[BILLING CODE: 6750-01S]

FEDERAL TRADE COMMISSION

[File No. 152 3134]

Lenovo (United States) Inc.; Analysis to Aid Public Comment

AGENCY: Federal Trade Commission.

ACTION: Proposed consent agreement.

SUMMARY: The consent agreement in this matter settles alleged violations of federal law prohibiting unfair or deceptive acts or practices. The attached Analysis to Aid Public Comment describes both the allegations in the complaint and the terms of the consent order -- embodied in the consent agreement -- that would settle these allegations.

DATES: Comments must be received on or before October 5, 2017.

ADDRESSES: Interested parties may file a comment online or on paper, by following the instructions in the Request for Comment part of the **SUPPLEMENTARY INFORMATION** section below. Write: "Lenovo (United States) Inc., Matter No. 152 3134" on your comment, and file your comment online at https://ftcpublic.commentworks.com/ftc/lenovoconsent by following the instructions on the web-based form. If you prefer to file your comment on paper, write "Lenovo (United States) Inc., Matter No. 152 3134" on your comment and on the envelope, and mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue, NW, Suite CC-5610 (Annex D), Washington, DC 20580, or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street, SW, 5th Floor, Suite 5610 (Annex D), Washington, DC 20024.

FOR FURTHER INFORMATION CONTACT: Linda Holleran Kopp, (202-326-2267) and Tiffany George (202-326-3040), Bureau of Consumer Protection, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

SUPPLEMENTARY INFORMATION: Pursuant to Section 6(f) of the Federal Trade Commission Act, 15 U.S.C. 46(f), and FTC Rule 2.34, 16 CFR 2.34, notice is hereby given that the above-captioned consent agreement containing a consent order to cease and desist, having been filed with and accepted, subject to final approval, by the Commission, has been placed on the public record for a period of thirty (30) days. The following Analysis to Aid Public Comment describes the terms of the consent agreement, and the allegations in the complaint. An electronic copy of the full text of the consent agreement package can be obtained from the FTC Home Page (for September 5, 2017), on the World Wide Web, at https://www.ftc.gov/news-events/commission-actions.

You can file a comment online or on paper. For the Commission to consider your comment, we must receive it on or before October 5, 2017. Write "Lenovo (United States) Inc., Matter No. 152 3134" on your comment. Your comment - including your name and your state - will be placed on the public record of this proceeding, including, to the extent practicable, on the public Commission Website, at https://www.ftc.gov/policy/public-comments.

Postal mail addressed to the Commission is subject to delay due to heightened security screening. As a result, we encourage you to submit your comments online. To make sure that the Commission considers your online comment, you must file it at https://ftcpublic.commentworks.com/ftc/lenovoconsent by following the instructions on the web-based form. If this Notice appears at http://www.regulations.gov/#!home, you also may file a comment through that website.

If you prefer to file your comment on paper, write "Lenovo (United States) Inc., Matter No. 152 3134" on your comment and on the envelope, and mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue, NW, Suite CC-5610 (Annex D), Washington, DC 20580, or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street, SW, 5th Floor, Suite 5610 (Annex D), Washington, DC. 20024. If possible, submit your paper comment to the Commission by courier or overnight service.

Because your comment will be placed on the publicly accessible FTC Website at https://www.ftc.gov, you are solely responsible for making sure that your comment does not include any sensitive or confidential information. In particular, your comment should not include any sensitive personal information, such as your or anyone else's Social Security number; date of birth; driver's license number or other state identification number, or foreign country equivalent; passport number; financial account number; or credit or debit card number. You are also solely responsible for making sure that your comment does not include any sensitive health information, such as medical records or other individually identifiable health information. In addition, your comment should not include any "trade secret or any commercial or financial information which . . . is privileged or confidential" – as provided by Section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule 4.10(a)(2), 16 CFR 4.10(a)(2) – including in particular competitively sensitive information such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

Comments containing material for which confidential treatment is requested must be filed in paper form, must be clearly labeled "Confidential," and must comply with FTC Rule 4.9(c). In particular, the written request for confidential treatment that accompanies the comment must

include the factual and legal basis for the request, and must identify the specific portions of the comment to be withheld from the public record. *See* FTC Rule 4.9(c). Your comment will be kept confidential only if the General Counsel grants your request in accordance with the law and the public interest. Once your comment has been posted on the public FTC Website – as legally required by FTC Rule 4.9(b) – we cannot redact or remove your comment from the FTC Website, unless you submit a confidentiality request that meets the requirements for such treatment under FTC Rule 4.9(c), and the General Counsel grants that request.

