

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

10 CV 9569

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

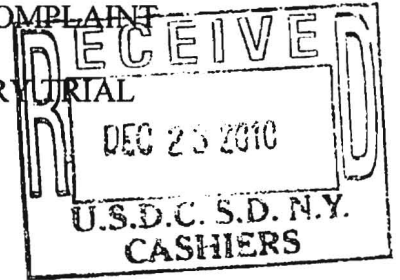
Civil Action No. _____

Plaintiff,

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

v.



MCDONALD'S CORPORATION, a
Delaware Corporation;
CBS CORPORATION, a Delaware
Corporation; MAZDA MOTOR OF
AMERICA, INC., a California Corporation;
MICROSOFT CORPORATION, a
Washington Corporation; and DOES 1-50,

Defendants.

Plaintiff, individually and on behalf of all others similarly situated, makes the following allegations based on her personal knowledge of her own acts and observations and, otherwise, upon information and belief based on investigation of counsel.

NATURE OF THE CASE

1. Plaintiff believes this matter is related to the matter of *Bose v. Interclick, Inc.*, Case No. 1:10-cv-09183-DAB.

2. While visiting websites that displayed Defendants' advertisements, Defendants used their ad displays as a cover for mining Plaintiff's computer to identify websites she had previously visited.

3. Defendants acted in concert with Interclick, mining consumers' web browser histories for entries of particular relevance to Defendants' respective, customized advertising campaigns.

4. Defendants circumvented the privacy and security controls of consumers who, like Plaintiff, had configured their browsers to prevent third-party advertisers from monitoring their online activities.

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

PARTIES

6. Ms. Bose (“Plaintiff”) is a resident of the City, County, and State of New York.

7. Defendant McDonald's Corporation (“McDonald's”) owns, franchises, and operates the largest retail fast food restaurant chain in the United States. McDonald's is a Delaware corporation with principal offices at One McDonald's Plaza, Oak Brook, Illinois 60523.

8. Defendant Microsoft Corporation (“Microsoft”) creates and licenses a wide array of software products and services ranging from operating systems, browsers, and online services, and sells devices that include gaming consoles and mobile telephones. Microsoft is a Washington corporation with principal offices at One Microsoft Way, Redmond, Washington.

9. Defendant CBS Corporation is the ultimate owner and operator of CBS Sports/SportsLine.com, Inc. (“CBS Sportsline”), a provider of online, sports-related information and entertainment. CBS Corporation is a Delaware corporation with principal offices at 51 West 52nd Street, New York, New York 10019.

10. Defendant Mazda Motor of America, Inc. (“Mazda”) oversees the sales, marketing, parts, and customer service support activities of hundreds of Mazda dealers in the U.S. and other North American countries. Mazda is the United States subsidiary of Mazda Motor Corporation, a Japanese corporation, and is headquartered at 7755 Irvine Center Drive, Irvine, California 92618.

11. Each of the defendants designated as Does 1-50 (“Does”) is an individual, corporation, or other business or legal entity, the actual name and location of which is unknown to Plaintiff. Plaintiff designates each such defendant by a fictitious “Doe” name and alleges that, during the Class Period (defined below), each Doe defendant engaged in conduct of a character and consequence like the conduct Plaintiff attributes to the defendants specifically named above. For Doe defendants whose actual identities Plaintiff discovers, Plaintiff will name such defendants by amending her complaint filed in this matter, as permitted by the court.

12. The defendants named and designated above are collectively referred to in this complaint as “Defendants.”

JURISDICTION AND VENUE

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

14. Venue is proper in this District under Title 28, United States Code, Section 1391(b) because Defendants’ improper conduct alleged in this complaint occurred in, was directed from, and/or emanated from this judicial district, including through the actions of Manhattan-based interCLICK, Inc. that are alleged in this complaint.

FACTUAL ALLEGATIONS

A. Defendants' Advertising Campaigns

15. In mid-2010, McDonald's mounted a month-long online advertising campaign tied to its World Cup sponsorship and designed to increase consumer traffic on its website, where consumers could play an online, World Cup-themed game with prize chances. A participating consumer had to enter a unique, nine-digit code from a peel-off game piece acquired from the packaging of a McDonald's sandwich. In addition, each participating consumer had to provide personally identifying information to McDonald's, including name, date of birth, telephone number, mailing address, and email address. Consumers could also play the World Cup game on mobile phones served by one of 23 wireless carriers.

