Alexander M. Schack, Esq., Bar No. 99126
Natasha A. Naraghi, Esq., Bar No. 284711
LAW OFFICES OF ALEXANDER M. SCHACK
16870 West Bernardo Drive, Suite 400
San Diego, CA 92127
Tel: (858) 485-6535 Fax: (858) 485-0608
alexschack@amslawoffice.com
natashanaraghi@amslawoffice.com

Geoffrey J. Spreter, Esq., Bar No 257707
SPRETER LEGAL SERVICES, APC
601 3rd Street
Coronado, CA 92118
Telephone: 619-865-7986
spreterlegalservices@gmail.com

E. Elliot Adler, Esq., Bar No. 229030
ADLER LAW GROUP, APLC
402 W. Broadway, Suite 860
San Diego, CA 92101
Tel: (619) 531-8700 Fax: (619) 342-9600
elliotadler@gmail.com

Attorneys for Plaintiff, individually and on behalf of all others similarly situated

UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF SOUTHERN CALIFORNIA

JESSICA N. BENNETT, individually and on behalf of all others similarly situated, Plaintiff, v. LENOVO (UNITED STATES), INC., and SUPERFISH, INC.,	Case No. '15CV0368 CAB RBB **CLASS ACTION** COMPLAINT FOR: 1) VIOLATION OF CALIFORNIA PENAL CODE §§631 and 637.2 2) VIOLATION OF FEDERAL WIRETAP ACT TITLE I OF THE ECPA (18 U.S.C. §2510, *et seq.)* 3) TRESSPASS TO PERSONAL

Defendants.	4) PROPERTY/CHATTELS-CALIFORNIA COMMON LAW VIOLATIONS OF CALIFORNIA'S UNFAIR COMPETITION LAW (Cal. Bus. & Prof. Code §§17200, *et seq.)* DEMAND FOR JURY TRIAL

Plaintiff, Jessica N. Bennett, individually, and on behalf of all persons similarly situated ("Class Members"), by and through her attorneys, for her complaint against Defendants Lenovo, Inc. and Superfish, Inc. ("Defendants"), states and alleges as follows:

INTRODUCTION

1. Defendants have unlawfully used and damaged Plaintiff's computer to make money for themselves, while willfully disregarding Plaintiff's rights to use and enjoy her personal property.

2. Defendants sold new computers with harmful and offensive spyware and/or malware (hereinafter referred to singularly as "Spyware"). The Spyware tracked Plaintiff's Internet use, invaded her privacy, and damaged her computer. Relying on Spyware as the key to getting inside Plaintiff's computer and learning her Internet browsing habits, Defendants invaded Plaintiff's privacy and interfered with Plaintiff's right to use and enjoy her computer. Defendants' misconduct also

substantially diminished the value of her property. The putative classes in this case have been violated and damaged in the same ways.

PARTIES

3. Plaintiff Jessica N. Bennett is a California citizen who resides in San Diego County, California.

4. Defendant Lenovo (United States), Inc., ("Lenovo") is a Delaware Corporation with its headquarters and principal place of business in Morrisville, North Carolina. Lenovo is the United States operating subsidiary of Lenovo Group Limited, a Hong Kong corporation with its principal place of business in Beijing, China. Lenovo Group Limited is a multinational computer technology company, which, through its subsidiaries including Lenovo, designs, develops, manufacturers and sells personal computers, tablet computers, smartphones, workstations, servers, electronic storage devices and smart televisions. Lenovo collected more than $38.7 billion in revenue for its most recent fiscal year; Lenovo's laptop business accounts for approximately half of Lenovo's overall revenue.

5. Defendant Superfish, Inc. ("Superfish") is a Delaware Corporation with its principal place of business in Palo Alto, California.

6. Plaintiff is informed and believes and based thereon alleges that at all relevant times each of the Defendants was the agent, servant, employee, subsidiary, affiliate, partner, assignee, successor-in-interest, alter ego, joint venturer, and/or other

representative of each of the remaining Defendants and was acting in such capacity in doing the things herein alleged.

JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction over all claims in this action pursuant to the Class Action Fairness Act, 28 USC § 1332(d)(2), the amount in controversy exceeds $5 million, and the proposed class includes in excess of 100 members.