Visit the FTC Website at http://www.ftc.gov to read this Notice and the news release describing it. The FTC Act and other laws that the Commission administers permit the collection of public comments to consider and use in this proceeding, as appropriate. The Commission will consider all timely and responsive public comments that it receives on or before October 5, 2017. For information on the Commission's privacy policy, including routine uses permitted by the Privacy Act, see https://www.ftc.gov/site-information/privacy-policy.

Analysis of Agreement Containing Consent Order to Aid Public Comment

The Federal Trade Commission has accepted, subject to final approval, an agreement containing a consent order from Lenovo (United States), Inc. ("Lenovo").

The proposed consent order has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission again will review the agreement and the comments received and will decide whether it should withdraw from the agreement or make final the agreement's proposed order.

This matter involves Lenovo, one of the world's largest personal computer manufacturers, and its preinstallation on certain consumer laptops of VisualDiscovery, an ad-

injecting software developed by Superfish, Inc. and customized for Lenovo. VisualDiscovery injected pop-up ads of similar-looking products sold by Superfish's retail partners whenever a consumer's cursor hovered over a product image while browsing on a shopping website. For example, when a consumer's cursor hovered over an image of owl-shaped pendants on a shopping website like amazon.com, VisualDiscovery would show the user pop-up ads of similar-looking owl pendants. To do so, VisualDiscovery acted as a "man-in-the-middle" between consumers' browsers and the websites they visited, including encrypted https:// websites. This man-in-the-middle technique allowed VisualDiscovery to see all of a consumer's sensitive personal information that was transmitted on the Internet, such as login credentials, Social Security numbers, financial account information, medical information, and email communications. VisualDiscovery then collected, transmitted to Superfish servers, and stored a more limited subset of user information, including the website addresses visited by consumers, consumers' IP addresses, and a unique identifier assigned by Superfish to each user's laptop. Superfish had the ability to collect additional information from Lenovo users through VisualDiscovery at any time.

To facilitate its injection of pop-up ads into encrypted https:// websites, VisualDiscovery installed a self-signed root certificate in the laptop's operating system. This allowed VisualDiscovery to replace the digital certificates for https:// websites with VisualDiscovery's own certificates for those websites and caused consumers' browsers to automatically trust the VisualDiscovery-signed certificates. Digital certificates are part of the Transport Layer Security (TLS) protocol that, when properly validated, serve as proof that consumers are communicating with the authentic https:// website and not an imposter.

As alleged in the complaint, VisualDiscovery's substitution of digital certificates for https:// websites with its own certificates for those websites created two significant security vulnerabilities. First, VisualDiscovery did not adequately verify that websites' digital certificates were valid before replacing them with its own certificates, which were automatically trusted by consumers' browsers. This rendered a critical browser security function useless because browsers would no longer warn consumers that their connections were untrusted when they visited potentially spoofed or malicious websites with invalid digital certificates.

The complaint also alleges that VisualDiscovery created a second security vulnerability by using a self-signed root certificate with the same private encryption key and the same easy-to-crack password on every laptop rather than employing private keys unique to each laptop. This violated basic encryption key management principles because attackers who cracked the simple password on one consumer's laptop could then target every affected Lenovo user with man-in-the-middle attacks that could intercept consumers' electronic communications with any website, including those for financial institutions and medical providers. Such attacks would provide attackers with unauthorized access to consumers' sensitive personal information, such as Social Security numbers, financial account numbers, login credentials, medical information, and email communications. This vulnerability also made it easier for attackers to deceive consumers into downloading malware onto any affected Lenovo laptop. The risk that this vulnerability would be exploited increased after February 19, 2015, when news of these vulnerabilities became public and bloggers posted instructions on how the vulnerabilities could be exploited.

The complaint alleges that Lenovo failed to discover these significant security vulnerabilities because it failed to take reasonable measures to assess and address security risks created by third-party software it preinstalled on its laptops. Specifically, Lenovo allegedly:

- failed to adopt and implement written data security policies applicable to third-party preinstalled software;
- failed to adequately assess the data security risks of third-party software prior to preinstallation;
- failed to request or review any information prior to preinstallation about Superfish's data security policies, procedures or practices;
- failed to require Superfish by contract to adopt and implement reasonable data security measures;
- failed to assess VisualDiscovery's compliance with reasonable data security standards; and
- failed to provide adequate data security training for employees responsible for testing third-party software.

