IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

MIKE HARRIS and JEFF DUNSTAN, individually and on behalf of a class of similarly situated individuals,	)	
Plaintiffs,	)	Case No. 1:11-5807
v.	)	
COMSCORE, INC., a Delaware corporation,	)	
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiffs Mike Harris and Jeff Dunstan bring this Class Action Complaint against Defendant comScore, Inc. ("comScore") for its unauthorized infiltration of millions of unsuspecting consumer's personal computers, as well as other deceptive and unfair business practices perpetrated in conjunction with its data collection software. Plaintiffs, for their Class Action Complaint, allege as follows upon personal knowledge as to themselves and their own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by their own attorneys.

INTRODUCTION

1. comScore designs, distributes, and deploys its data collection software in a deceptive and calculated fashion to unlawfully monitor the most personal online movements of millions of consumers without their knowledge.

2. comScore provides high profile clients such as the Wall Street Journal, the New York Times, and Fox News with detailed data that it collects from millions of consumers online (hereinafter referred to as "monitored consumers"). These clients pay enormous fees for access to comScore's highly valuable and comprehensive store of information about consumers.

3. comScore asserts that its data provides insight into the purchasing habits, market trends, and other online behavior of consumers. In order to gather such extensive data, comScore relies upon a large pool of consumers with comScore's software operating on their computers: "[C]entral to most comScore services is the comScore panel, the largest continuously measured consumer panel of its kind. With approximately 2 million worldwide consumers under continuous measurement, the comScore panel utilizes a sophisticated methodology that is designed to accurately measure people and their behavior in the digital environment."[1]

4. As one of the biggest players in the Internet research industry, statistics gleaned from comScore's consumer data are featured in major media outlets on a daily basis. However, what lies beneath comScore's data gathering techniques is far more sinister and shocking to all but the few who fully understand its business practices. Namely, comScore has developed highly intrusive and robust data collection software known by such names as RelevantKnowledge, OpinionSpy, Premier Opinion, OpinionSquare, PermissionResearch, and MarketScore (hereinafter collectively referred to in the singular as "Surveillance Software") to surreptitiously siphon exorbitant amounts of sensitive and personal data from consumers' computers. Through subsidiaries bearing innocuous names, comScore uses deceitful tactics to disseminate its software and thereby gain constant monitoring access to millions of hapless consumers' computers and networks.

5. comScore's sophisticated computer applications monitor every action conducted by users. This data is sent to comScore's servers, and then organized and sold to Defendant's clients.[2]

---

[1] comScore Methodology, http://www.comscore.com/About_comScore/Methodology (last visited August 17, 2011).

[2] To accommodate this wealth of information, comScore maintains two of the largest data warehouses in the world. These data storage facilities are comprised of more than five hundred (500) servers, with combined storage accommodation for two-hundred and eighty (280) terabytes, or two-hundred and eighty thousand (280,000) gigabytes of data.

6. To extract this data, comScore's Surveillance Software injects code into the user's web browser to monitor everything viewed, clicked, or inputted online. In addition, the software opens ports,[3] modifies the consumer's firewall, and places "root certificates"[4] on the affected computer to ensure unimpeded access.

7. The scope and breadth of data that comScore collects from unsuspecting consumers is terrifying. By way of illustration, comScore's Surveillance Software constantly collects and transmits the following data, among others, from a consumer's computer to comScore's servers:

a) the monitored consumer's usernames and passwords;

b) queries on search engines like Google;

c) the website(s) the monitored consumer is currently viewing;

d) credit card numbers and any financial or otherwise sensitive information inputted into any website the monitored views;

e) the goods purchased online by the monitored consumer, the price paid by the monitored consumer for the goods, and amount of time the monitored consumer views the goods before purchase;

f) specific advertisements clicked by the monitored consumer.

8. After the Surveillance Software is installed on a monitored consumer's computer, all Internet traffic from the consumer's computer is re-routed through comScore servers before reaching a destination website.

