wiley

NEWSLETTER

The Lenovo-FTC Settlement Highlights Risks of Certain Data Analytics Practices

Privacy in Focus

Settlement Summary

On September 5, 2017, the Federal Trade Commission (FTC) announced it had entered a no-fault settlement with Lenovo, Inc., over allegations that the company preinstalled ad software which compromised customers' online security and privacy.[1] The FTC's complaint, originally filed in 2014, alleged that certain consumer laptops sold in the United States came pre-installed with a "man-in-the-middle" adware program developed by a company called Superfish, Inc. According to the FTC, this adware operated without the users' knowledge or consent, intercepted users' web traffic, accessed sensitive customer data, and created security vulnerabilities.[2]

When the FTC settlement with Lenovo was announced, Acting FTC Chairman Maureen Ohlhausen told reporters that the settlement "sends a very important message" to companies that "everyone in the chain really needs to pay attention" to data security. Companies, including manufacturers, software and technology providers, and companies that used third-party vendors to interact with or manage customer data, should closely monitor the collection of user data. Missteps could result in FTC enforcement, restrictive settlements, widespread state consumer protection claims, and class action litigation.

Brought under Section 5 of the FTC Act, the FTC's complaint alleged unfair and deceptive acts. Specifically, the FTC charged Lenovo with one count of deceptive failure to disclose, for not disclosing to consumers how the adware would operate. It also charged Lenovo with two counts of unfairness for (1) unfair preinstallation of man-in-the-middle software, "without [providing] adequate notice or

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

[obtaining] informed consent" from users; and (2) unfair security practices, for Lenovo's failure "to take reasonable measures to assess and address security risks created by third-party software preinstalled on its laptop..."[3].

Under the FTC's Consent Order, Lenovo is prohibited from misrepresenting any features of preinstalled software related to consumer Internet browsing-based advertising. In addition, Lenovo must obtain affirmative user consent before installing such software on its laptops, provide instructions for how the consumer may revoke consent to the covered software's operation, and provide reasonable and effective means for consumers to opt out, disable, or remove all the covered software's operations, including uninstallation. Further, for a period of 20 years, Lenovo is required to implement a comprehensive software security program for most preloaded software, which is subject to third-party audits. The FTC may also seek monetary fines if Lenovo fails to abide by the Consent Order.[4] In a separate agreement, Lenovo agreed to pay $3.5 million to settle charges brought by the State Attorneys General under state consumer protection laws.[5]

How the Superfish Adware Worked

In 2014, Lenovo partnered with Superfish to sell new Lenovo laptops pre-installed with Superfish-created adware called VisualDiscovery. Superfish specializes in visual search technology that can analyze a picture or video and determine what object is featured in that image. Using that technology, VisualDiscovery generates advertisements with links for products that are similar to what the user is searching for and observing on their laptop's screen. These targeted ads are inserted into a user's web browser and appear as if they were part of the website the user was visiting.

In order to encrypt web traffic, browsers and web servers use Hypertext Transfer Protocol Secure (HTTPS). Using HTTPS, a server sends a public certificate to the user's browser through which the user's browser can verify the identity and authenticity of the website. The public certificates for these HTTPS connections are issued by a handful of trusted certificate authorities, such as Symantec. After verification using the certificate, the browser and server are able to generate an encryption key for the communication session, allowing each party to encrypt and decrypt the communications.

According to the FTC's Complaint, the Superfish adware on Lenovo laptops interrupted this process. Instead of communicating directly with a website using HTTPS, a user on a Lenovo laptop first communicates with VisualDiscovery, which operated as a proxy. The adware installed a root certificate that replicated the root certificate that would normally be supplied by a trusted website. Using its own root certificate, the adware verified to the user's browser that it was communicating with a trusted website. From the user's point of view, the transaction appeared to be a normal, encrypted HTTPS transaction.

The adware, however, decrypted the user's web traffic and analyzed it to generate targeted ads. VisualDiscovery then re-encrypted the traffic and forwarded it to the website the user requested. The FTC referred to this as a man-in-the-middle attack because both the user and the website were unaware that a third party (in this case, Superfish) had intercepted their communication.

