10 CIV 9183

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----------X

SONAL BOSE, Individually,
on Behalf of Herself and All Others
Similarly Situated,

Plaintiffs,

v.

INTERCLICK, INC.,
a Delaware Corporation,

Defendant.

----------X

Civil Action No.

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff, individually and on behalf of all others similarly situated, alleges as follows upon personal knowledge as to her own acts and observations and, otherwise, upon information and belief based on investigation of counsel.

NATURE OF THE CASE

1. In this complaint, Plaintiff alleges that Defendant Interclick, a web ad-serving company, monitored her web browsing in ways she would not expect or detect.

2. In particular, to circumvent measures Plaintiff took to prevent just such monitoring, Interclick served online advertisements that included hidden code to "sniff" Plaintiff's browser history and to deposit Adobe Flash local shared objects on her computer to monitor her online activities on an ongoing basis.

3. Plaintiff alleges that Interclick invaded her privacy, misappropriated her personal information, and interfered with the operability of her computer—conduct and consequences for which she now seeks relief.

PARTIES

4. Plaintiff is a resident of the City, County, and State of New York.

5. Defendant interCLICK, Inc. ("Interclick" or "Defendant") operates an online advertising network. Interclick is a publicly traded Delaware Corporation with corporate headquarters at 257 Park Avenue South, Sixth Floor, New York, New York 10010.

JURISDICTION AND VENUE

6. This Court has subject-matter jurisdiction over this action pursuant to Title 28, United States Code, Section 1331.

7. Venue is proper in this District under Title 28, United States Code, Section 1391(b) because defendant Interclick is a corporation headquartered in the City and State of New York.

8. In addition, venue is proper in this District under Title 28, United States Code, Section 1391(b) because Defendant's improper conduct alleged in this complaint occurred in, was directed from, and/or emanated from this judicial district.

FACTUAL ALLEGATIONS

A. Interclick's Business

9. Interclick earns its revenue from advertiser (or ad agency) clients that pay Interclick to display their advertisements on web pages.

10. For the month of December 2009, comScore Media Metrix ranked Interclick 10th among U.S. Internet ad networks, with an audience of approximately 149 million unique users, over 72 percent of the total Internet audience that month.

11. When a consumer visits a web page that includes a third-party advertisement, the display of the advertisement occurs because the web page causes the consumer to communicate with the ad network's systems; thus, Interclick's "audience" consists of consumers who visited websites on which Interclick displayed its clients' advertisements, not consumers who chose to communicate with Interclick or necessarily knew of Interclick's existence.

12. Interclick delivers its clients' advertisement on an ad network consisting of web-sites, or "publishers," which Interclick pays for their inventory. "Inventory" is advertising display space on a web pages.

13. The inventory Interclick purchases from websites is remnant inventory, also called "non-premium" inventory. After websites sell their premium inventory—which they typically sell directly to advertisers, with guarantees regarding factors such as ad placement, times of day, and volume of traffic—the remaining, unsold inventory is remnant inventory.

14. For premium inventory, advertisers typically pay based on CPMs (cost per thousand ad views).

15. For delivering their ads on remnant inventory, advertisers pay Interclick performance-based fees.

16. Performance-based fees vary based on how the consumer viewing an ad responds, for example, by mousing over the ad, clicking on it, or clicking through to complete a purchase transaction.

B. Interclick's Flash LSO Exploit

17. Because Interclick's derives its revenue primarily from performance-based fees, Interclick tries to maximize "return on ad spend" by engaging in behavioral targeting.

18. Like many online, third-party services, Interclick tracks consumers by depositing and reading browser cookies containing unique identifiers and browsing history information that it uses to create behavioral profiles; when a profiled consumer visits a web page on which Interclick serves advertisements, Interclick uses the profile to select particular categories of ads with which to target the user.

19. A consumer who does not want to be tracked by third parties such as Interclick can set her browser controls to block third-party cookies. For example, in Safari, this control is accessed as follows:

> *Safari > Preferences > Security > Accept cookies: Only from sites I visit / Block cookies from third parties and advertisers*

20. In addition, a consumer can delete browser cookies previously stored by third parties to attempt to prevent the third party from associating previously acquired tracking data with the consumer's subsequent web activity.

