

Complaint

IN THE MATTER OF

LENOVO (UNITED STATES) INC.CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF
SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT*Docket No. C-4636; File No. 152 3134**Complaint, December 20, 2017 – Decision, December 20, 2017*

This consent order addresses Lenovo (United States), Inc.’s preinstallation on certain consumer laptops of VisualDiscovery, an ad-injecting software developed by Superfish, Inc. and customized for Lenovo. The complaint alleges that VisualDiscovery’s substitution of digital certificates for https:// websites with its own certificates for those websites created significant security vulnerabilities. The complaint further 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. The consent order prohibits Lenovo from making any misrepresentations about certain preinstalled software on its personal computers and 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.

Participants

For the *Commission*: *Tiffany George* and *Linda Holleran Kopp*.

For the *Respondent*: *Rebecca Engrav* and *Janis Kestenbaum, Perkins Coie LLP*.

COMPLAINT

The Federal Trade Commission, having reason to believe that Lenovo (United States) Inc. has violated Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a), and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Lenovo (United States) Inc. (“Lenovo”) is a Delaware corporation with its principal office or place of business

Complaint

located at 1009 Think Place, Morrisville, North Carolina 27560-9002.

2. The acts and practices of Respondent alleged in the Complaint have been in or affecting commerce, as “commerce” is defined in Section 4 of the Federal Trade Commission Act.

RESPONDENT’S BUSINESS PRACTICES

3. Respondent is one of the world’s largest manufacturers of personal computers, including desktop computers, laptops, notebooks, and tablets. Respondent employs approximately 7,500 people in the United States.

4. In August 2014, Respondent began selling certain laptop models to U.S. consumers with a preinstalled ad-injecting software (commonly referred to as “adware”), known as VisualDiscovery. VisualDiscovery was developed by Superfish, Inc. , a Delaware corporation with its principal office or place of business located in Palo Alto, California.

5. VisualDiscovery delivered pop-up ads to consumers of similar-looking products sold by Superfish’s retail partners whenever a consumer’s cursor hovered over the image of a product on a shopping website. For example, if a consumer’s cursor hovered over a product image while the consumer viewed owl pendants on a shopping website like Amazon.com, VisualDiscovery would overlay pop-up ads onto that website of other similar-looking owl pendants sold by Superfish’s retail partners.

6. VisualDiscovery also operated as a local proxy that stood between the consumer’s browser and all the Internet websites that the consumer visited, including encrypted https:// websites (commonly referred to as a “man-in-the-middle” or a “man-in-the-middle” technique). 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 web-based email communications. VisualDiscovery then collected, transmitted to Superfish servers, and stored a more limited subset of user

Complaint

information, including: the URL visited by the consumer; the text appearing alongside images appearing on shopping websites; the name of the merchant website being browsed; the consumer's IP address; and a unique identifier assigned by Superfish to the user's laptop (collectively, "consumer Internet browsing data"). Superfish had the ability to collect additional information from Lenovo users through VisualDiscovery at any time.

**THE PREINSTALLATION OF VISUALDISCOVERY ON
LENOVO LAPTOPS**

7. VisualDiscovery is a Lenovo-customized version of Superfish's ad-injecting software, WindowShopper. During the course of discussions with Superfish, Lenovo required a number of modifications to Superfish's WindowShopper program. The most significant modification resulted from Lenovo's requirement that the software inject pop-up ads on multiple Internet browsers, including browsers that the consumer installed after purchase. This condition required WindowShopper to change the way it delivered ads.

8. To provide Respondent's required functionality, Superfish licensed and incorporated a tool from Komodia, Inc. With this tool, VisualDiscovery operated on every Internet browser installed on consumers' laptops, and injected pop-up ads on both <http://> and encrypted <https://> websites.

9. To facilitate its injection of pop-up ads into encrypted <https://> connections, VisualDiscovery replaced the digital certificates for <https://> websites visited by consumers with Superfish's own certificates for those websites. Digital certificates, part of the Transport Layer Security (TLS) protocol, are electronic credentials presented by <https://> websites to consumers' browsers that, when properly validated, serve as proof that consumers are communicating with the authentic website and not an imposter.