16. Before the spring 2010 start of the major league baseball season, CBS Sportsline promoted its online fantasy sports platform in an advertising campaign designed to improve its market share position against competitors by registering new users and re-engaging users who had previously registered.

17. In 2010, Mazda launched a two-month advertising campaign promoting its new models and summer sales events and designed to increase consumer traffic on its website and identify potential buyers.

18. In 2010, Microsoft mounted a seven-month advertising campaign to promote sales of its new Windows Smartphone.

B. Defendants' Activities with Interclick

19. To conduct these online advertising campaigns, each Defendant engaged interCLICK, Inc. ("Interclick").

20. Interclick is an online advertising network and services provider with principal offices at 257 Park Avenue South, Sixth Floor, New York, New York 10010.

21. Interclick and Defendants worked together in planning, executing, and monitoring the success of Defendants' respective online advertising campaigns.

22. Interclick specializes in "behavioral advertising," that is, Interclick tracks individual consumers to collect information about their web-browsing activities, which it compiles in individual profiles and analyzes to determine which advertisements to display to which consumers.

23. Interclick continually updates its database of consumer profiles with information acquired from and about consumers in its online advertising campaigns.

24. Interclick expends substantial resources to augment its profile database by merging information about consumers' online and offline shopping, interests, and characteristics. Interclick acquires this additional information from data brokers.

25. The information Interclick acquires from data brokers and merges with its database of individual consumer profiles includes consumer household-level information regarding age, income, education, family circumstances, location, lifestyle, shopping patterns, and interests, and including SKU-level purchasing information.

26. Interclick augmented its profile database with individual-level information it acquired from Defendants in the process of optimizing and measuring the success of advertising campaigns. For example, Defendants and Interclick cooperated to identify consumers are "hand raisers" who clicked on an advertisement to visit the advertiser's website, register to enter the advertisers' sweepstakes or play online games, or make purchases.

27. Interclick's profiles are stored and analyzed in a data warehouse designed to allow Interclick to mine and correlate the large volumes of highly granular consumers data it acquires.

28. Interclick has maintained consumer profiles since June 2007.

29. Interclick significantly increased its data warehousing and analysis capabilities in early 2010. Interclick has stated that it "organizes and values billions of data points daily to construct the most responsive digital audiences for major digital marketers."

30. Interclick's compilation and analyses of consumer profile data resulted in the deanonymization of data in consumer profiles such that the profiles constitute consumers' personally identifiable information.

31. Interclick further augments its consumer profiles with information it scrapes from consumers browser history records while it serves advertisements, by engaging in browser history sniffing. Interclick engages in browser history sniffing on behalf of Defendants, to obtain information about entities with whom consumers have communicated and with whom Interclick and Defendants have no affiliation.

32. Defendants and Interclick used browser history sniffing to identify Defendants' competitors with whom consumers communicated and websites consumers visited that might indicate consumers' levels of interest in Defendants' products and services.

33. All the consumer information Interclick acquired while executing an ad campaign for any one Defendant was merged into Interclick's consumer profile database and subsequently used for behavioral targeting on behalf of all Defendants.

34. Defendants' acquisition of consumers' information through browser history sniffing was contrary to Internet communications and interactive advertising standards.

35. In any given month, Interclick's ad-serving activities allow it to communicate with two-thirds to three-quarters of all U.S. consumers who use the Internet.

36. Because Defendants, including Doe Defendants, represent a wide variety of businesses, Interclick's services on behalf of Defendants allow it to communicate with and profile virtually every U.S. consumer.

C. Plaintiff's Experience and Class Consequences

37. Plaintiff is a U.S. consumer who has frequently used the Internet during the Class Period.

38. Plaintiff previously determined that Interclick had created and subsequently utilized an Adobe Flash LSO, or "Flash cookie," ("LSO") on Plaintiff's computer. Plaintiff believes Interclick did so for purposes of tracking and profiling her Internet activities, and so believes Interclick has continued to maintain information about her in its consumer profile database.