9. Furthermore, comScore's Surveillance Software seeks out and scans every file on the monitored consumer's computer (including word processing documents, emails, PDFs, image files, spreadsheets, etc.), and sends information resulting from examination of those files to comScore's servers.

---

[3] In this context, "ports" are incoming and outgoing portals on a system which facilitate communications between computers over the Internet.

[4] "Root certificates" are more fully explained in ¶¶ 60-66 of this Complaint.

10. Although comScore claims that its software only mines data from the individual consumer's computer, it designed its Surveillance Software to scan files located on any network the host computer is connected to, and sends data about those files back to comScore's servers. In this way, every available file housed on the monitored consumer's local network is accessed by comScore without authorization.

11. In addition, comScore designed its software to intercept packets traversing local wireless networks. Consequently, any monitored consumer running the Surveillance Software inadvertently exposes every nearby user on his or her network to comScore's interception of private data.

12. Because of Defendant's covert methods for deploying its software, millions of monitored consumers remain wholly unaware that their every movement online is under constant surveillance by comScore.

13. To induce individuals to download and install its software, comScore "bundles" its Surveillance Software with software developed by third parties. The third-party software is generally offered at no cost, and includes popular items such as free screensavers and games, and functional applications such as music-copying programs, or greeting-card templates. comScore pays the third-party every time a consumer downloads the bundled software.

14. In many cases, comScore provides no method for the monitored consumer to uninstall its software, and often deceives the consumer into thinking that all of comScore's nefarious software has been removed. Moreover, comScore designed its computer applications to resist attempts to uninstall the Surveillance Software. For example, when a consumer uninstalls the third-party freeware program, comScore's Surveillance Software will *not* be removed.

15. comScore designed its Surveillance Software to be highly persistent. User attempts to disable comScore's applications are wholly ineffectual, as the software automatically

re-starts itself when deactivated. As a result, it is impossible to "turn off" comScore's 24/7 monitoring.

16. Even if a monitored consumer can manage to manually uninstall the Surveillance Software, Defendant programmed its applications to secretly leave behind a comScore root certificate. As discussed in more detail in Section VII *infra*, leaving an untrusted root certificate on a user's computer exposes that individual to attacks by hackers, and allows comScore to re-monitor the consumer's computer in the future.

17. Defendant's Terms of Service ("TOS") do not reveal the extensive and highly intrusive amount of data collected by comScore from consumers' computers.

18. On information and belief, comScore has intentionally designed its Surveillance Software and business practices to surreptitiously maximize both the number of consumers monitored by Defendant, as well as the breadth of information collected.

19. comScore's nefarious tactics drive Defendant's bottom line by enabling the company to sell valuable consumer information to clients for enormous fees. While highly lucrative to the company, comScore's methods demonstrate a wholesale disregard for consumer privacy rights and violate numerous state and federal laws.

PARTIES

20. Plaintiff Mike Harris is a natural person and citizen of the State of Illinois.

21. Plaintiff Jeff Dunstan is a natural person and citizen of the State of California.

22. Defendant comScore, Inc. is a Delaware corporation with its headquarters located at 11950 Democracy Drive, Suite 600, Reston, Virginia 20190. Defendant does business throughout the State of Illinois and the United States.

JURISDICTION AND VENUE

23. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331. This Court has jurisdiction over Defendant because it conducts business in Illinois and/or because the improper conduct alleged in the Complaint occurred in, was directed

from, and/or emanated or exported from Illinois. Personal jurisdiction is additionally proper because Plaintiff Mike Harris is a resident of Illinois.

24. Venue is proper in this District under 28 U.S.C. § 1391(a) because the injury arose in this District. Venue is additionally proper because Defendant transacts significant business in this District, including entering into consumer transactions.