21. Mechanisms to block and delete third-party cookies are generally available to consumers using commercial browsers.

22. Interclick augmented its tracking technology by using tracking mechanisms that users could not reasonably block or delete: Interclick stored tracking data on consumers' computers in Adobe Flash local shared objects ("LSOs," sometimes referred to as "Flash cookies").

23. Adobe Flash Player, which Adobe distributes to consumers without requiring monetary payment, is installed on the majority of U.S. consumers' computers.

24. LSOs are files designed to be used by consumers' Adobe Flash Player software, for purposes such as storing a consumer's volume control preference for audio content or retaining the score of a video game the consumer plays in multiple sessions; Adobe Corporation has stated that LSOs were designed to support consumers' ability to experience "rich Internet application" content using the Adobe Flash Player. Letter to FTC, Adobe Systems Inc., Jan. 27, 2010, available at http://www.ftc.gov/os/comments/privacyroundtable/544506-00085.pdf (last accessed Dec. 6, 2010).

25. Interclick stored LSOs on consumers' computers for purposes other than delivering content to play on consumers' Flash Players or to retain settings for playing Flash content chosen by consumers.

26. Instead, Interclick used LSOs as a substitute and back-up for browser cookies so it could track, profile, and serve targeted advertisements to consumers without being subject to the controls consumers reasonably expected to have over such third-party interactions on the Internet: for consumers whose browser controls were set to block third-party cookies, Interclick used LSOs; and for consumers who had deleted Interclick's browser cookies, Interclick recreated the deleted browser cookies by using the contents stored in LSOs.

27. Interclick's use of this technology was independently confirmed in a report issued by academic researchers and titled, "Flash Cookies and Privacy," which found that a user visiting a website would receive a standard, browser cookie, and an identical, Interclick LSO or "Flash cookie;" if the user deleted the browser cookie, the LSO would be used to "re-spawn" the browser cookie; these operations happened without any notice to the user and without any consent from the user; in addition, both the browser cookie and the LSO set by Interclick would contain a common user identifier. "Flash Cookies and Privacy," A. Soltani, S. Canty, Q. Mayo, L. Thomas,

C.J. Hoofnagle, Univ. Cal., Berkeley, Aug. 10, 2009 at 3, available at

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862 (last accessed Dec. 6, 2010).

28. In its letter to the Federal Trade Commission earlier this year, Adobe Systems Incorporated stated, "Adobe condemns the practice of using Local Storage to back up browser cookies for the purpose of restoring them later without user knowledge and express consent." Letter to FTC, Adobe Systems Inc., Jan. 27, 2010, p. 9, available at

http://www.ftc.gov/os/comments/privacyroundtable/544506-00085.pdf (last accessed Dec. 6, 2010).

29. Interclick reportedly claims it no longer uses LSOs for ad targeting.

30. For consumers, including Plaintiff, on whose computers Interclick has deposited LSOs, those LSOs continue to reside and remain available to Interclick.

31. Unlike third-party browser cookies, for which commercial browsers provide consumers some measure of control, consumers have no reasonable means to decline, detect, or delete LSOs.

C. Interclick's Browser-history sniffing Exploit

32. In the course of displaying advertisements, Interclick executes program code that records the consumer's history of browsing of browsing websites other than the one on which Interclick is displaying its ad to the consumer.

33. This technique of acquiring consumers' web activity data is known as "browser history sniffing" or a "history-sniffing attack." History sniffing exploits the standard browser function that causes a user's previously visited links to be displayed in a different color than links a user has not visited.

34. Interclick's purpose in performing history sniffing was to determine whether a consumer had previously visited certain web pages.

35. Interclick performed history-sniffing as follows: (a) in its code to display an advertisement to a consumer, Interclick embedded history-sniffing code invisible to the consumer; (b) the history-sniffing code contained a list of web page hyperlinks; (c) although the hyperlinks were not displayed to the consumer, the consumer's browser automatically assigned each link a color designation based on whether the user had previously visited the web page associated with

the link; (d) the history-sniffing code performed an examination of the list of color-designated hyperlinks; (e) the history-sniffing code transmitted the results of this examination to Interclick's servers.

36. Interclick's use of this technology was independently confirmed in a report published by academic researchers. *See* "An Empirical Study of Privacy-Violating Information Flows in JavaScript Web Applications," D. Jang, R. Jhala, S. Lerner, H. Shacham, Univ. Cal., San Diego, Oct. 2010, sec. 4, available at http://cseweb.ucsd.edu/~d1jang/papers/ccs10.pdf (last accessed Dec. 6, 2010).