The complaint alleges that Lenovo's failure was an unfair act that caused or was likely to cause substantial consumer injury that consumers could not reasonably avoid, and that there were no countervailing benefits to consumers or competition.

The Commission's complaint also alleges that Lenovo failed to make adequate disclosures about VisualDiscovery to consumers. Lenovo did not disclose to consumers that it had preinstalled VisualDiscovery prior to purchase, and the software had limited visibility on the consumer's laptop. Lenovo only disclosed VisualDiscovery through a one-time pop-up window the first time consumers visited a shopping website that stated,

> Explore shopping with VisualDiscovery: Your browser is enabled with VisualDiscovery which lets you discover visually similar products and best prices while you shop.

The pop-up window contained a small opt-out link at the bottom of the pop-up that was easy for consumers to miss. If a consumer clicked on the pop-up's 'x' close button, or anywhere else on the screen, the consumer was opted in to the software.

The complaint alleges that this pop-up window's disclosures were inadequate and violated Section 5 of the FTC Act by failing to disclose, or failing to disclose adequately, that VisualDiscovery would act as a man-in-the-middle between consumers and all the websites they visited, including encrypted https:// websites, and collect and transmit certain consumer Internet browsing data to Superfish. These facts would be material to consumers' decisions whether or not to use VisualDiscovery.

The complaint also alleges that Lenovo's preinstallation of the ad-injecting software that, without adequate notice or informed consent, acted as a man-in-the-middle between consumers and all the websites they visited, including encrypted https:// websites, and collected and transmitted certain consumer Internet browsing data to Superfish was an unfair act that caused or was likely to cause substantial injury to consumers, and that was not offset by countervailing benefits to consumers or competition and was not reasonably avoidable by consumers.

The proposed consent order contains provisions designed to prevent Lenovo from engaging in similar acts and practices in the future.

Part I of the proposed order prohibits Lenovo from making any misrepresentations about certain preinstalled software on its personal computers.

Part II of the proposed order requires Lenovo to obtain a consumer's affirmative express consent, with certain limited exceptions, prior to any preinstalled software a) injecting advertisements into a consumer's Internet browsing session, or b) transmitting, or causing to transmit, the consumer's personal information to any person or entity other than the consumer. Lenovo must also provide instructions for how consumers can revoke their consent to the software's operation by providing a reasonable and effective means for consumers to opt out, disable or remove the software.

Parts III and IV of the proposed order require Lenovo to implement a mandated software security program that is reasonably designed to address security risks in software preinstalled on its personal computers, and undergo biennial software security assessments of its mandated software security program by a third party.

Parts V through IX of the proposed order are standard reporting and compliance provisions. Part V requires dissemination of the order now and in the future to all current and future principals, officers, directors, and managers, and to persons with managerial or supervisory responsibilities relating to Parts I – IV of the order. Part VI mandates that Lenovo submit a compliance report to the FTC one year after issuance, and then notices, as the order specifies, thereafter. Parts VII and VIII requires Lenovo to retain documents relating to its compliance with the order for a five-year period, and to provide such additional information or documents necessary for the Commission to monitor compliance. Part IX states that the Order will remain in effect for 20 years.

The purpose of this analysis is to aid public comment on the proposed order. It is not intended to constitute an official interpretation of the complaint or proposed order, or to modify in any way the proposed order's terms.

By direction of the Commission.

Donald S. Clark,

Secretary.

Statement of Acting Chairman Maureen K. Ohlhausen

In the Matter of Lenovo, Inc.

I support this important case and the strong settlement. I write separately to caution against an over broad application of our failure to disclose (sometimes called "deceptive omission") authority. We should hew to longstanding case law and avoid circumventing congressionally-established limits on our authority. I therefore respectfully disagree with my colleague's position that we should expand Count I to allege additional failures to disclose.

Most FTC deception cases involve an express misrepresentation ("This sugar pill cures cancer") or an express statement that gives rise to an implied claim that is false or misleading ("Many people who take this sugar pill don't die of cancer").