39. Based on reports of Defendants' browser-history sniffing activities, Interclick's role as a major online ad network, the presence of an Interclick LSO on her computer, and the scope of Interclick's communications with the population of U.S. Internet users, and the number and duration of Defendants' online advertising campaigns, Plaintiff believes her web-browsing has been the subjected to Defendants' browser-history sniffing and collection of information using LSOs as tracking devices.

40. Plaintiff did not expect, receive notice of, or consent to Defendants' performance of browser-history sniffing or LSO-based tracking on her computer and did not want Defendants to engage in such activity.

41. Defendants' activities were in conflict with the privacy policies and/or terms of use of the websites Plaintiff visited, which were valid contracts between Plaintiff and the owners/operators of such websites; in particular, the contracts did not provide notice of Defendants' browser history sniffing, profiling, and deanonymization activities.

42. Defendants had knowledge of the existence of such contracts between Plaintiff and the websites she visited and, through their service provider, Interclick, knew which specific websites Plaintiff visited and interacted with Interclick.

43. Defendants intentionally procured Interclick to engage in browser history sniffing, profiling, and deanonymization activities, which rendered such websites' privacy commitments false and misleading and constituted violations of Plaintiffs' and such websites contracts.

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

45. Plaintiff's communications on the Internet, during which time Interclick used and collected her information on behalf of Defendants, were electronic communications.

46. Thus, Defendants engaged in and/or caused interception of communications without authorization.

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

48. 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.

49. Plaintiff did not consent to being personally identified to Interclick or for her personally identifiable information to be shared with and used on behalf of Defendants.

50. Defendants' actions were knowing, surreptitious, and without notice and so were conducted without authorization and exceeding authorization.

51. Defendants misappropriated Plaintiff's personal information.

52. Defendants' conduct caused economic loss to Plaintiff in that her personal information has discernable value, both to Defendant and to Plaintiff.

53. Defendants deprived Plaintiff of and/or diminished the economic value of her personal information.

54. Defendants used Plaintiff's personal information for their own economic benefit.

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

56. 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.

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

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

59. Plaintiff and Class Members have been harmed by Defendants' deceptive acquisition of their personal 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

60. 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 who, since June 1, 2007, were profiled by or whose profiles were used by interCLICK, Inc. in the course of its activities with and on behalf of Defendants.

61. Excluded from the Class are Defendants, their legal representatives, assigns, and successors, and any entities in which Defendants have controlling interests. Also excluded is the judge to whom this case is assigned and the judge's immediate family.

62. The "Class Period" is June 1, 2007 to the present.

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

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

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

66. 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.

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

68. 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.

69. 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.

70. The factual and legal bases of Defendants' 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 Defendants' wrongful conduct.

71. 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 Defendants, without authorization, performed browser-history sniffing on computers to which Class Members enjoyed rights of possession superior to those of Defendants;
- b. whether Defendants, without authorization, created personally identifiable profiles of Class Members;

c. Whether Defendants violated: (i) the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (ii) the Electronic Communications Privacy Act, 18 U.S.C. § 2510; (iii) Section 349 of the New York General Business Law; and (iv) other violations of common law.

d. Whether Defendants misappropriated valuable information assets of Class Members;

e. Whether Defendants created or caused or facilitated the creation of personally identifiable consumer profiles of Class Members;

f. Whether Defendants continue to retain and/or make use of, through Inter-click, valuable information assets from and about Class Members;

g. What uses of such information were exercised and continue to be exercised by Defendants;

h. Whether Defendants invaded the privacy of Class Members;

i. Whether Defendants' actions constituted trespass to personal property;

j. Whether Defendants' actions evince an implied contract between Defendants and Class Members; and

k. Whether Defendants have been unjustly enriched.

72. 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

73. 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.

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

75. 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).

76. Defendants 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.

77. 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.

78. 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.

79. 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).

80. Defendants 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, Defendants intentionally caused damage without authorization to those Class Members' computers by impairing the integrity of the computers.

81. Defendants 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.

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

83. 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."

84. 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."

85. 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.

86. As a result of these takings, Defendants' 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.

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

88. Defendants' unlawful access to Plaintiff's and Class Members' computers and electronic communications has caused Plaintiff and Class Members irreparable injury. Unless restrained and enjoined, Defendants 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.*

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

90. 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 the meaning of 18 U.S.C. § 2511(1).