FACTUAL BACKGROUND

I. About comScore

25. comScore is an Internet research corporation that provides marketing data to a wide variety of clients, generally in the form of aggregated reports about online consumer behavior. To collect the data necessary for its reports, comScore monitors consumers' actions using proprietary software ("Surveillance Software") operating on users' computers.

26. The data collected about monitored consumers by the Surveillance Software is transmitted, often in real-time, to comScore's servers. This information is aggregated and organized for Defendant's marketing reports, which are then sold to its clients. comScore currently monitors at least two million computers worldwide.[5]

27. comScore's clients vary widely by industry and size, and include high-profile companies such as the New York Times, the Wall Street Journal, Proctor and Gamble, and Eli Lilly and Company. These companies use comScore's reports for, among other things, statistics for news articles and gauging consumer interest in products and services.

28. comScore is capable of parsing enormous amounts of information and extrapolating narrowly defined trends and statistics, as evidenced by the following quote from the New York Times: "ComScore found a decline of 10 percent in time spent on Web-based email among 18- to 24-year-olds, about the same as it found for people up to the age of 54."[6]

---

[5] comScore Quarterly Report - November 9, 2010, http://ir.comscore.com/secfiling.cfm?filingID=950123-10-103289 (last visited January 1, 2011).

[6] E-Mail's Big Demographic Split, http://bits.blogs.nytimes.com/2010/12/21/e-mails-big-demographic-split/ (last visited January 2, 2011).

29. To provide the highly targeted research data noted above, comScore—through its Surveillance Software—constantly collects, monitors, and analyzes every online move, no matter how private, of over two million persons.

30. Unfortunately, most, if not all monitored consumers are not aware of the depth of data comScore mines from their computers everyday. In many cases, consumers are not even aware of the Surveillance Software's very existence.

II. comScore's Methods for Recruiting and Retaining Individuals to Use Its Monitoring Software

31. As stated in Section I *supra*, comScore tracks the online behavior of over two million (2,000,000) consumers worldwide. To accomplish this, comScore has developed proprietary software that monitors every action conducted on an individual's computer. comScore deploys this software primarily by two methods: 1) online respondent acquisition and 2) a third-party application provider program.[7]

32. Online respondent acquisition simply refers to comScore's method of paying affiliate partners to post comScore's advertisements on their websites in an effort to solicit consumers to download comScore's Surveillance Software. To entice consumers to download the Surveillance Software, comScore offers sweepstakes enrollments and prizes in exchange for membership in its "program."[8] Potential members are also offered software, such as computer games, for free.[9]

33. The second and more devious method that comScore uses to induce consumers to install its Surveillance Software is through its third-party application provider program. This method involves comScore paying developers to bundle the Surveillance Software with the third-

---

[7] comScore Media Matrix U.S. Methodology (hereinafter "comScore report"), http://thearf-org-aux-assets.s3.amazonaws.com/downloads/research/comScore-RReview.pdf, pg. 9 (last visited January 1, 2011).

[8] About RelevantKnowledge, http://www.relevantknowledge.com/about.aspx (last visited January 2, 2011).

[9] Member Benefits, http://www.permissionresearch.com/Benefits.aspx (last visited January 1, 2011).

party application provider's software. The third-party computer application included in the bundled software may be a free screensaver, game, CD burning software, greeting card template, or any other type of "freeware." In many cases, the existence of the Surveillance Software bundled with the freeware is only disclosed, in an inconspicuous fashion, *after the installation process has already begun.*

34. For example, if a consumer downloads a free screensaver bundled with comScore's Surveillance Software, the third-party developer of the screensaver is then paid by comScore for the download of the bundled software.

35. comScore's monitoring software is marketed through subsidiaries bearing names such as TMRG, Inc. and VoiceFive, Inc., with varying names for its Surveillance Software, such as RelevantKnowledge, OpinionSpy, Premier Opinion, OpinionSquare, PermissionResearch, and MarketScore.