Although the FTC and the courts have also recognized that a failure to disclose can be deceptive, this has limits.[1] For every product there is a potentially enormous amount of information that at least some consumers might wish to know when deciding whether to

[1] *International Harvester Co.*, 104 FTC 949 (1984), represents the Commission's most comprehensive effort to define deceptive omissions, and that framework remains in place today. *See also, Cliffdale Associates, Inc.*, 103 FTC 110, App. A at 2 (1984) ("Deception Statement").

purchase or use it.[2] Copious disclosures would be both impractical and unhelpful, and the law sensibly does not require sellers to disclose all information that a consumer might find important.

Thus, the FTC has generally found a failure to disclose to be deceptive in two categories of cases. First, the FTC has found "half-truths" to be deceptive, where a seller makes a truthful statement that creates a material misleading impression that the seller does not correct.[3] Most of the FTC's failure to disclose cases are half-truth cases, and many could be restyled as cases of implied false or misleading claims. For example, a complaint addressing the claim that "Many people who take this sugar pill don't die of cancer" could allege an implied false claim that the pill cures cancer, or could allege a deceptive failure to disclose that the pill does not reduce the chances of dying from cancer.

Second, and less frequently, the FTC has found a seller's silence to be deceptive "under circumstances that constitute an implied but false representation."[4] Such implied false representations can arise from "ordinary consumer expectations as to the irreducible minimum performance standards of a particular class of good."[5] Stated differently, offering a product for sale implies that the product is "reasonably fit for [its] intended uses," and that it is "free of gross safety hazards."[6] If the product does not meet ordinary consumer expectations of minimum performance, or if the product is not reasonably fit for its intended uses, the seller must disclose that. For example, it would be deceptive for an auto dealer to sell, without a disclosure, a normal-

[2] *International Harvester*, 104 FTC at 1059 (explaining why the FTC does not treat pure omissions as deceptive).

[3] *Id.* at 1057-58.

[4] *Id.* at 1058.

[5] *Id.*

[6] *Id.* at 1058-59.

looking car with a maximum speed of 35 miles per hour.[7] Consumers expect cars to be able to reach highway speeds, and thus the dealer must disclose to the buyer that the car does not meet that ordinary expectation.

In such cases, an omission is misleading under the FTC Act if the consumers' ordinary fundamental expectations about the product were violated. Mere annoyances that leave the product reasonably fit for its intended use do not meet this threshold.[8] Thus, a dealer's failure to disclose that some might find a car's seatbelt warning to be annoyingly loud would not be a deceptive omission because consumers have no ordinary expectations about car seatbelt warnings that would mislead them absent a disclosure.

As *International Harvester* sets out at length, a deceptive omission is distinct from an unfair failure to warn or other forms of unfair omissions.[9] The FTC has brought such cases under its unfairness authority where it has met the statutorily mandated higher burden of showing that the conduct causes or is likely to cause substantial consumer injury that is not reasonably avoidable by the consumer and is not outweighed by benefits to consumers or competition.[10]

Turning to the case at hand, the complaint alleges that VisualDiscovery advertising software on Lenovo laptops acted as a man-in-the-middle between consumers and the websites they visited. As such, the software had access to all secure and unsecure consumer-website communications and rendered useless a critical security feature of the laptops' web browsers.

---

[7] *Id.* at n.29.

[8] *Id.* at 1058; Deception Statement at n.4 ("Not all omissions are deceptive, even if providing the information would benefit consumers.… Failure to disclose that the product is not fit constitutes a deceptive omission.")

[9] *Id.* at 1051 ("It is important to distinguish between the circumstances under which omissions are deceptive … and the circumstances under which they amount to an unfair practice.").

[10] 15 U.S.C. §45(n).

Such practices introduced gross hazards inconsistent with ordinary consumer expectations about the minimum performance standards of software. As a result, the man-in-the-middle functionality and the problems it generated made VisualDiscovery unfit for its intended use as software. Thus, Count I properly alleges that Lenovo failed to disclose, or disclose adequately, that VisualDiscovery acted as a man-in-the-middle.[11]

Although Commissioner McSweeny and I both support Count I, she would add allegations that Lenovo failed to disclose that VisualDiscovery injected ads into shopping websites and slowed web browsing. She argues that the injected ads and slowed web browsing altered the internet experience of consumers, and thus VisualDiscovery failed to meet "ordinary consumer expectations as to the irreducible minimum performance standards of [that] particular class of good."[12]