10. VisualDiscovery was able to replace the websites' digital certificates because it installed a self-signed root certificate in the laptop's operating system, which caused consumers' browsers to automatically trust the VisualDiscovery-signed certificates. This allowed VisualDiscovery to act as a man-in-the-middle, causing

Complaint

both the browser and the website to believe that they had established a direct, encrypted connection, when in fact, the VisualDiscovery software was decrypting and re-encrypting all encrypted communications passing between them without the consumer's or the website's knowledge.

11. Superfish informed Respondent of its use of the Komodia tool and warned that it might cause antivirus companies to flag or block the software. And in fact, as discussed *infra* at Paragraphs 20-24, the modified VisualDiscovery software (using the Komodia tool) created two significant security vulnerabilities that put consumers' personal information at risk of unauthorized access. Without requesting or reviewing any further information, Lenovo approved Superfish's use of the Komodia tool.

12. After a security researcher reported to Respondent that there were problems with VisualDiscovery's interactions with https:// websites in September 2014, Respondent began to preinstall a second version of VisualDiscovery in December 2014 that did not operate on https:// websites or contain the root certificate that created the security vulnerabilities discussed *infra*. Respondent did not update laptops that had the original version of VisualDiscovery preinstalled or stop the shipment of those laptops. In total, over 750,000 U.S. consumers purchased a Lenovo laptop with VisualDiscovery preinstalled, with over half of those consumers purchasing laptops with the original version of VisualDiscovery preinstalled.

**RESPONDENT'S DISCLOSURES ABOUT
VISUALDISCOVERY'S PREINSTALLATION AND
OPERATION WERE INADEQUATE**

13. Respondent did not make any disclosures about VisualDiscovery to consumers prior to purchase. It did not disclose the name of the program; the fact that the program would act as a man-in-the-middle between consumers and all websites with which they communicated, including sensitive communications with encrypted https:// websites; or the fact that the program would collect and transmit consumer Internet browsing data to Superfish.

Complaint

14. The VisualDiscovery software was designed to have limited visibility on the consumer's laptop. For example, the software was always on and running in the background without the consumer having to do anything to start or otherwise activate the software. There was no desktop icon for VisualDiscovery; there was no icon in the computer's applications tray to indicate that VisualDiscovery was running; and VisualDiscovery was not listed among the 'All Programs' list of installed programs, available when the consumer clicked on the Windows' Start button. The software was only visible on the laptop if consumers navigated to the Control Panel, where consumers could uninstall the program through Windows' 'Add/Remove' feature.

15. After consumers had purchased their laptops, VisualDiscovery displayed a one-time pop-up window the first time consumers visited a shopping website. Respondent worked with Superfish to customize the language of this pop-up window for its users. This pop-up 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 also 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. An example of the initial pop-up window is attached as Exhibit A.

16. The initial pop-up window failed to disclose, or failed to disclose adequately that VisualDiscovery would act as a man-in-the-middle between consumers and all websites with which they communicated, including sensitive communications with encrypted https:// websites, and collect and transmit consumer Internet browsing data to Superfish. These facts would be material to consumers in their decision of whether or not to use VisualDiscovery.

17. The omitted information was not available to consumers from other sources. VisualDiscovery's Privacy Policy and End

Complaint

User License Agreement (EULA), available via hyperlinks in the initial pop-up window, similarly omitted the material information.

18. Even if consumers saw and clicked on the opt-out link, the opt-out was ineffective. Clicking on the link would only stop VisualDiscovery from displaying pop-up ads; the software still acted as a man-in-the-middle between consumers and all websites with which they communicated, including sensitive communications with encrypted https:// websites.

**VISUALDISCOVERY CREATED SECURITY
VULNERABILITIES THAT PUT CONSUMERS'
PERSONAL INFORMATION AT RISK OF
UNAUTHORIZED ACCESS**

19. VisualDiscovery's substitution of websites' digital certificates with its own certificates created two security vulnerabilities related to the TLS protocol. The TLS protocol uses digital certificates that, when properly validated, serve as proof that consumers are communicating with the authentic https:// website. When a user connects to a website with an invalid certificate, the browser will warn the user that the connection is untrusted. An untrusted connection indicates that unknown parties could intercept any information sent over that connection or that the endpoint of the connection may not be the website the consumer intended to visit.

20. Here, however, 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 caused consumers to not receive warning messages from their browsers if they visited potentially spoofed or malicious websites with invalid digital certificates, and rendered a critical security feature of modern web browsers useless.