Beyond legal and privacy concerns, many data security experts argued that the Superfish adware was a security disaster, because of vulnerabilities in the way the adware encrypts and decrypts information.[6] Superfish used the same root certificate and the same password to decrypt the private key on every Lenovo laptop, which hackers could have used to easily imitate a trusted website or decrypt all traffic sent using an adware-installed Lenovo laptop.[7]

Class Action Lawsuits

Beyond the FTC and state charges, multiple plaintiffs' attorneys filed class action lawsuits against Lenovo and Superfish. Among a variety of claims, plaintiffs alleged that the defendants violated the Computer Fraud and Abuse Act (CFAA).[8] The CFAA is broad in scope and generally prohibits knowingly accessing a computer without authorization or exceeding authorized access and causing harm.[9] The CFAA provides both criminal and civil sanctions and was designed to prevent traditional hacking attacks. It has also been used in a wide variety of contexts beyond traditional hacking, and federal courts often struggle to define what conduct violates the CFAA.

In June 2015, a federal multidistrict litigation panel consolidated some of the Lenovo lawsuits in the Northern District of California. In January 2016, Lenovo filed a motion to dismiss. Judge Whyte issued an order in October 2016, granting Lenovo's motion to dismiss in part. The court dismissed the claims under the federal Electronic Communications Privacy Act as well as several related state claims.

However, with respect to the CFAA claim, and several other statutory unauthorized access and consumer protection claims, Lenovo's motion to dismiss was denied.[10] In denying Lenovo's motion, the court stated "Lenovo entered into an agreement with Superfish to preinstall VisualDiscovery on several laptop models and 'share in any revenues that flowed from the partnership.'" Further, plaintiffs alleged that Lenovo executives were provided with demonstrations of the VisualDiscovery adware, and "some [executives] expressed concerns" about the SSL decoder programs and how the adware may negatively impact Lenovo laptops.[11] As of October 2017, the case, *In re: Lenovo Adware Litigation*, remains active.

Why This Matters

Technologies are changing rapidly, and the application of decades-old laws like the Wiretap Act and the CFAA to these new technologies is not straightforward and has resulted in ambiguity about whether certain technologies and practices are legal. With more companies monetizing ad revenue and leveraging big data, businesses need to be aware that the FTC will scrutinize not only their use and handling of consumer data, but also the practices of third-party vendors with access to that data. Hardware manufacturers, like Lenovo, may receive scrutiny for software preinstalled on their products.

These claims are highly fact-dependent but typically turn on two primary issues: first, whether the user has given consent to a business to use their personal data; and second, the nature of the technical arrangement between the user, the business, and any third-party vendors. For companies that are evaluating the legality of a new data collection practice, the analysis should include a detailed understanding about how the technology works and what notification will be provided to consumers.

[1] FTC, Lenovo Settles FTC Charges it Harmed Consumers With Preinstalled Software on its Laptops that Compromised Online Security (Sept. 5, 2017), *available at* https://www.ftc.gov/news-events/press-releases/2017/09/lenovo-settles-ftc-charges-it-harmed-consumers-preinstalled.

[2] *In the Matter of Lenovo (United States) Inc.*, Complaint, FTC File No. 152 3134 (Sept. 2017), *available at* https://www.ftc.gov/system/files/documents/cases/1523134_lenovo_united_states_complaint.pdf.

[3] *Id.*

[4] *See Lenovo Consent Order*.

[5] *See, e.g.* Press Release, Cal. Dep't of Justice, Attorney General Becerra Announces $3.5M Settlement with Lenovo for Preinstalling Software that Compromised Security of its Computers (Sept. 5, 2017), *available at* https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-35m-settlement-lenovo-preinstalling-software; *see also* Press Release, N.J. Dep't of Law & Pub. Safety, Attorney General Announces $3.5 Million Multi-State Settlement with Lenovo over Hacker-Vulnerable Software (Sept. 5, 2017), *available at* http://nj.gov/oag/newsreleases17/pr20170905a.html.

[6] *See* U.S. Computer Emergency Readiness Team, Alert (TA15-051A) Lenovo Superfish Adware Vulnerable to HTTPS Spoofing, (Feb. 20, 2015), *available at* https://www.us-cert.gov/ncas/alerts/TA15-051A.

[7] *See* Aditi Jhaveri, "Superfish software on Lenovo notebooks: What you can do," FTC Consumer Info. (Feb. 27, 2015), *available at* https://www.consumer.ftc.gov/blog/2015/02/superfish-software-lenovo-notebooks-what-you-can-do.

[8] 18. U.S.C. §§ 1030 *et seq.*

[9] *See* 18 U.S.C. § 1030(a).

[10] *In re: Lenovo Adware Litigation*, No. 15-md-02624, 2016 WL 6277245 (N.D. Cal. Oct. 27, 2016).

[11] *In re: Lenovo Adware Litigation*, 2016 WL 6277245, at *6.