37. Research results showed that, on the web pages on which Interclick performed browser-history sniffing, Interclick's hidden list of hyperlinks contained links for as many 222 websites. *See Id*.

38. Research results showed that Interclick performed browser-history sniffing n a variety of websites, including health, finance, and movie websites, and websites associated with Japanese manga publications and anime video productions popular with a U.S. audience that includes minors. *See Id.*

39. In the research results, Interclick was the entity most frequently associated with the browser-history sniffing. *See Id.*

40. Browser sniffing constitutes cross-domain activity that violates global Internet standards.

D. Interclick's "Enhancement" of Consumers' Information

41. A substantial cost for Interclick is its purchase of consumer data from other entities.

42. Interclick merges the purchased data with the information it acquires through its online contact with consumers to enhance its consumer profiles.

43. Interclick states that it "organizes and valuates billions of data points daily to construct the most responsive digital audiences for major digital marketers."

E. Plaintiff's Experience

44. On or about late October 2010, Plaintiff examined the contents of her local storage associated with the Adobe Flash Player application on her computer and discovered an LSO set by interclick.com.

45. It is Plaintiff's belief that this object is or is part of a tracking device used by Interclick to monitor and profile her Internet activities.

46. Plaintiff did not expect, receive notice of, or consent to the installation of an Interclick LSO and did not want such a device to be installed on her computer.

47. Defendant's use of LSOs to monitor Plaintiff's Internet communications exceeded the scope of any authorization that could have been granted by any publisher on whose web pages Defendant engaged in acquisition of Plaintiff's browser history information.

48. Based on reports of Interclick's browser-history sniffing activities, Interclick's role as a major online ad network, and the presence of an interclick.com LSO on her computer, Plaintiff believes her web-browsing has been the subjected to Interclick's browser-history sniffing.

49. Plaintiff did not expect, receive notice of, or consent to Interclick's performance of browser-history sniffing on her computer and did not want Interclick to engage in such activity.

50. Defendant's browser-history sniffing exceeded the scope of any authorization that could have been granted by any publisher on whose web pages Defendant engaged in acquisition of Plaintiff's browser history information.

51. Plaintiff considers information about her online activities to be in the nature of confidential information that she protects from disclosure by periodically deleting cookies.

52. Plaintiff considers information about any website she has visited to be in the nature of confidential information that she does not expect to be available to an unaffiliated website from a different domain.

53. Plaintiff's experience is typical of the experiences of Class Members.

F. User Consequences

54. Defendant's actions in depositing LSOs on consumers' computers, in addition to circumventing consumers' browser controls, affected consumers' reasonable expectations regarding their abilities to control third-party monitoring and information collection in that: (a) many consumers are aware of browser cookies but are unaware of LSOs; (b) consumers browsers are generally equipped with utilities identifying and controlling third-party browser cookies but consumers but have no reasonable means of identifying or managing LSOs, particularly LSOs repurposed by third-party advertising networks of whose presence consumers are unlikely to be aware; (c) to the extent Adobe Corporation purports to offer tools for managing LSOs, such tools reside on Adobe's servers, are proprietary to Adobe, and are not reasonably usable; (d) unlike browser cookies, which are four kilobytes, LSOs may be up to 100 kilobytes in size; (e) unlike browser cookies which, by default, expire at the end of a consumer's browser session, LSOs have no default expiration; (f) unlike browser cookies, which are stored by and accessible to the consumer through utilities in the consumer's browser or browsers, LSOs are

browser-independent; (g) unlike browser cookies, the specifications for the manner in which LSOs can be created and manipulated is controlled by a single vendor, Adobe; (h) unlike browser cookies, Adobe's design of LSOs permits third-parties' cross-domain access; and (i) and unlike browser cookies, Adobe's design of LSOs permits third parties' nontransparent override of consumers' encrypted (HTTPS) web communications.

55. Defendant's actions in depositing and using LSOs and browser-history sniffing code were surreptitious and without notice and so were conducted without authorization and exceeding authorization.

56. Plaintiff and Class Members sought to maintain the secrecy and confidentiality of their personal information assets acquired by Defendant.

57. The confidential character of Plaintiff and Class Members' personal information is further demonstrated by their utilization of browser privacy controls and their reasonable reliance on global standards that protect users from cross-domain activity.