21. VisualDiscovery created an additional security vulnerability because it used a self-signed root certificate that employed the same private encryption key, with the same easy-to-crack password ("komodia") on every laptop, rather than employing private keys unique to each laptop. This practice violated basic encryption key management principles because

Complaint

attackers could exploit this vulnerability to issue fraudulent digital certificates that would be trusted by consumers' browsers. Not only was the password easy to crack – security researchers did so in less than hour – but once attackers had cracked the password on one consumer's laptop, they could target every Lenovo user with VisualDiscovery preinstalled 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.

22. The risk that this vulnerability would be exploited increased after February 19, 2015, when security researchers published information about both vulnerabilities and bloggers described how to exploit the private encryption key vulnerability. The next day, on February 20, 2015, the United States Computer Emergency Readiness Team (US-CERT), a division of the Department of Homeland Security responsible for analyzing and reducing cyber threats and vulnerabilities, issued a public warning about the VisualDiscovery security vulnerabilities. US-CERT recommended that consumers remove VisualDiscovery with a free removal tool offered by Respondent that would also remove its root certificate. Many consumers spent considerable time removing VisualDiscovery and its root certificate from their affected laptops. Merely opting out, disabling, or uninstalling VisualDiscovery would not address the security vulnerabilities.

23. Respondent stopped shipping laptops with VisualDiscovery preinstalled on or about February 20, 2015, although some of these laptops, including laptops with the original version of VisualDiscovery preinstalled, were still being sold through various retail channels as late as June 2015.

Complaint

**RESPONDENT FAILED TO IMPLEMENT REASONABLE
SECURITY REVIEWS OF ITS CUSTOMIZED
VISUALDISCOVERY SOFTWARE**

24. Respondent failed to take reasonable measures to assess and address security risks created by third-party software preinstalled on its laptops. For example,

- a. Respondent failed to adopt and implement written data security standards, policies, procedures or practices that applied to third-party software preinstalled on its laptops;
- b. Respondent failed to adequately assess the data security risks of third-party software prior to preinstallation;
- c. Respondent did not request or review any information about Superfish's data security policies, procedures and practices, including any security testing conducted by or on behalf of Superfish during its software development process, nor did Respondent request or review any information about the Komodia tool after Superfish informed Respondent that it could cause VisualDiscovery to be flagged by antivirus companies;
- d. Respondent failed to require Superfish by contract to adopt and implement reasonable data security measures to protect Lenovo users' personal information;
- e. Respondent failed to assess VisualDiscovery's compliance with reasonable data security standards, including failing to reasonably test, audit, assess or review the security of VisualDiscovery prior to preinstallation; and
- f. Respondent did not provide adequate data security training for those employees responsible for testing third-party software.

Complaint

25. As a result of these security failures, Respondent did not discover VisualDiscovery's significant security vulnerabilities, as described above. Respondent could have discovered the VisualDiscovery security vulnerabilities prior to preinstallation by implementing readily available and relatively low-cost security measures.

26. Consumers had no way of independently knowing about Respondents' security failures and could not reasonably have avoided possible harms from such failures.

**RESPONDENT'S PREINSTALLATION OF
VISUALDISCOVERY HARMED CONSUMERS**

27. VisualDiscovery harmed consumers with respect to accessing the Internet. Accessing the Internet, including for private, encrypted communications, represents a central use of consumer laptops.

28. VisualDiscovery prevented consumers from having the benefit of basic security features provided by their Internet browsers for encrypted https:// connections, as described above. The non-profit Electronic Frontier Foundation (EFF) found that affected Lenovo laptop users who participated in its SSL Observatory research project visited websites with invalid certificates, but did not receive warnings from their browsers that the potentially malicious websites they visited were improperly authenticated. Some consumers have also complained that they suffered from fraudulent bank account and credit card activity within months of buying their affected Lenovo laptops.

29. VisualDiscovery also caused many websites to load slowly, render improperly, or not load at all. According to a test conducted by Superfish on an affected Lenovo laptop, VisualDiscovery slowed Internet upload speeds by approximately 125 percent and download speeds by almost 25 percent. In one noted incident, a consumer could not use his Lenovo laptop to log onto his employer's Virtual Private Network (VPN) because the employer's network did not recognize the Superfish digital certificate.

Complaint

30. These harms are not outweighed by countervailing benefits to consumers or competition, and are not reasonably avoidable by consumers.