91. Defendants 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.

92. 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.

93. 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.

94. Defendants 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.

95. Defendants 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.

96. Defendants 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.

97. Defendants' 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.

98. Defendants' 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.

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

100. Defendants 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 Defendants' systems or to protect Defendants' rights or property.

101. 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.

102. Defendants are 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.

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

104. 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 Defendants' profits obtained from the above described violations. Unless restrained and enjoined, Defendants 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

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

106. Defendants' actions alleged herein constitute unlawful, unfair, deceptive, and fraudulent business practices.

107. Defendants' conduct constitutes acts, uses and/or employment by and/or their 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.

108. Defendants' acts and omissions were generally directed at the consuming public.

109. 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.

110. Defendants' 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.

111. Defendants' acts and omissions, including Defendants' 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.

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

113. Plaintiff, on her own behalf, and on behalf of the Class Members, seeks damages, injunctive relief, including an order enjoining Defendants' 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

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

115. 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.

116. By engaging in the acts alleged in this complaint, without authorization or consent of Plaintiff and Class Members, Defendants 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. Defendants' acts constituted an intentional interference with the use and enjoyment of the computers. By the acts described above,

Defendants have repeatedly and persistently engaged in trespass to personal property in violation of the common law.

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

118. Defendants engaged in deception and concealment in order to gain access to Plaintiff and Class Members' computers and personal information.

119. Defendants' 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 Defendants. Such use, interference and/or intermeddling was without consent, or in the alternative, in excess of consent.

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

121. Defendants' trespass to chattels, nuisance, and interference caused real and substantial damage to Plaintiff and Class Members.

122. As a direct and proximate result of Defendants' trespass to chattels, nuisance, interference and unauthorized access of and intermeddling with Plaintiff's and Class Member's property, Defendants have 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.

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

COUNT V
Breach of Implied Contract

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

125. 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.

126. 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 Defendants collected Plaintiff's and Class Members' personal information without authorization or consent of Plaintiff and Class Members, Defendants unjustly enriched themselves 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.

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

COUNT VI
Tortious Interference with Contract

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

129. The common law prohibits intentional interference in contracts between other parties that cause one of the parties to breach the contract without justification, resulting in damages. 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. 1) the existence of a valid contract between the plaintiff and a third party; (2) the defendant's knowledge of the contract; (3) the defendant's intentional procurement of the third-party's breach of the contract without justification; (4) actual breach of the contract; and (5) damages resulting therefrom.

130. By engaging in the acts alleged in this complaint, including the execution of browser-history sniffing code by which Defendants collected Plaintiff and Class Members' personal information without authorization or consent of Plaintiff and Class Members and the compilation of deanonymized, personally identifiable profiles, Defendants unjustly enriched themselves 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.

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

COUNT VII
Unjust Enrichment

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

133. A benefit has been conferred upon Defendants by Plaintiff and the Class whereby Defendants, directly or indirectly, have received and retained information regarding online communications and activity of Plaintiff and Class Members. Defendants have 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.

134. Defendants appreciate and/or have knowledge of said benefit.

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

136. 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 Defendants 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 Defendants' 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 Defendants from engaging in the acts alleged above;
 - ii. requiring Defendants to provide reasonable notice and choice to consumers regarding Defendants' data collection, profiling, merger, and de-anonymization activities;
 - iii. requiring Defendants to disgorge to Plaintiff and Class Members or to whomever the Court deems appropriate all of Defendants' ill-gotten gains;
 - iv. requiring Defendants 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;
 - v. requiring Defendants to provide Plaintiff and other Class Members reasonable means to decline, permanently, participation in Defendants' collection of data from and about them;

- vi. awarding Plaintiff and Class Members full restitution of all benefits wrongfully acquired by Defendants through the wrongful conduct alleged above; and
 - vii. 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 Defendants;
- 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 Defendants for all money to which Plaintiff and the Class are entitled in equity;
- F. restrain, by preliminary and permanent injunction, Defendants, 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 punitive 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 22, 2010

Respectfully submitted,
KamberLaw, LLC

By: s/ David A. Stampley

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