8. This Court also has subject matter jurisdiction over the federal claims in this action pursuant to 28 USC § 1331.

9. This Court also has subject matter jurisdiction over the state law claims in this action pursuant to 28 USC § 1367(a) because they are so related to the federal claims that they form part of the same case or controversy under Article III of the U.S. Constitution.

10. Additionally, Defendants purposefully avail themselves of the jurisdiction of this Court, through their promotion, marketing, and sale of their products in the State of California, and through significant and pervasive contacts with the State of California sufficient to render the exercise of jurisdiction by this Court in a manner that appropriately applies traditional notions of fair play and substantial justice.

11. Venue is proper in this District under 28 U.S.C. § 1391 because Defendants conduct business in this District. Furthermore, a substantial portion of the events giving rise to Plaintiff's claims arose here.

FACTUAL BACKGROUND

12. Plaintiff purchased a Lenovo Yoga 2 laptop for use in her business as a blog writer in late 2014. Plaintiff used the laptop to correspond with clients.

13. Shortly after purchase, Plaintiff Bennett noticed pop ups on her computer. Plaintiff was writing a blog post for a client when she noticed spam advertisements involving scantily clad women appearing on her client's website. Plaintiff looked at a couple of other sites and did not see any advertisements, so she assumed the client's website was the problem. She sent an email to her client suggesting that their site had been hacked.

14. A few hours later, Plaintiff was doing research for a different client when she saw the same block of advertisements intruding on a different, very well-known site. It was then that Plaintiff knew that her computer was infected with Spyware. Plaintiff became extremely distressed that her new laptop contained Spyware and thought that it may have been hacked.

15. Plaintiff searched web forums for help on removing the malicious Spyware on her computer and learned that numerous other consumers were experiencing similar problems with the Superfish product on their recently purchased

Lenovo laptop. It was only after further research did Plaintiff learn that the Lenovo laptops came preinstalled with the Superfish Spyware.

16. One Lenovo user, for example, posted on the Lenovo message board (http://forums.lenovo.com/t5/Yoga-Flex-Laptops-and/Pre-installed-Superfish-Visual-Discovery-on-Lenovo-Flex-2-15/td-p/1896989:

> "While setting up a Lenovo Flex 2-15 and uninstalling some of the unwanted software, I came across the Superfish Visual Discovery software.
>
> After doing some research into Superfish Visual Discovery, I consider this software to be quite invasive. It sits between you and whatever sites you visit to monitor your sessions and extract information (it says photos) to serve you advertisements for similar products you may be looking for. What's even more concerning is that it does this for HTTPS connections that the user would expect to be private between themselves and the server they *believe* they are securely connecting to.
>
> I "uninstalled" it via the "Programs and Features" in Windows 8.1, however I noticed that there are still remnants of the Superfish software left behind.
>
> - There are Superfish root certificates left behind.
> - There are Superfish registry entries left behind, some of them relating to SuperfishIEAddon.dll (which there appears to be no add-ons for Superfish in IE for me, but I would like to be sure), and other related registry entries.
> - Possibly other remnants of the software I have not seen?
>
> I have spoken on two separate occasions with Lenovo phone support, both times they insisted that this Superfish software was not installed by Lenovo and that it is malicious and should be removed, at which time they offered to charge me either a one-time fee of $120, or sell me a monthly software support subscription. I insisted that this Superfish software came pre-installed from the factory, citing where it said "Install Date" in the "Programs and Features" (which was the same install date as the rest of the Lenovo software), as well as the registry entry where Superfish is listed under the "MFGApps" string value. Also, I told them about the folder "Program Files\Lenovo\VisualDiscovery" (if I remember the path name correctly) which used to exist, but I was told this

was the virus trying to implant itself somewhere.

I find it surprising that the Lenovo software support reps were not aware that Lenovo included Superfish with their laptops.

I and most likely others would appreciate that Lenovo provide a removal tool to *COMPLETELY* remove this Superfish software (and any remnants that remain for those who have already uninstalled it, like myself) i.e. ALL of it's associated files, registry entries, ie add-ons, firefox extensions, chrome extensions, etc. , and provide any other direction as necessary."

17. On February 19, 2015, Reuters published an article addressing Lenovo's installation of the Superfish Spyware on its computers (http://finance.Defendants. com /news /lenovo-stop-pre-installing-controversial-152140699.html).