FTC ACT VIOLATIONS
Count One – Deceptive Failure to Disclose

31. As alleged in Paragraphs 13-18, Respondent represented, directly or indirectly, expressly or by implication, to consumers that VisualDiscovery was enabled on their browser and would allow consumers to discover similar looking products with the best prices.

32. Respondent's representation failed to disclose, or failed to disclose adequately, that VisualDiscovery would act as a man-in-the-middle between consumers and all websites with which communicated, including sensitive communications with encrypted https:// websites, and collect and transmit consumer Internet browsing data to Superfish, as alleged in Paragraph 6.

33. Respondent's failure to disclose the material information described in Paragraph 32, in light of the representation set forth in Paragraph 31, was, and is, a deceptive act or practice.

34. The acts and practices of Respondent as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

Count Two – Unfair Preinstallation of Man-in-the-Middle Software

35. As alleged in Paragraphs 13-18, 27 and 29-30, Respondent's preinstallation of ad-injecting software that, without adequate notice or informed consent, acted as a man-in-the-middle between consumers and all the websites with which they communicated, including sensitive encrypted https:// websites, and collected and transmitted consumer Internet browsing data to Superfish, caused or is likely to cause substantial injury to consumers, that is not offset by countervailing benefits to consumers or competition, and is not reasonably avoidable by consumers. This practice was, and is, an unfair act or practice.

Complaint

36. The acts and practices of Respondent as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

Count Three – Unfair Security Practices

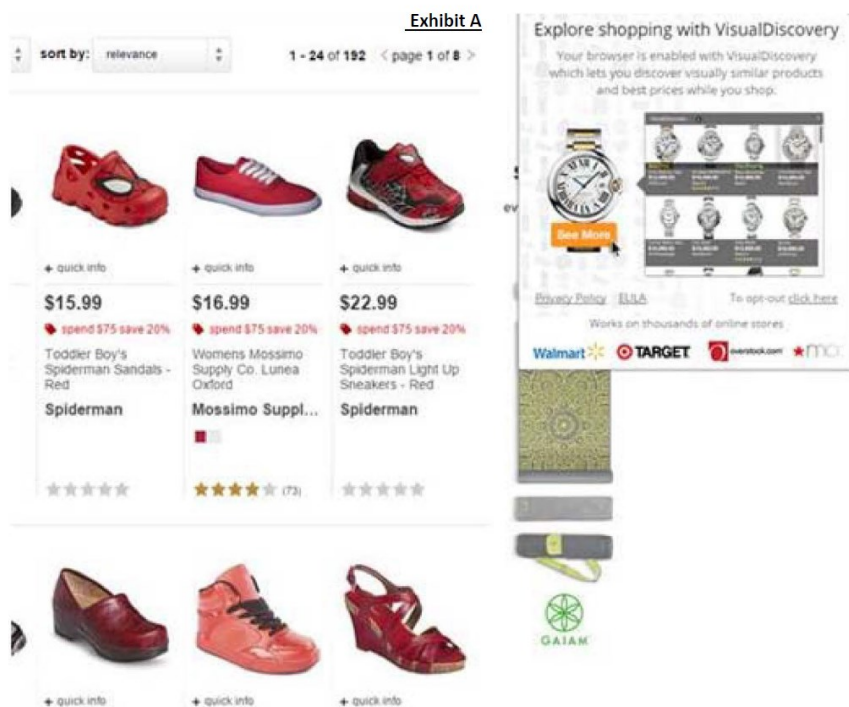
37. As alleged in Paragraphs 19-29, Respondent's failure to take reasonable measures to assess and address security risks created by third-party software preinstalled on its laptops, caused or is likely to cause substantial injury to consumers, that is not offset by countervailing benefits to consumers or competition, and is not reasonably avoidable by consumers. This practice was, and is, an unfair act or practice.

38. The acts and practices of Respondent as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

THEREFORE, the Federal Trade Commission this twentieth day of December, 2017, has issued this complaint against Respondent.

By the Commission.

Decision and Order

Exhibit A**DECISION AND ORDER**

The Federal Trade Commission (“Commission”) initiated an investigation of certain acts and practices of the Respondent named in the caption. The Commission’s Bureau of Consumer Protection (“BCP”) prepared and furnished to Respondent a draft Complaint. BCP proposed to present the draft Complaint to the Commission for its consideration. If issued by the Commission, the draft Complaint would charge the Respondent with violation of the Federal Trade Commission Act.