58. The confidential character of Plaintiff and Class Members' personal information is further demonstrated by Interclick's use of surreptitious and deceptive methods to deposit LSOs and performing browser-history sniffing on Plaintiff and Class Members' computers.

59. Defendant has misappropriated Plaintiff and Class Members' personal information.

60. Defendant's conduct has caused economic loss to Plaintiff and Class Members in that their personal information has discernable value, both to Defendant and to Plaintiff and Class Members.

61. Defendant has deprived Plaintiff and Class Members of the economic value of their personal information and/or diminished its value to Plaintiff and Class Members.

62. Defendant has used Plaintiff and Class Members' personal information for Defendant's own economic benefit.

63. The aggregated loss and damage sustained by the Class, as defined herein, includes economic loss with an aggregated value of at least $5,000 during a one-year period.

64. Defendant perpetrated the acts and omissions set forth in this complaint through an organized campaign of deployment, which constituted a single act.

65. Based on Defendant's actions in acquiring Plaintiff and Class Members' personal information, an implied contract existed between Defendant and Class Members, to which Defendant's assent may be fairly inferred, and under which contract Defendant was unjustly enriched.

66. Plaintiff and Class Members have been harmed by Defendant's deceptive acquisition of their persona information in the loss of their rights to use, share, and maintain the confidentiality of their information, each according to his or her own discretion.

CLASS ALLEGATIONS

67. Pursuant to the Federal Rules of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3), Plaintiff brings this action as a class action on behalf of herself and all others similarly situated as members of the Class, defined as follows:

> All persons residing in the United States that accessed a website that resulted in an interclick.com Adobe Flash local shared object being stored on their computers or whose browser histories were inspected by Interclick.

68. Excluded from the Class are Defendant, its legal representatives, assigns, and successors, and any entity in which Defendant has a controlling interest. Also excluded is the judge to whom this case is assigned and the judge's immediate family.

69. Plaintiff reserves the right to revise this definition of the Class based on facts learned in the course of litigating this matter.

70. The Class consists of millions of individuals and other entities, making joinder impractical.

71. The claims of Plaintiff are typical of the claims of all other Class Members.

72. Plaintiff will fairly and adequately represent the interests of the other Class Members. Plaintiff has retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiff and her counsel are committed to prosecuting this action vigorously on behalf of Class Members and have the financial resources to do so. Neither Plaintiff nor her counsel has any interests adverse to those of the other Class Members.

73. Absent a class action, most Class Members would find the cost of litigating their claims to be prohibitive and would have no effective remedy.

74. The class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation in that it conserves the resources of the courts and the litigants, and promotes consistency and efficiency of adjudication.

75. Defendant has acted and failed to act on grounds generally applicable to Plaintiff and other Class Members, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members.

76. The factual and legal bases of Defendant's liability to Plaintiff and other Class Members are the same, resulting in injury to Plaintiff and all of the other Class Members. Plaintiff and other Class Members have all suffered harm and damages as a result of Defendant's wrongful conduct.

77. There are many questions of law and fact common to Plaintiff and the Class Members and those questions predominate over any questions that may affect individual Class Members. Common questions for the Class include, but are not limited to the following:

a. Whether Defendant, without authorization, created and/or manipulated Adobe Flash Player local stored objects on computers to which Class Members enjoyed rights of possession superior to those of Defendant;

b. For what purpose Defendant created and/or manipulated Adobe Flash Player local stored objects on Class Members' computers;

c. whether Defendant, without authorization, performed browser-history sniffing on computers to which Class Members enjoyed rights of possession superior to those of Defendant;

d. For what purpose Defendant performed browser history-sniffing on Class Members' computers;

e. Whether Defendant violated: (i) the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (ii) the Electronic Communications Privacy Act, 18 U.S.C. § 2510; and (iii) Section 349 of the New York General Business Law

f. Whether Defendant misappropriated valuable information assets of Class Members;

g. Whether Defendant continues to retain valuable information assets from and about Class Members;

h. What uses of such information were exercised and continue to be exercised by Defendant;

i. Whether Defendant invaded the privacy of Class Members;

j. Whether Defendant's actions constituted trespass to personal property;

k. Whether Defendant's actions evince an implied contract between Defendant and Class Members; and

l. Whether Defendant has been unjustly enriched.