18. In the article, several security experts are quoted concerning the potential security threats that users of Lenovo computers incurred and will continue to incur:

"Robert Graham, CEO of U.S.-based security research firm Errata Security, said Superfish was malicious software that hijacks and throws open encrypted connections, paving the way for hackers to also commandeer these connections and eavesdrop, in what is known as a man-in-the-middle attack."

"Graham and other experts said Lenovo was negligent, and that computers could still be vulnerable even after uninstalling Superfish. The software throws open encryptions by giving itself authority to take over connections and declare them as trusted and secure, even when they are not."

"The way the Superfish functionality appears to work means that they must be intercepting traffic in order to insert the ads," said Eric Rand, a researcher at Brown Hat Security. "This amounts to a wiretap."

19. In a blog post by Marc Rogers, a security expert with extensive knowledge of computer security features, Mr. Rogers discusses how the Superfish

compromises a consumers' personal information and security.

(http://marcrogers.org/2015/02/19/lenovo-installs-adware-on-customer-laptops-and-compromises-all-ssl/:)

"Superfish Features:

- Hijacks legitimate connections.
- Monitors user activity.
- Collects personal information and uploads it to its servers
- Injects advertising in legitimate pages.
- Displays popups with advertising software
- Uses man-in-the-middle attack techniques to crack open secure connections.
- Presents users with its own fake certificate instead of the legitimate site's certificate.

This presents a security nightmare for affected consumers.

1. Superfish replaces legitimate site certificates with its own in order to compromise the connections so it can inject its adverts. This means that anyone affected by this adware cannot trust any secure connections they make

2. Users will not be notified if the legitimate site's certificate has been tampered with, has expired or is bogus. In fact, they now have to rely on Superfish to perform that check for them. Which it does not appear to do.

3. Because Superfish uses the same certificate for every site it would be easy for another hostile actor to leverage this and further compromise the user's connections.

4. Superfish uses a deprecated SHA1 certificate. SHA1 has been replaced by SHA-256 because attacks against SHA1 are now feasible with ordinary computing hardware. This is insult on top of injury. Not only are they compromising people's SSL connections but they are doing it in the most cavalier, insecure way possible.

5. Even worse, they use crackable 1024-bit RSA!

6. The user has to trust that this software which has compromised their secure connections is not tampering with the content, or stealing sensitive data such as usernames and passwords.

7. If this software or any of its control infrastructure is compromised, an attacker would have complete and unrestricted access to affected customers banking sites, personal data and private messages."

20. Mr. Rogers goes on to demonstrate how the Superfish Spyware creates fake security certificates for websites, which would compromise the security of the computer.

21. Defendants' Spyware causes computers to slow down, takes up bandwidth over an Internet connection, uses up memory on a computer, causes the loss of data, compromises computer security features and frustrates computer users. Defendants' Spyware and popup advertisements decrease productivity by requiring that hours be spent figuring out how to get them off of a computer, closing advertising windows, and waiting for a slower machine to operate. Furthermore, computer users are forced to keep their computers running longer (due to the slowed performance) which utilizes more electricity, decreases the useful life of a computer, and causes increased Internet access charges. The cumulative impact of not only multiple ads, but also the threat of future ads and monitoring, impedes computer usage.

22. As detailed herein, Defendants' installation of Superfish on Plaintiff's computer and the interception of confidential information violated several federal and state laws concerning computer privacy.

CLASS ACTION ALLEGATIONS

23. Plaintiff brings this action, individually and on behalf all others similarly situated pursuant to Federal Rule of Civil Procedure 23, and seeks certification for the following National Class and California Subclass (collectively, "Class")

National Class: All purchasers of a Lenovo computer in the United States who purchased a computer with the Superfish program preinstalled on it during the period January 1, 2012 to the present.

California Sub-Class: All purchasers of a Lenovo computer in the State of California who purchased a computer with the Superfish program preinstalled on it during the period January 1, 2012 to the present.

24. Excluded from the proposed Class are Lenovo (United States), Inc., its parents, subsidiaries, affiliates and controlled persons, as well as the officers and directors (and their immediate family) of Lenovo (United States), Inc., its parents, subsidiaries, affiliates and controlled persons. Also excluded from the proposed Class are Superfish, Inc., its parents, subsidiaries, affiliates and controlled persons, as well as the officers and directors (and their immediate family) of Superfish, Inc., its

parents, subsidiaries, affiliates and controlled persons. Also excluded is any judicial officer assigned to this case.

25. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure 23:

Numerosity. The members of the Class are so numerous that joinder of all members is impracticable. While the exact number of Class Members is unknown to Plaintiff at the present time and can only be ascertained through appropriate discovery, Plaintiff believes that there are in excess of one million members of the Class located throughout the United States. It would be impracticable to join the Class Members individually.

Existence and predominance of common questions of law. Common questions of law and fact exist as to all members of the Class and predominate over any questions solely affecting individual members of the Class. Among the many questions of law and fact common to the Class are:

a) Whether Defendants' conduct violates the California Invasion of Privacy Act.

b) Whether Defendants' conduct violates the Electronic Communications Privacy Act.

c) Whether Plaintiff and the Class Members are entitled to statutory damages under the California Invasion of Privacy Act and the Electronic Communications Privacy Act.

d) Whether Defendants committed a trespass to chattels.

e) Whether Defendants' conduct violates California's Unfair Competition law.

Typicality. Plaintiff's claims are typical of the claims of the members of the Class. Plaintiff and all members of the Class have been harmed by Defendants' unlawful activities alleged herein and are entitled to identical statutory damages.

Adequacy. Plaintiff will adequately represent the proposed Class Members. They have retained counsel competent and experienced in class actions to pursue this action vigorously. Plaintiff has no interests contrary to or in conflict with the interests of Class Members.

Superiority. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. Plaintiff knows of no difficulty to be encountered in the management of this action that would preclude its maintenance as a class action.

COUNT ONE
VIOLATION OF CALIFORNIA PENAL CODE §§ 631 and 637.2
CALIFORNIA INVASION OF PRIVACY ACT ("CIPA")
(Against All Defendants)

26. Plaintiff incorporates each and every allegation above as if fully set forth herein.

27. California Penal Code § 631(a) makes it unlawful, by means of any machine, instrument or contrivance, to purposefully intercept the content of a communication over any "telegraph or telephone wire, line, cable or instrument," or to read or attempt to read or learn the content of any such communications without the consent of all parties to the communication.

28. Plaintiff's internet searches and communications with websites and third parties are communications within the meaning of Section 631.

29. Defendants intercepted the communications to and from Class Members using Spyware and servers that qualify as machines, instruments or contrivances as defined by the CIPA.

30. Plaintiff and Class Members did not consent to Defendants' interception of their internet searches and private communications.

31. Defendants are not a party to the communications with Plaintiff and Class Members.

32. Defendants are "persons" within the meaning of the CIPA. Plaintiff and Class Members were and are injured by Defendants' unlawful interception of their internet searches and communications.

33. Defendants knowingly and willfully intercepted Plaintiff's and Class Members' internet communications while they were "in transit."

34. Defendants' conduct in violation of the CIPA occurred in the State of California because those acts resulted from business decisions, practices and operating policies that Defendants developed, implemented and/or utilized in California which are unlawful and constitute criminal conduct in Defendant Superfish's state of residence and principal place of business. Defendants also profited from their conduct in the State of California.

35. As a result of Defendants' violations of Section 631, Plaintiff and Class Members are entitled to relief under Section 637.2, including:

(i) Appropriate declaratory relief;

(ii) Statutory damages of $5,000 per class member; and

(iii) Reasonable attorneys' fees.

COUNT TWO
VIOLATION OF THE FEDERAL WIRETAP ACT
TITLE I OF THE ECPA (18 U.S.C. § 2510 *et seq.*)
(Against All Defendants)

36. Plaintiff incorporates each and every allegation above as if fully set forth herein.

37. The ECPA provides a private right of action against one who "intentionally intercepts, endeavors to intercept, or procures any other person to

intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C.A. § 2511 and 2520.

38. Defendants intentionally and without consent intercepted Plaintiff's and Class Members' communications with Internet sites and search engines for tortious purposes, specifically to spy on their private Internet browsing use and to trespass on their computer. At this time, Defendants intentionally accessed the Spyware that it had placed on these computers. Defendants also intentionally used its Spyware to intercept communications by Plaintiff and Class Members to Internet sites.

39. Defendants further disclosed to others the content of electronic communications knowing that the communications were unlawfully obtained.

40. Defendants collected Plaintiff's personal information and the personal information of Class Members without consent or compensation, and to misappropriate personality, thereby obtaining detailed, free market research and consumer analysis rather than paying for it.