Respondent and BCP thereafter executed an Agreement Containing Consent Order (“Consent Agreement”). The Consent Agreement includes: 1) statement by Respondent that it neither

Decision and Order

admits nor denies any of the allegations in the Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, it admits the facts necessary to establish jurisdiction; and 2) waivers and other provisions as required by the Commission's Rules.

The Commission considered the matter and determined that it had reason to believe that Respondent has violated the Federal Trade Commission Act, and that a Complaint should issue stating its charges in that respect. The Commission accepted the executed Consent Agreement and placed it on the public record for a period of 30 days for the receipt and consideration of public comments. The Commission duly considered any comments received from interested persons pursuant to Section 2.34 of its Rules, 16 C.F.R. § 2.34. Now, in further conformity with the procedure prescribed in Rule 2.34, the Commission issues its Complaint, makes the following Findings, and issues the following Order:

Findings

1. The Respondent is a Delaware corporation, with its principal office or place of business located at 1009 Think Place, Morrisville, North Carolina 27560-9002.
2. The Commission has jurisdiction over the subject matter of this proceeding and over the Respondent, and the proceeding is in the public interest.

ORDER**Definitions**

For purposes of this Order, the following definitions apply:

- A. "Respondent" means Lenovo (United States) Inc., and its successors and assigns.
- B. "Affirmative express consent" means that:
 1. Prior to the initial operation of any covered software, it shall be clearly and conspicuously

Decision and Order

disclosed, separate and apart from any “end user license agreement,” “privacy policy,” “terms of use” page or similar document, the following:

- a. For any covered software that displays advertising,
 - i. the fact that the covered software will display advertisements, including any pop-up advertisements; and
 - ii. the frequency and circumstances under which such advertisements are displayed to the consumer; and
- b. For any covered software that transmits, or causes to be transmitted, covered information to a person or entity other than the consumer,
 - i. the fact that the software will transmit, or cause to be transmitted, the covered information to a person or entity other than the consumer;
 - ii. the types of covered information that will be transmitted to a person or entity other than the consumer;
 - iii. the types of covered information that the receiving person or entity will share with third parties, which does not include an entity with a common corporate ownership and branding of Respondent or the software provider, a third party service provider, or any person or entity otherwise excluded by the Proviso in Part II of this Order;
 - iv. the identity or specific categories of such third parties; and
 - v. the purposes for sharing such covered information.

Decision and Order

2. At the time this disclosure is made, a clear and conspicuous mechanism shall be provided for a consumer to indicate assent to the operation of the covered software by taking affirmative action authorizing its operation.
- C. “Application software” means any computer program designed for and used by consumers (*e.g.*, database programs, word processing programs, games, Internet browsers, or browser add-ons) that Respondent preinstalls or causes to be preinstalled onto a covered product. Application software does not include device drivers; system software designed to configure, optimize or maintain a computer; operating systems; software bundled, integrated or included with operating systems; or software otherwise provided to Respondent for preinstallation on a covered product by an operating system provider.
- D. “Clear(ly) and conspicuous(ly)” means that a required disclosure is difficult to miss (*i.e.*, easily noticeable) and easily understandable by ordinary consumers, including in all of the following ways:
1. In any communication that is solely visual or solely audible, the disclosure must be made through the same means through which the communication is presented. In any communication made through both visual and audible means, such as a television advertisement, the disclosure must be presented simultaneously in both the visual and audible portions of the communication even if the representation requiring the disclosure (“triggering representation”) is made through only one means.
 2. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.

Decision and Order

3. An audible disclosure, including by telephone or streaming video, must be delivered in a volume, speed, and cadence sufficient for ordinary consumers to easily hear and understand it.
 4. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable.
 5. On a product label, the disclosure must be presented on the principal display panel.
 6. The disclosure must use diction and syntax understandable to ordinary consumers and must appear in each language in which the triggering representation appears.
 7. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.
 8. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.
 9. When the representation or sales practice targets a specific audience, such as children, the elderly, or the terminally ill, “ordinary consumers” includes reasonable members of that group.
- E. “Covered information” means the following information from or about an individual consumer that is input into, stored on, accessed or transmitted through application software: (a) a first and last name; (b) a physical address; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) login credentials and passwords; (e) a telephone number; (f) a Social Security number; (g) a driver’s license or other government-issued identification number; (h) a financial institution account number; (i) credit or debit

Decision and Order

card information; (j) any portion of the content of a consumer's communications; (k) any portion of the content of a consumer's files (*e.g.*, documents, photos or videos); and (l) precise geolocation information sufficient to identify a street name and name of a city or town.