I respectfully disagree. Lenovo failed to disclose that VisualDiscovery would act as a man-in-the-middle. However, Lenovo *did* disclose that the software would introduce advertising into consumers' web browsing, although its disclosure could have been better. Furthermore, to the extent ordinary consumers expect anything from advertising software, they likely expect it to affect their web browsing and to be intrusive, as the popularity of ad blocking technology shows. In addition, unlike the man-in-the-middle technique, VisualDiscovery's ad placement and web browsing effects did not introduce gross hazards obviously outside of consumers' ordinary expectations for advertising software. In short, although VisualDiscovery's ad placement and

[11] Count I of the complaint is pled in the form of a half-truth, but could also be pled as a failure to correct a false representation implied from circumstances, and so I address Commissioner McSweeny's argument as framed.

[12] Statement of Commissioner Terrell McSweeny at 1 (*citing International Harvester*, 104 FTC at 1058).

effect on web browsing may have been irritating to many, those features did not make VisualDiscovery unfit for its intended use. Therefore, I do not find Lenovo's silence about those features to be a deceptive omission.

Fortunately, the outcome in this case does not depend on resolving our disagreement on the application of deceptive omission to advertising software. My goal in writing separately is to maintain the clear distinction set forth in *International Harvester* between deceptive failures to disclose and unfair omissions.[13] When evaluating the legality of a party's silence, we must be careful not to circumvent unfairness's higher evidentiary burden by simply restyling an unfair omission as a deceptive omission.

[13] *International Harvester*, 104 FTC at 1051.

Statement of Commissioner Terrell McSweeny

In the Matter of Lenovo, Inc.

I support the Commission's complaint against Lenovo, but I am troubled by conduct in this case that the Commission fails to challenge. According to the complaint, Lenovo, Inc. preinstalled software on computers that was designed to serve advertisements to consumers while they were browsing websites. The software, called VisualDiscovery, acted as a "man-in-the-middle" between the consumers and all of the websites with which they communicated. It allegedly actively contravened the security posture of consumers' computers, leaving them vulnerable both to attack from cyber-criminals and to transmitting personal information across the web to Superfish, Inc. servers. These unfair practices violate the Federal Trade Commission Act and are appropriately challenged by the FTC in Counts II and III of the complaint.

But Lenovo's unlawful conduct went beyond the data security failings alleged in the complaint. The complaint also describes how the software it preinstalled on computers would: (1) inject pop-up ads every time consumers visited a shopping website; and (2) disrupt web browsing by reducing download speeds by almost 25 percent and upload speeds by 125 percent. These facts were not disclosed to consumers and these omissions were deceptive.

Moreover, the FTC alleges that the VisualDiscovery software was designed to be difficult to discover. Consumers were initially made aware of the existence of the VisualDiscovery software via a pop-up window the first time they visited an ecommerce site. But clicking to close that window *opted consumers into the program*. The initial pop-up window failed to disclose that VisualDiscovery would follow the consumers from shopping site to shopping site; slow the performance and functionality of the web sites they visited; and compromise their security and privacy throughout each online browsing session.

Under Section 5 of the FTC Act, the failure to disclose information necessary to prevent the creation of a false impression is a deceptive practice.[1] A seller's silence may make an implied representation "based on ordinary consumer expectations as to the irreducible minimum performance standards of a particular class of good."[2] In this case, Lenovo deceptively omitted that VisualDiscovery would alter the very internet experience for which most consumers buy a computer. I believe that if consumers were fully aware of what VisualDiscovery was, how it compromised their system, and how they could have opted out, most would have decided to keep VisualDiscovery inactive.

This is an exceptionally strong case and clearly articulates how the Commission uses its unfairness tools to protect the data security and privacy of consumers. I support Count I, but believe the FTC should have included additional deceptive conduct alleged in the complaint within the count. The FTC should not turn a blind eye to deceptive disclosures and opt-ins, particularly when consumers' privacy and security are at stake.

[1] *FTC Policy Statement on Deception*, 103 F.T.C. 174, 175 (1984) (appended to *Cliffdale Assocs., Inc.*,
103 F.T.C. 110 (1984)).

[2] *Int'l. Harvester Co.*, 104 F.T.C. 949, 1058 (1984).

[FR Doc. 2017-19385 Filed: 9/12/2017 8:45 am; Publication Date: 9/13/2017]