41. Pursuant to 18 U.S.C. § 2520(a), Plaintiff and Class Members are entitled to:

(i) statutory damages of $100 per day per violation per class member, up to $10,000 per class member;

(ii) costs; and

(iii) reasonable attorneys' fees.

COUNT THREE
TRESSPASS TO PERSONAL PROPERTY/CHATTELS-CALIFORNIA COMMON LAW
(Against All Defendants)

42. At all times relevant hereto, Plaintiff and Class Members were the owners of computers on which Defendants installed and operated malicious Spyware.

43. At all relevant times, Defendants and/or their agents intentionally and without consent, used Plaintiff's computer and the computers of the Class Members, gained access to their computers, monitored their Internet usage, sent advertisements to these infected computers, accessed various components and systems within these computers, obtained access to information about Plaintiff and Class Members and their computers, took up space on these computers, and/or dispossessed Plaintiff and Class Members of access to their computers.

44. The installation and operation of the spyware on Plaintiff's and Class Members' computers impairs the condition and the value of Plaintiff and Class Members' computers

45. In doing so, Defendants intentionally intermeddled with, damaged, and deprived Plaintiff and Class Members of their computers' full use and benefits.

46. As a proximate result of Defendants' installation and operation of the Spyware on computers of Plaintiff and Class Members, Plaintiff and the Class Members suffered harm.

COUNT FOUR
Violations Of California's Unfair Competition Law
(Cal. Bus. & Prof. Code §§ 17200 et seq.)
(Against All Defendants)
(Brought On Behalf Of The California Subclass)

47. Plaintiff adopts and incorporates each and every allegation of this complaint as if stated fully herein.

48. The California Business and Professions Code § 17200 et seq., the Unfair Competition Law ("UCL") defines unfair competition to include any unlawful, unfair, or fraudulent business act or practice. Unlawful, unfair, or fraudulent business acts are those which are in violation of federal, state, county, or municipal statutes, as well as regulations. The UCL provides for injunctive relief and restitution for violations. Cal. Bus. & Prof. Code § 17203.

49. Defendants' conduct as alleged herein constitutes unlawful, unfair, and fraudulent business acts and practices. As a proximate result of Defendants' unlawful installation and operation of the spyware on the computers of Plaintiff and the Class Members, Plaintiff and Class Members suffered harm and lost money and/or property.

50. By engaging in the above described acts and practices, Defendants have committed one or more acts of unfair competition within the meaning of the UCL.

51. Defendants' business practices and acts are "fraudulent" because they are likely to deceive, and did deceive Plaintiff and members of the consuming public.

Specifically, Defendants intentionally and misleadingly sold new computers with preinstalled Spyware.

52. Defendants' conduct as alleged herein constitutes unfair and unlawful business acts or practices as proscribed by Section 17200, et seq., of the California Business & Professions Code ("UCL").

53. Defendants' conduct – the installation and operation of Spyware on Plaintiff's and Class Members' computers and/or the unauthorized access of Plaintiff's and Class Members' computers resulting in damages and loss to Plaintiff and Class Members – constitutes "unlawful" business acts or practices by virtue of Defendants' violation of the 18 U.S.C.A. 2511, California Business and Professions Code Sections 22947.2, 22947.3, 22947.4, and California Penal Code §502.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

(a) That the Court enter an order certifying the class, appointing Plaintiff as representative of the class, and appointing Plaintiff's counsel as class counsel;

(b) That the Court enter judgment against Defendants for the causes of action alleged against it;

(c) That Plaintiff be awarded statutory damages as provided by California and federal law, plus interest, as well as litigation costs reasonably incurred and attorneys' fees;

(d) That the Court order the disgorgement of all revenues unjustly earned by Defendants for selling new computers with preinstalled Spyware;

JURY DEMAND

Plaintiff, individually and for the Class she seeks to represent, demand trial by jury on each and every triable issue.

Date: February 19, 2015

Respectfully submitted,

/s/ Natasha A. Naraghi
Natasha A. Naraghi, Esq.
LAW OFFICES OF ALEXANDER M. SCHACK
16870 W. Bernardo Drive, #400
San Diego, CA 92128
(858) 485-6535 (858) 485-0608 fax
natashanaraghi@amslawoffice.com

/s/ Geoffrey J. Spreter
Geoffrey J. Spreter, Esq.
SPRETER LEGAL SERVICES, APC
601 3rd Street
Coronado, CA 92118
Telephone: 619-865-7986
spreterlegalservices@gmail.com