- F. "Covered product" means any personal computer (*i.e.*, desktop computers, laptops, laptops that convert into tablets or vice versa, and notebooks) that is manufactured by or on behalf of Respondent and is sold to U.S. consumers. Covered products do not include servers and server peripherals, mobile handsets or smartphones, or tablets or similar devices that are sold without an integrated or detachable physical keyboard. Covered products also do not include the actual personal computers specifically sold to enterprise customers with over 1,000 employees.
- G. "Covered software" means:
1. Application software that injects advertisements into a consumer's Internet browsing session, including pop-up advertisements; or
 2. Application software that transmits, or causes to be transmitted, covered information to a person or entity other than the consumer, except when
 - a. the covered information is used only in an aggregated and/or de-identified form that does not disclose, report, or otherwise share any individually identifiable information; or
 - b. the covered information is transmitted or used solely for one or more of the following purposes:
 - i. being reasonably necessary for the software to perform a function or service that the consumer requests or otherwise interacts with;

Decision and Order

- ii. authenticating the consumer;
- iii. configuring or setting up the software; or
- iv. assessing or analyzing the software's performance (*e.g.*, to find or fix problems in the software, assess how consumers are using the software, or to make improvements to the software).

Covered software does not include Internet browsers, antivirus software, parental control software, or other computer security software.

- H. "Feature" means one or more of the following attributes of covered software: (a) the covered software's benefits, efficacy, or features; (b) the fact that it will display advertising, including pop-up advertisements; (c) the frequency and circumstances under which the covered software will display advertising; and (d) the fact of and extent to which the covered software will transmit, or cause to be transmitted, covered information to a person or entity other than the consumer.
- I. "Software provider" means any person or entity other than Respondent that sells, leases, licenses, or otherwise provides application software.
- J. "Third party service provider" means any person or entity that is contractually required by Respondent or a software provider to: (a) use or receive covered information collected by or on behalf of Respondent or the software provider for and at the direction of Respondent or the software provider, and for no other individual or entity; (b) not disclose the covered information, or any individually identifiable information derived from it, to any individual or entity other than Respondent or the software provider; and (c) not use the covered information for any other purpose.

Decision and Order

I. Prohibited Misleading Representations

IT IS ORDERED that Respondent, its officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with the advertising, promotion, offering for sale, sale, or distribution of covered software shall not make a misrepresentation, in any manner, expressly or by implication, about any feature of the covered software.

II. Affirmative Express Consent Provision

IT IS FURTHER ORDERED that, commencing no later than 120 days after the date of service of this Order, Respondent, its officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, shall not preinstall or cause to be preinstalled any covered software unless Respondent or the software provider:

- A. will obtain the consumer's affirmative express consent;
- B. provides instructions for how the consumer may revoke consent to the covered software's operation, which can include uninstalling the covered software; and
- C. provides a reasonable and effective means for consumers to opt out, disable or remove all of the covered software's operations, which can include uninstalling the covered software.

Provided, however, that affirmative express consent will not be required if sharing the covered information is reasonably necessary to comply with applicable law, regulation or legal process.

Decision and Order

III. Mandated Software Security Program

IT IS FURTHER ORDERED that Respondent must, no later than the date of service of this Order, establish and implement, and thereafter maintain a comprehensive software security program that is reasonably designed to (1) address software security risks related to the development and management of new and existing application software, and (2) protect the security, confidentiality, and integrity of covered information. The content, implementation and maintenance of the software security program must be fully documented in writing. The software security program must contain administrative, technical, and physical safeguards appropriate to Respondent's size and complexity, the nature and scope of Respondent's activities, the nature of the application software, the security policies and practices of the software provider, and the sensitivity of the covered information, including:

- A. the designation of an employee or employees to coordinate and be responsible for the software security program;
- B. the identification of internal and external risks to the security, confidentiality, or integrity of covered information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment must include consideration of risks in each area of relevant operation, including: (1) employee training and management; (2) application software design, including the processing, storage, transmission and disposal of covered information by the application software; and (3) the prevention, detection, and response to attacks, intrusions, or other vulnerabilities;
- C. the design and implementation of reasonable safeguards to control these risks, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;

Decision and Order

- D. the development and use of reasonable steps to select and retain software or service providers capable of maintaining security practices consistent with this Order, and requiring software and service providers, by contract, to implement and maintain appropriate safeguards; and
- E. the evaluation and adjustment of the software security program in light of the results of the testing and monitoring required by sub-provision C, any changes to Respondent's operations or business arrangements, or any other circumstances that Respondent knows or has reason to know may have an impact on the effectiveness of the software security program.