III. Consumers are Not Informed About the Information Collected by ComScore's Surveillance Software

36. As discussed herein, comScore's intrusive methods for collecting highly sensitive information from consumers' computers are staggering. However, comScore's Terms of Service ("TOS") presented (or not presented) to the user paint a far different picture than reality.

37. comScore's full Privacy Policy and Terms of Service *fail* to disclose the following facts regarding Surveillance Software operations performed on a consumer's computer:

(a) the Surveillance Software scans files on both local and network volumes;

(b) the Surveillance Software has full rights to access and change any file on the consumer's computer;

(c) the Surveillance Software opens an HTTP "backdoor" to transmit data;

(d) the Surveillance Software analyzes packets of data as they enter and leave a consumer's computer over a local network, and data as they are transferred to and from other computers on the consumer's network.

(e) the Surveillance Software has no user interface from which a consumer

can turn off the software, modify the settings, or otherwise determine what information the software is collecting;

(f) the Surveillance Software implants a "root certificate" that modifies the consumer's computer security settings, and the "root certificate" remains on a consumer's system even after the Surveillance Software is removed;

(g) the Surveillance Software modifies a computer's firewall settings;

(h) the Surveillance Software redirects all internet traffic through comScore's servers before routing it to the consumer's intended website;

(i) the Surveillance Software injects code without user intervention into various web browsers and instant messaging applications;

(j) the Surveillance Software can be upgraded, modified, and controlled remotely, without consumer intervention or permission;

(k) the Surveillance Software will not be deleted if a consumer deletes the free application (*e.g.* free screensaver) with which the Surveillance Software was bundled;

(l) the Surveillance Software will interact with, scan, and monitor networked computers beyond simply the original user's computer.

38. Often, comScore's TOS do not display any actual reference to Defendant's full license agreement whatsoever. (*See* Exhibit A, attached hereto as a true and accurate copy of comScore's Premier Opinion Surveillance Software Terms of Service bundled with a screensaver.**)** Most

39. In many instances, when a consumer installs third-party applications bundled with comScore's Surveillance Software, the graphical display shown to the user makes it appear that only one piece of software is being installed. For example, if a person installs a free screensaver bundled with Defendant's RelevantKnowledge Surveillance Software, a screen will appear *during, and not before,* the installation process displaying a brief description of comScore's

product. Importantly, however, the screen is presented seamlessly with the rest of the installation.

40. Other comScore TOS display screens are presented to the user during the bundled software installation process in such a way that the average, non-expert consumer would not notice the hyperlink to Defendant's full agreement. Examples of these inadequacies include comScore designing its TOS without a functioning link to the full terms, or wedging the link within a sentence, only offset by color.

IV. comScore's Surveillance Software is Constantly Monitoring The Consumer and Transmitting Data to Its Servers

A. comScore Infiltrates Existing Software on the User's Computer

41. Once installed, comScore's Surveillance Software continuously transmits the monitored consumer's online actions back to its servers. In fact, *all* Internet traffic from the consumer's computer is sent through comScore servers before reaching a destination website.

42. In order to collect information about a monitored consumer, comScore designed its Surveillance Software to scan and examine a wide variety of items on the consumer's computer. Through its Surveillance Software, comScore injects code into the monitored consumer's web browser, i.e. Internet Explorer, Safari, Firefox, to monitor *everything* viewed, clicked, or typed into the browser.

43. Additionally, to facilitate its monitoring, comScore's Surveillance Software adds an exception to a the computer's firewall, allowing it unfettered access. Because certain consumers' firewalls are stricter than others, such an attempt to modify the firewall settings, or the subsequent redirection of Internet traffic resulting from the firewall modification, often causes the firewall to lockdown or "freeze" the computer to prevent further harm.

