ROPES & GRAY

ALERT

Privacy & Data Security

January 11, 2016

The FTC's Recent Enforcement Action Against Oracle Further Expands the Growing Pool of Potential Data Security Defendants

Attorneys

Heather Egan Sussman
Douglas H. Meal
James S. DeGraw
Seth C. Harrington
David McIntosh
Mark P. Szpak
Michelle Visser
Paul D. Rubin
Marc P. Berger
David T. Cohen
Sunil Shenoi

On December 21, 2015, Oracle Corporation ("Oracle") reached an agreement with the Federal Trade Commission ("FTC") to settle charges that it allegedly deceived customers regarding the security provided by updates to its Java Platform, Standard Edition software ("Java SE"). The proposed consent order requires Oracle to provide information about older versions of Java SE on consumers' computers and to give consumers the ability to easily uninstall older versions of Java SE. The action is significant because it represents a growing trend in which public and private plaintiffs seek to hold parties responsible for alleged data security failures even though such parties did not themselves collect or receive personal information from consumers. In addition, the case illustrates the FTC's willingness to seek to hold companies responsible for what some might consider boilerplate statements about the security of their products, even when there is no suggestion that such statements influenced consumers' purchasing decisions.

I. Overview of the Action

The FTC's enforcement action against Oracle relates to Java SE, which has been installed on over 850 million personal computers. Java SE provides support for a vast array of features consumers use when browsing the web, including online gaming, chatrooms, and 3D images.

Sun Microsystems first debuted Java SE in the late 1990s. After acquiring Sun in 2010, Oracle has released several new versions of Java SE. According to the FTC, when consumers installed certain updates to Java SE in approximately 2010 or later, they were shown messages stating that "Java provides safe and secure access to . . . Java content" and that consumers would have "the latest . . . security improvements." Since at least 2010, however, Oracle allegedly was aware of at least 44 types of malware that had been developed. For example, the FTC alleged that attackers used known exploit kits to install key loggers that would capture consumers' usernames and passwords, which *could* be used to log into a consumer's financial accounts. In addition, since at least 2011, Oracle allegedly knew but did not inform consumers (hereinafter, the "incomplete disclosure") that Java SE updates did not automatically remove all prior versions of Java SE that had been installed on a consumer's computer.

According to the FTC, Oracle's alleged incomplete disclosure was a deceptive act that violated Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a), and affected consumers in three ways. First, the FTC alleged that consumers were more likely to unknowingly have older, allegedly less secure versions of Java SE installed on their computers. Second, attackers allegedly targeted the vulnerabilities in the older versions of Java SE and obtained consumers' personal information. Finally, by failing to inform consumers that the Java SE update process did not remove all previously installed versions from consumers' computers, Oracle allegedly left consumers vulnerable to the foreseeable risk that attackers would target these computers through malware and steal consumers' personal information.

The FTC and Oracle agreed to a proposed order that requires Oracle to (i) notify existing Java SE users that they may have older, allegedly less secure versions of Java SE on their computer, (ii) provide information to consumers about

versions of Java SE that would be installed before and after installing a Java SE update, and how to remove any older versions, and (iii) provide consumers with information and a tool for uninstalling older versions of Java SE. The proposed order also requires that Oracle refrain from misrepresenting (i) the privacy or security of Java SE or similar software, or (ii) how to uninstall older iterations of the software.

II. Expanding the Pool of Defendants

The FTC's enforcement action against Oracle is notable in several respects. First, the action underscores the recent trend by plaintiffs and regulatory agencies to expand the pool of defendants in data security litigation and regulatory enforcement actions. Traditionally, the FTC and other public and private actors have sought to hold liable companies that collect or use personal information that is the subject of an alleged breach. *See e.g.*, FTC, Protecting Consumer Privacy in an Era of Rapid Change, at 22 (2012), *available here* (stating that the FTC's proposed privacy framework applies to "commercial entities that collect or use consumer data"). Recently, data breach plaintiffs and regulatory authorities have sought to expand the boundaries of liability to any party who may have had some role in putting personal information at risk of unauthorized access. The FTC has been one of the primary forces behind this trend, with enforcement actions against TRENDnet, Inc. (manufacturer of web-based cameras), Upromise, Inc. (developer of web-browser toolbar), and this recent action against Oracle, among others, illustrating the FTC's shift in focus toward product manufacturers and application providers that allegedly expose personal information (broadly construed) to a risk of unauthorized access. *See 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).