78. The questions of law and fact common to Class Members predominate over any questions affecting only individual members, and a class action is superior to all other available methods for the fair and efficient adjudication of this controversy.

CLAIMS FOR RELIEF

79. Based on the foregoing allegations, Plaintiff's claims for relief include the following:

COUNT I
Violations of the Computer Fraud and Abuse Act,
18 U.S.C § 1030, *et seq.*

80. Plaintiff incorporates the above allegations by reference as if fully set forth herein.

81. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030, referred to as "CFAA," regulates fraud and related activity in connection with computers, and makes it unlawful to intentionally access a computer used for interstate commerce or communication, without authorization or by exceeding authorized access to such a computer, thereby obtaining information from such a protected computer, within the meaning of U.S.C. § 1030(a)(2)(C).

82. Defendant violated 18 U.S.C. 1030 by intentionally accessing Plaintiff's and Class Members' computers without authorization or by exceeding authorization, thereby obtaining information from such a protected computer.

83. The CFAA, 18 U.S.C. § 1030(g) provides a civil cause of action to "any person who suffers damage or loss by reason of a violation of CFAA.

84. The CFAA, 18 U.S.C. § 1030(a)(5)(A)(i) makes it unlawful to "knowingly cause the transmission of a program, information, code, or command and as a result of such conduct, intentionally cause damage without authorization, to a protected computer," of a loss to one or more persons during any one-year period aggregating at least $5,000 in value.

85. Plaintiff's computer is a "protected computer . . . which is used in interstate commerce and/or communication" within the meaning of 18 U.S.C. § 1030(e)(2)(B).

86. Defendant violated 18 U.S.C. § 1030(a)(5)(A)(i) by knowingly causing the transmission of a command to be downloaded to Plaintiff's computer, which is a protected computer as defined above. By storing LSOs and executing browser-history sniffing code to access collect, and transmits details of Plaintiff's web activities and communications, Defendant intentionally caused damage without authorization to those Class Members' computers by impairing the integrity of the computers.

87. Defendant violated 18 U.S.C. 1030(a)(5)(A)(ii) by intentionally accessing Plaintiff's and Class Members' protected computers without authorization, and as a result of such conduct, recklessly caused damage to Plaintiff's and Class Members computers by impairing the integrity of data and/or system and/or information.

88. Defendant violated 18 U.S.C. 1030 (a)(5)(A)(iii) by intentionally accessing Plaintiff's and Class Members' protected computers without authorization, and as a result of such conduct, caused damage and loss to Plaintiff and Class Members.

89. Plaintiff and Class Members suffered damage by reason of these violations, as defined in 18 U.S.C. 1030(e)(8), by the "impairment to the integrity or availability of data, a program, a system or information."

90. Plaintiff and Class Members have suffered loss by reason of these violations, as defined in 18 U.S.C. 1030(e)(11), by the "reasonable cost . . . including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."

91. Plaintiff and Class Members have suffered loss by reason of these violations, including, without limitation, violation of the right of privacy, and disclosure of personal information that is otherwise private, confidential, and not of public record.

92. As a result of these takings, Defendant's conduct has caused a loss to one or more persons during any one-year period aggregating at least $5,000 in value in real economic damages.

93. Plaintiff and Class Members have additionally suffered loss by reason of these violations, including, without limitation, the right of privacy.

94. Defendant's unlawful access to Plaintiff's and Class Members' computers and electronic communications has caused Plaintiff and Class Members irreparable injury. Unless restrained and enjoined, Defendant will continue to commit such acts. Plaintiff's and Class Members' remedy at law is not adequate to compensate it for these inflicted and threatened injuries, entitling Plaintiff and Class Members to remedies including injunctive relief as provided by 18 U.S.C. § 1030(g).

COUNT II
Violations of the Electronic Communications Privacy Act,
18 U.S.C. § 2510, *et seq.*

95. Plaintiff incorporates the above allegations by reference as if fully set forth herein.

96. The Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510, referred to as "ECPA," regulates wire and electronic communications interception and interception of

oral communications, and makes it unlawful for a person to "willfully intercept [], endeavor [] to intercept, or procure . . . any other person to intercept or endeavor to intercept any wire, oral, or electronic communication," within he meaning of 18 U.S.C. § 2511(1).

97. Defendant violated 18 U.S.C. § 2511 by intentionally acquiring and/or intercepting, by device or otherwise, Plaintiff and Class members' electronic communications, without knowledge, consent, or authorization.