IV. Software Security Assessments by a Third Party

IT IS FURTHER ORDERED that, in connection with compliance with the Provision of this Order titled Mandated Software Security Program, Respondent must obtain initial and biennial assessments ("Assessments"):

- A. The Assessments must be obtained from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. A professional qualified to prepare such Assessments must be a person qualified as a Certified Secure Software Lifecycle Professional (CSSLP) with professional experience with secure Internet-accessible, consumer-grade devices; an individual qualified as a Certified Information Systems Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA) with professional experience with secure Internet-accessible consumer-grade devices; or a qualified individual or entity approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission.
- B. The reporting period for the Assessments must cover: (1) the first 180 days after the issuance date of the Order for the initial Assessment, and (2) each 2-year

Decision and Order

period thereafter for 20 years after issuance of the Order for the biennial Assessments.

- C. Each Assessment must:
1. set forth the specific administrative, technical, and physical safeguards that Respondent has implemented and maintained during the reporting period;
 2. explain how such safeguards are appropriate to Respondent's size and complexity, the nature and scope of Respondent's activities, the nature of the application software, the security policies and practices of the application software provider, and the sensitivity of the covered information;
 3. explain how the safeguards that have been implemented meet or exceed the protections required by the Provision of this Order titled Mandated Software Security Program; and
 4. certify that the Mandated Software Security Program is operating with sufficient effectiveness to provide reasonable assurance that the security of the application software preinstalled on covered products and the security, confidentiality, and integrity of covered information is protected, and that the Mandated Software Security Program has so operated throughout the reporting period.
- D. Each Assessment must be completed within 60 days after the end of the reporting period to which the Assessment applies. Respondent must submit the initial Assessment to the Commission within 10 days after the Assessment has been completed. Respondent must retain all subsequent biennial Assessments, at least until the Order terminates. Respondent must submit any biennial Assessments to the Commission within 10 days of a request from a representative of the Commission.

Decision and Order

V. Acknowledgments of the Order

IT IS FURTHER ORDERED that Respondent obtain acknowledgments of receipt of this Order:

- A. Respondent, within 10 days after the effective date of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.
- B. For 5 years after the issuance date of this Order, Respondent must deliver a copy of this Order to: (1) all principals, officers, and directors; (2) all employees, agents, and representatives with managerial responsibilities related to the subject matter of the Order; and (3) any business entity resulting from any change in structure as set forth in the Provision titled Compliance Report and Notices. Delivery must occur within 10 days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.

VI. Compliance Report and Notices

IT IS FURTHER ORDERED that Respondent makes timely submissions to the Commission:

- A. One year after the issuance date of this Order, Respondent must submit a compliance report, sworn under penalty of perjury, in which Respondent must: (a) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission, may use to communicate with Respondent; (b) identify all of Respondent's business entities by all of their names; (c) describe the activities of each business, including the goods and services offered; (d) describe in detail whether and how Respondent is in compliance with each Provision of this Order, including a discussion of all of the costs incurred and changes made by the Respondent to comply with the

Decision and Order

Order; and (e) provide a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.