Not to be outdone, state attorneys general and individual and class action plaintiffs have similarly sought to expand the pool of defendants liable for a data breach. For example, a federal court held that Cotton Patch Cafe, Inc.'s claims for violation of Texas's Deceptive Trade Practices Act, negligent misrepresentation, and fraud by nondisclosure claims could proceed to trial against Micros Systems, Inc. (payment processing equipment provider), where Cotton Patch claimed that the credit card processing system sold by Micros to Cotton Patch did not comply with industry regulations and caused a data breach at a Cotton Patch restaurant. *Cotton Patch Cafe, Inc. v. Micros Sys., Inc.*, CIV.A. MJG-09-03242, 2012 WL 5986773 (D. Md. Nov. 27, 2012). Similarly, in 2015, the Connecticut Attorney General's Office and class action plaintiffs initiated an investigation and a federal lawsuit, respectively (both of which are still ongoing), against Lenovo Inc. (computer manufacturer) and Superfish (application provider) regarding Superfish software that was pre-installed on Lenovo computers and allegedly put consumers at risk of hacker activity. Press Release, State of Connecticut Office of the Attorney General, AG Jepsen Opens Inquiry into Lenovo, Superfish Privacy and Security Concerns (Mar. 2, 2014), *available here*; *In re: Lenovo Adware Litig.*, Case No. 5:15-md-02624 (N.D. Cal. 2015) (consolidating approximately 22 cases in a multi-district litigation).

A security compliance assessor also recently was sued in connection with data breaches. Trustwave Holdings Inc., an IT security firm, has been sued in connection with the 2013 data breach of the South Carolina Department of Revenue, for which Trustwave allegedly performed security services, but Trustwave successfully defeated the action at the motion to dismiss stage. Trustwave also was sued twice in connection with its alleged assessments of Target Corporation's compliance with payment card industry security standards in the years prior to Target's 2013 data breach, but one suit was voluntarily dismissed and Trustwave was dropped from the other suit when it was consolidated with other suits against Target in the MDL litigation.

Even a third-party contractor whose work was unrelated to the data security field has been sued when its client suffered a data breach that was allegedly linked to the contractor. In 2015, the Office of Personnel Management ("OPM") and KeyPoint Government Solutions ("KeyPoint") were sued in connection with OPM's 2015 data breach. KeyPoint, which conducts background investigations for the federal government, suffered its own data breach in December 2014 in which KeyPoint's OPM credentials were allegedly stolen and then used by intruders to gain unauthorized access to OPM's systems. The case is currently pending.

Overall, governmental and private plaintiffs appear interested in suing any parties with any role affecting the security of a company or individual that suffers a breach. As defendants fight back, courts may be called upon to determine

the point at which a party's role in allegedly putting personal information at risk is too attenuated to warrant liability for a data breach.

III. Statements about Security

The FTC's enforcement action against Oracle also represents another example of how the FTC continues to aggressively pursue enforcement actions based on statements commonly used in technology product marketing. The FTC's complaint pointed to two messages about security that customers might view during the Java SE installation process. One message indicated that by utilizing Java's auto-update process, consumers would have "the latest . . . security improvements." This statement is not far-reaching – Java SE consumers might not have been able to receive security updates sooner than by using the auto-update feature, and the security improvement may well have been the most recent ones released. The second message merely said that "Java provides safe and secure access to . . . Java content."

The FTC based its claims on these statements even though, as the FTC's complaint acknowledged, in 2010 Oracle had disclosed in a separate FAQ page that consumers could have older versions of Java SE on their computers and that by removing the older versions "Java applications will run with the most up-to-date security." While the FTC acknowledged this disclosure, the FTC found it inadequate since it was not linked to the allegedly deceptive statements and did not expressly explain that the update process did not automatically remove all older versions of Java SE.

The FTC's action against Oracle also further illustrates the FTC's aggressive interpretation of the "materiality" requirement for a deception claim. Courts have held that a deception claim under Section 5 of the FTC Act requires proof that a representation, omission, or practice was material, meaning that it "involves information that is important to consumers and, hence, likely to affect their choice of, or conduct regarding, a product." *FTC v. Cantkier*, 767 F. Supp. 2d 147, 152 (D.D.C. 2011) (quoting *F.T.C. v. Cyberspace.Com LLC*, 453 F.3d 1196, 1201 (9th Cir. 2006)). In support of this requirement, the FTC alleged only that Oracle's alleged failure to disclose that all prior versions of Java SE would not be removed during the update process "would be material to consumers' decisions whether to take further action after 'updating' Java SE to protect their computers." The notion that consumers carefully digest all statements made about data security during the software update process, and then make decisions about "whether to take further action," is debatable.

By arguing that such statements by Oracle during the Java SE installation process qualified as a deceptive act under the FTC Act – even though the company's website had already made disclosures regarding potential security issues associated with older versions of the software and the statements were not made in an advertising context – the FTC may ironically discourage some companies from providing information to consumers about their data security practices, out of fear that any perceived incompleteness in the statements will be treated as "deceptive." The FTC's decision to proceed in this case underscores that companies should carefully weigh the risks of making statements about data security, particularly when there is no legal or business need to make the statements. Those companies that do decide to make statements about data security should take note of the FTC's apparent contention in the Oracle matter that caveats needed to make a statement non-deceptive must appear in proximity to the statement.

* * * * *

For more information regarding the settlement between the FTC and the Oracle or to discuss data security practices generally, please feel free to contact Heather Egan Sussman, Doug Meal, Jim DeGraw, Seth Harrington, David McIntosh, Mark Szpak, Michelle Visser, Paul Rubin, Marc Berger, David Cohen, or another member of Ropes & Gray's leading privacy & data security team.