98. The contents of data transmissions from and to Plaintiff and Class Members' personal computers constitute "electronic communications" within the meaning of 18 U.S.C. § 2510.

99. Plaintiff is a "person whose . . . electronic communication is intercepted . . . or intentionally used in violation of this chapter" within the meaning of 18 U.S.C. § 2520.

100. Defendant violated 18 U.S.C. § 2511(1)(a) by intentionally intercepting, endeavoring to intercept, or procuring any other person to intercept or endeavor to intercept Plaintiff's electronic communications.

101. Defendant violated 18 U.S.C. 2511(1)(c) by intentionally disclosing, or endeavoring to disclose, to any other person, the contents of Plaintiff's electronic communications, knowing or having reason to know that the information was obtained through the interception of Plaintiff's electronic communications.

102. Defendant violated 18 U.S.C. § 2511(1)(d) by intentionally using or endeavoring to use, the contents of Plaintiff's electronic communications, knowing of having reason to know that the information obtained through the interception of Plaintiff's electronic communications.

103. Defendant's intentional interception of these electronic communications was without Plaintiff or the Class Members' knowledge, consent, or authorization and was undertaken without a facially valid court order or certification.

104. Defendant's intentional interception of these electronic communications was without the knowledge, consent, or authorization of the publishers' websites with which Plaintiff and Class Members were communicating and was undertaken without a facially valid court order or certification.

105. Defendant intentionally used such electronic communications, with knowledge, or having reason to know, that the electronic communications were obtained through interception, for an unlawful purpose.

106. Defendant unlawfully accessed and used, and voluntarily disclosed, the contents of the intercepted communications to enhance their profitability and revenue through advertising. This disclosure was not necessary for the operation of Defendant's system or to protect Defendant's rights or property.

107. The Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2520(a) provides a civil cause of action to "any person whose wire, oral, or electronic communications is intercepted, disclosed, or intentionally used" in violation of ECPA.

108. Defendant is liable directly and/or vicariously for this cause of action. Plaintiff therefore seeks remedy as provided for by 18 U.S.C. § 2520, including such preliminary and other equitable or declaratory relief as may be appropriate, damages consistent with subsection (c) of that section to be proven at trial, punitive damages to be proven at trial, and a reasonable attorney's fees and other litigation costs reasonably incurred.

109. Plaintiff and Class Members have additionally suffered loss by reason of these violations, including, without limitation, violation of the right of privacy.

110. Plaintiff and the Class, pursuant to 18 U.S.C. § 2520, are entitled to preliminary, equitable, and declaratory relief, in addition to statutory damages of the greater of $10,000 or $100 per day for each day of violation, actual and punitive damages, reasonable attorneys' fees, and Defendant's profits obtained from the above described violations. Unless restrained and enjoined, Defendant will continue to commit such acts. Plaintiff's remedy at law is not adequate to compensate it for these inflicted and threatened injuries, entitling Plaintiff to remedies including injunctive relief as provided by 18 U.S.C. 2510.

COUNT III
Violation of Section 349 of New York General Business Law
Deceptive Acts and Practices

111. Plaintiff incorporates the above allegations by reference as if fully set forth herein.

112. Defendant's actions alleged herein constitute unlawful, unfair, deceptive, and fraudulent business practices.

113. Defendant's conduct constitutes acts, uses and/or employment by Defendant and/or its agents or employees of deception, fraud, unconscionable and unfair commercial practices, false pretenses, false promises, misrepresentations and/or the knowing concealment, suppression, and/or omission of material facts with the intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of services, and with the subsequent performance of services and transactions, in violation of section 349 of New York's General Business Law.

114. Defendant's acts and omissions were generally directed at the consuming public.

115. The unfair and deceptive trade acts and practices of Defendant have directly, foreseeably, and proximately caused damages and injury to Plaintiff and other members of the Class.

116. Defendant's violations of Section 349 of New York's General Business Law have damaged Plaintiff and other Class Members, and threaten additional injury if the violations continue.

117. Defendant's acts and omissions, including Defendant's misrepresentations, have caused harm to Class Members in that Class Members have suffered the loss of privacy through the exposure of the personal and private information and evasion of privacy controls on their computers.