- B. Respondent must submit a compliance notice, sworn under penalty of perjury, within 14 days of any change in the following: (a) any designated point of contact; or (b) the structure of Respondent or any entity that Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.
- C. Respondent must submit notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against such Respondent within 14 days of its filing.
- D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: “I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____,” and supplying the date, signatory’s full name, title (if applicable), and signature.
- E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: *In re Lenovo (United States) Inc.*

Decision and Order

VII. Recordkeeping

IT IS FURTHER ORDERED that Respondent must create certain records for 20 years after the issuance date of the Order, and retain each such record for 5 years, unless otherwise specified below. Specifically, Respondent must create and retain the following records:

- A. accounting records showing the revenues from all covered products sold, the costs incurred in generating those revenues, and resulting net profit or loss;
- B. personnel records showing, for each person who must receive a copy of this Order pursuant to Part V.B., that person's: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;
- C. copies or records of all U.S. consumer complaints relating to covered software or the security of application software, whether received directly or indirectly, such as through a third party, and any response;
- D. a copy of each representation subject to this Order;
- E. for 5 years after the date of preparation of each Assessment required by this Order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of Respondent, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning Respondent's compliance with related Provisions of this Order, for the compliance period covered by such Assessment; and
- F. all records necessary to demonstrate full compliance with each provision of this Order, including all submissions to the Commission.

Decision and Order

VIII. Compliance Monitoring

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondent's compliance with this Order:

- A. Within 10 days of receipt of a written request from a representative of the Commission, Respondent must submit additional compliance reports or other requested information, which must be sworn under penalty of perjury, and produce records for inspection and copying.
- B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with Respondent. Respondent must permit representatives of the Commission to interview anyone affiliated with any Respondent who has agreed to such an interview. The interviewee may have counsel present.
- C. The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondent or any individual or entity affiliated with Respondent, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

IX. Order Effective Dates

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order. This Order will terminate on December 20, 2037, or 20 years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

Concurring Statement

- A. any Provision in this Order that terminates in less than 20 years;
- B. this Order's application to any Respondent that is not named as a defendant in such complaint; and
- C. this Order if such complaint is filed after the Order has terminated pursuant to this Provision.

Provided, further, that if such complaint is dismissed or a federal court rules that the Respondent did not violate any provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

**Statement of Acting Chairman Maureen K. Ohlhausen
In the Matter of Lenovo, Inc.
September 5, 2017**

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”).

Concurring Statement

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 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,”

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”).

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.*

Concurring Statement

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-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

⁶ *Id.* at 1058-59.

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).

Concurring Statement

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. 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 McSweeney 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 McSweeney's argument as framed.

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

Concurring Statement

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.

Concurring and Dissenting Statement

**Statement of Commissioner Terrell McSweeney
In the Matter of Lenovo, Inc.
September 5, 2017**

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

Analysis to Aid Public Comment

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.

**ANALYSIS OF 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.

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).

Analysis to Aid Public Comment

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'

Analysis to Aid Public Comment

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;

Analysis to Aid Public Comment

- 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.

Analysis to Aid Public Comment

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

Analysis to Aid Public Comment

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.

Complaint

IN THE MATTER OF

**INTEGRA LIFESCIENCES HOLDINGS
CORPORATION**

AND

JOHNSON & JOHNSONCONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF
SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT AND
SECTION 7 OF THE CLAYTON ACT*Docket No. C-4624; File No. 171 0084**Complaint, September 26, 2017 – Decision, December 21, 2017*

This consent order addresses the \$1 billion acquisition by Integra LifeSciences Holdings Corporation of certain assets of Johnson & Johnson's Codman Neuro division. The complaint alleges that the acquisition, if consummated, would violate Section 7 of the Clayton Act and Section 5 of the Federal Trade Commission Act by substantially lessening competition in the U.S. markets for intracranial pressure monitoring systems, cerebrospinal fluid collection systems, non-antimicrobial external ventricular drainage catheters, fixed pressure valve shunt systems, and dural grafts. The consent order requires the parties to divest all rights and assets to Natus Medical Incorporated related to Integra's intracranial pressure monitoring systems and fixed pressure valve shunt systems, as well as Codman's cerebrospinal fluid collection systems, non-antimicrobial external ventricular drainage catheters, and dural grafts.

Participants

For the *Commission*: Anne R. Schenof, Danielle Sims, Aylin M. Skroejer and David Von Nirschl.

For the *Respondents*: Jessica Bratten, Patrick English, Amanda Reeves and E. Marcellus Williamson, Latham & Watkins LLP; Jonathan Cheng, Kristin Sanford and Laura Wilkinson, Weil, Gotshal & Manges LLP.

COMPLAINT

Pursuant to the Clayton Act and the Federal Trade Commission Act ("FTC Act"), and its authority thereunder, the Federal Trade Commission ("Commission"), having reason to believe that Respondent Integra LifeSciences Holdings Corporation ("Integra"), a corporation subject to the jurisdiction