and tort causes of action against Lenovo for distributing laptops containing software – Superfish's VisualDiscovery – that allegedly intercepted secure communications between users' browsers and websites they visited, and then served advertisements based on the contents of the communication. Plaintiffs, the users who had bought the laptops, alleged that this invaded their privacy, resulted in significant disruption to their computers' functioning, and exposed them to the risk that hackers could intercept their communications. Plaintiffs brought various statutory claims based on alleged unauthorized access to plaintiffs' computers and consumer protection law claims based on Lenovo's alleged failure to disclose the installation of VisualDiscovery.

The court found that plaintiffs sufficiently alleged that they suffered injuries from the installation in the form of privacy intrusion and decreased laptop performance such that they had standing to sue under Article III of the U.S. Constitution. The court also found, however, that the alleged exposure to potential hacking was not sufficient for standing.

On the merits, the court declined to dismiss claims based on Lenovo's alleged unauthorized access to plaintiffs' computers and conspiracy with Superfish to do the same. But it refused to certify a class of these claims because individualized questions predominated regarding whether the software in fact accessed each plaintiff's laptop and data (given that consumers used their computers differently), as well as whether and to what extent such unauthorized access caused plaintiffs' alleged injuries.

The court permitted plaintiffs' statutory claims for "fraudulent omissions" under California consumer protection law. In the court's view, plaintiffs sufficiently alleged that Lenovo had exclusive knowledge of the privacy and performance risks associated with the installation of VisualDiscovery, such that Lenovo had a duty to disclose, but failed to disclose, the information to consumers. The court also certified a class on these claims, reasoning that proof

of these claims (unlike the unauthorized-access claims) did not depend on users' individual experiences with the software.

Edenborough v. ADT, LLC

In the other case, *Edenborough v. ADT, LLC*, plaintiff, a customer of home security company ADT, alleged that ADT's security systems used wireless transmissions that were unsecured and unencrypted, and that ADT misrepresented and failed to disclose information regarding these vulnerabilities at the time of sale in violation of California consumer protection statutes. The court dismissed the misrepresentation-based claims, finding ADT's public statements that its technology was "innovative," the "most advanced," and "make[s] the difference" were mere puffery. As in *Lenovo*, however, the court permitted plaintiffs' omission-based claims to proceed, finding that ADT had a duty to disclose the alleged vulnerability because, in the court's view, plaintiff sufficiently alleged that it was a material fact unknown to plaintiff.

Key Takeaways for Companies

ADT and *Lenovo* continue the recent trend by plaintiffs and regulatory agencies to expand the pool of defendants in data security litigation. Traditionally, the FTC and other public and private actors have sought to hold liable those companies that collect or use personal information that is the subject of an alleged breach. More recently, they have sought to expand the boundaries of liability to any party who allegedly may have had some role in putting internet-connected products, or the personal information transmitted through those products, at risk of unauthorized access. Private plaintiffs have been one of the primary forces behind this trend. *See, e.g.*, *Flynn v. FCA US LLC*, No. 3:15-cv-855, slip op. (S.D. Ill. Sept. 23, 2016) (partially sustaining claims premised on ability of cars to be hacked); *Cahen v. Toyota Motor Corp.*, 2015 WL 7566806 (N.D. Cal. Nov. 25, 2015) (dismissing such claims for lack of standing). The FTC has also made product security a top priority, with enforcement actions against ASUSTeK (seller of home internet routers), TRENDnet, Inc. (manufacturer of web-based cameras), Upromise, Inc. (developer of a web-browser toolbar), and Oracle (developer of a computing platform), among others. *See In re ASUSTeK*, C-4587, Complaint, FTC Dkt. No. C-4587 (July 18, 2016); *In re TRENDnet, Inc.*, Complaint, FTC Dkt. No. C-4426 (Jan. 16, 2014); *In re Upromise, Inc.*, Complaint, FTC Dkt. No. C-4351 (Mar. 27, 2012); *In re Oracle Corporation*, Complaint, FTC File No. 132 3115 (Dec. 21, 2015).

Because these cases are frequently, although not always, premised on the company's alleged misstatements or omissions regarding the product's vulnerability, companies should carefully evaluate what their public-facing statements say, and do not say, to consumers about potential security vulnerabilities in their products. As *ADT* and *Lenovo* demonstrate, in some circumstances staying silent about a vulnerability may expose a company to liability, but disclosure of a vulnerability can also create a risk of being found to have misrepresented the vulnerability in question.

Moreover, regulators and private plaintiffs have alleged claims in this area (such as for negligence or unfair trade practices) that do not hinge on what the company said or did not say about the vulnerability in question, but rather on whether the company acted "reasonably" in allowing the product to have that vulnerability in the first place or in addressing the vulnerability once it was discovered. Companies therefore also need to evaluate whether a security vulnerability in a given product could give rise to litigation or regulatory investigations on its own, regardless of what the company has or has not said to consumers regarding that vulnerability. This evaluation should include a consideration of whether and how to implement what the Federal Trade Commission has called "security by design," or building security into devices at the outset. *See* Federal Trade Commission Staff Report, *Internet of Things: Privacy & Security in a Connected World*, at iii (Jan. 2015).

For more information regarding *Lenovo* and *ADT* or to discuss data security practices generally, please feel free to contact Doug Meal, Heather Egan Sussman, Jim DeGraw, Seth Harrington, Mark Szpak, Michelle Visser, Paul

Rubin, Laura Hoey, Marc Berger, David Cohen, Joe Santiesteban, or another member of Ropes & Gray's leading privacy & data security team.