118. Plaintiff and Class Members have no adequate remedy at law.

119. Plaintiff, on her own behalf, and on behalf of the Class Members, seeks damages, injunctive relief, including an order enjoining Defendant's Section 349 violations alleged herein, and court costs and attorneys' fees, pursuant to NY Gen Bus. Law § 349.

COUNT IV
Trespass to Personal Property/Chattels

120. Plaintiff incorporates the above allegations by reference as if fully set forth herein.

121. The common law prohibits the intentional intermeddling with personal property in possession of another that results in the deprivation of the use of the personal property or impairment of the condition, quality, or usefulness of the personal property.

122. By engaging in the acts alleged in this complaint, without authorization or consent of Plaintiff and Class Members, Defendant dispossessed Plaintiff and Class Members from use and/or access to their computers, or parts of them. Further, these acts impaired the use, value, and quality of Plaintiff and Class Members' computers. Defendant's acts constituted an intentional interference with the use and enjoyment of the computers. By the acts described above, Defendant has repeatedly and persistently engaged in trespass to personal property in violation of the common law.

123. Without Plaintiff and Class Members' consent, or in excess of any consent given, Defendant knowingly and intentionally accessed Plaintiff and Class Members' property and caused injury to Plaintiff and the Members of the Class.

124. Defendant engaged in deception and concealment in order to gain access to Plaintiff and Class Members' computers.

125. Defendant's installation and operation of the LSOs and execution of browser-history sniffing code interfered and/or intermeddled with Plaintiff and Class Members' computers, including by circumventing their controls designed to prevent the information collection effected by Defendant. Such use, interference and/or intermeddling was without consent, or in the alternative, in excess of consent.

126. Defendant's installation and operation of the LSOs and execution of browser-history sniffing code impaired the condition and value of Plaintiff and Class Members' computers.

127. Defendant's trespass to chattels, nuisance, and interference caused real and substantial damage to Plaintiff and Class Members.

128. As a direct and proximate result of Defendant's trespass to chattels, nuisance, interference and unauthorized access of and intermeddling with Plaintiff's and Class Member's property, Defendant has injured and impaired in the condition and value of Class Members' computers as follows:

a. By consuming the resources of and/or degrading the performance of Plaintiff's and Class Members' computers (including space, memory, processing cycles and Internet connectivity);

b. By diminishing the use of, value, speed, capacity, and/or capability of Plaintiff and Class Members' computers;

c. By altering and controlling the functioning of Plaintiff's and Class Members' computers;

d. By devaluing, interfering with, and/or diminishing Plaintiff's and Class Members' possessory interest in their computers;

e. By infringing on Plaintiff's and Class Members' right to exclude others from their computers;

f. By infringing on Plaintiff's and Class Members' right to determine, as owners of their computers, which programs should be installed and operated on their computers;

g. By compromising the integrity, security, and ownership of Class Members' computers; and

h. By forcing Plaintiff and Class Members to expend money, time, and resources in order to remove the program installed on their computers without notice or consent.

129. Plaintiff and Class Members have no adequate remedy at law.

COUNT V
Breach of Implied Contract

130. Plaintiff incorporates the above allegations by reference as if fully set forth herein.

131. The common law prohibits the breaches of contract, including a contract implied under the circumstances of a relationship between parties, such that a breach results in the unjust and inequitable enrichment of one party at the expense of another.

132. By engaging in the acts alleged in this complaint, including the deposit and manipulation of LSOs and the execution of browser-history sniffing code by which Defendant collected Plaintiff and Class Members' personal information without authorization or consent of

Plaintiff and Class Members, Defendant unjustly enriched itself at the expense of Plaintiff and Class Members by appropriating their personal information, through surreptitious means and without their consent, for its own gain and to the detriment of Plaintiff and Class Members' interest in maintaining the confidentiality of their information and/or sharing it with parties of their own choosing.

133. Plaintiff and Class Members have no adequate remedy at law.

COUNT VI
Unjust Enrichment

134. Plaintiff incorporates the above allegations by reference as if fully set forth herein.

135. A benefit has been conferred upon Defendant by Plaintiff and the Class whereby Defendant, directly or indirectly, has received and retained information regarding online communications and activity of Plaintiff and Class Members. Defendant has received and retained information regarding specific purchase and transactional information that is otherwise private, confidential, and not of public record, and/or has received revenue from the provision of such information.

136. Defendant appreciates and/or has knowledge of said benefit.

137. Under principles of equity and good conscience, Defendant should not be permitted to retain the information and/or revenue that it acquired by virtue of its unlawful conduct. All funds, revenue, and benefits received by Defendant rightfully belong to Plaintiff and the Class, which Defendant has unjustly received as a result of its actions.

138. Plaintiff and Class Members have no adequate remedy at law.

DEMAND FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, prays for judgment against Defendant and that the Court may:

A. certify this case as a Class action on behalf of the Class defined above, appoint Plaintiff as Class representative, and appoint her counsel as Class counsel;

B. declare that Defendant's actions, as set forth above, violate the Computer Fraud and Abuse Act; the Electronic Communication Privacy Act; New York General Business Law Section 349; and such common law torts as are alleged above;

C. award injunctive and equitable relief as applicable to the Class *mutatis mutandis*, including:

i. prohibiting Defendant from engaging in the acts alleged above;

ii. requiring Defendant to disgorge to Plaintiff and Class Members or to whomever the Court deems appropriate all of Defendant's ill-gotten gains;

iii. requiring Defendant to delete all data from and about Plaintiff and Class Members that it collected and/or acquired from third parties through the acts alleged above;

iv. requiring Defendant to provide Plaintiff and other Class Members reasonable means to decline, permanently, participation in Defendant's collection of data from and about them;

v. awarding Plaintiff and Class Members full restitution of all benefits wrongfully acquired by Defendant through the wrongful conduct alleged above; and

vi. ordering an accounting and constructive trust to be imposed on the data from and about Plaintiff and Class Members and on funds or other assets obtained by unlawful means as alleged above, to avoid dissipation, fraudulent transfers, and/or concealment of such assets by Defendant;

D. award damages, including statutory damages where applicable, to Plaintiff and Class Members in an amount to be determined at trial;

E. award restitution against Defendant for all money to which Plaintiff and the Class are entitled in equity;

F. restrain, by preliminary and permanent injunction, Defendant, its officers, agents, servants, employees, and attorneys, and those participating with them in active concert, from identifying Plaintiff and Class Members online, whether by personal or pseudonymous identifiers, and from monitoring, accessing, collecting, transmitting, and merging with data from other sources any information from or about Plaintiff and Class Members;

G. award Plaintiff and the Class their reasonable litigation expenses and attorneys' fees; pre- and post-judgment interest to the extent allowable; restitution; disgorgement and other equitable relief as the Court deems proper; compensatory damages sustained by Plaintiff and the Class; statutory damages, including puni-

tive damages; and permanent injunctive relief prohibiting Defendant from engaging in the conduct and practices complained of herein; and

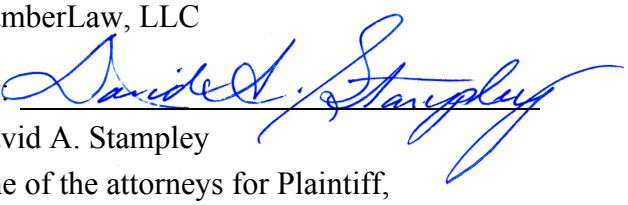
for such other and further relief as this Court deems just and proper.

JURY TRIAL DEMAND

Plaintiff hereby demands a trial by jury of all issues so triable.

Dated: December 8, 2010

Respectfully submitted,
KamberLaw, LLC

By: 
David A. Stampley
One of the attorneys for Plaintiff, individually and on behalf of a class of similarly situated individuals

Scott A. Kamber (SK5794)
skamber@kamberlaw.com
KamberLaw, LLC
100 Wall Street, 23rd Floor
New York, New York 10005
Telephone: (212) 920-3072
Facsimile: (212) 920-3081

David A. Stampley(DS0775)
dstampley@kamberlaw.com
KamberLaw, LLC
100 Wall Street, 23rd Floor
New York, New York 10005
Telephone: (212) 920-3072
Facsimile: (212) 920-3081

Joseph H. Malley (not admitted)
malleylaw@gmail.com
Law Office of Joseph H. Malley
1045 North Zang Boulevard
Dallas, Texas 75208
Telephone: (214) 943-6100

Robert K. Shelquist (not admitted)
Lockridge Grindal Nauen P.L.L.P.
100 Washington Avenue South, Suite 2200
Minneapolis, Minnesota 55401-2159
Telephone: (612) 339-6900
Facsimile: (612) 339-0981