B. comScore Transmits Users' Internet Activity to Its Servers

44. In addition to identifying the specific webpage that the monitored consumer is viewing, the Surveillance Software also transmits information to comScore revealing how much

the individual pays for items in online transactions,[10] how long the individual views items before purchase, and much more. For example, comScore's Surveillance Software observes and reports where the monitored individual's mouse is moving, such as whether or not the monitored consumer is hovering over an advertisement.

45. Perhaps more striking, the Surveillance Software is indiscriminate about the information gathered and sent to comScore's servers. Therefore, names, addresses, credit card numbers, Social Security Numbers, and search terms on search engines are all siphoned and transmitted to comScore.

C. comScore's Software Identifies Individual Users, and Cannot be Turned Off by the User

46. Because comScore requires precise demographic information to create its marketing reports, the Surveillance Software must distinguish which user is currently using the computer at what time. In other words, comScore must know whether or not a father (male, age 45) or his daughter (female, age 14) is using the computer, as that information is necessary to produce accurate demographic marketing reports. To that end, comScore has developed a patented procedure known as "User Demographic Reporting" for creating biometric signatures of consumers by tracking mouse movements and keystrokes. In this way, each time an individual uses the computer, comScore's Surveillance Software tracks his or her keystrokes and mouse movements until it identifies the user as the 14-year-old daughter or 45-year-old father in the household.

47. comScore's software is highly persistent and constantly runs in the background during all computer activities, yet provides no mechanism to turn it off. If, for any reason, the software stops running (including manual user attempts to stop it), it automatically restarts.

---

[10] In the aggregate, this information is used to provide insight into customer spending habits, as evidenced by the following quote from the Wall Street Journal: "From Nov. 1 through Sunday, online consumer spending totaled $17.55 billion, according to comScore Inc. (SCOR). Thanksgiving Day sales jumped 28% from year-earlier levels." Online Holiday Spending Up 12% From 2009 Levels, http://online.wsj.com/article/BT-CO-20101208-710098.html (last visited January 2, 2011).

Accordingly, it is nearly impossible for a consumer to disable the Surveillance Software to avoid spying on certain users of the computer system.

48. By definition, comScore's Surveillance Software is "spyware," meaning it is designed to gather data from a consumer's computer without consent and transfer it to a third party. Because of this characterization, scores of anti-virus and anti-spyware websites identify comScore applications as "severe" or "high risk" spyware or adware. For example, Microsoft's Malware Protection Center has singled out several comScore applications as problematic. In the same vein, numerous U.S. colleges and universities warn students of the dangers of running comScore's software and ban Internet traffic to Defendant's servers.

V. comScore Siphons Data From the Monitored Consumer's Computer and Local Network Without Authorization

49. comScore's TOS indicate that the application will only monitor and collect data about the computer on which it is installed. (*See* Exhibit A & B and *supra* Section III).

50. Defendant's TOS are devoid of any mention that *all files* on that individual's computer will be scanned—and that information about those files will be sent to comScore's servers.

A. comScore Scans All Available Files on the Local Network Attached to the Consumer's Computer

51. In clear contrast to comScore's TOS, its Surveillance Software additionally scans and sends information about available files located on the local network—not just the individual consumer's computer—to Defendant's servers.

52. Put another way, if a monitored consumer uses a local network to store and access files—a nearly ubiquitous practice among modern organizations—then the Surveillance Software also scans all accessible files on the network and sends information about the data to comScore's servers. Depending on the network, these files may include confidential business files, financial documents, trade secrets, or classified government documents.

B. comScore's Surveillance Software Intercepts Data Traveling Over the Monitored Consumer's Local Network

53. comScore's Surveillance Software also monitors and analyzes "packets" of information entering and leaving the monitored consumer's computer.

54. Worse still, comScore's Surveillance Software intercepts wireless packets traversing the local network. Accordingly, a monitored consumer using a computer on a local wireless network also subjects other nearby computers on the network to data collection by the Surveillance Software.

VI. To Avoid Disruption to its Data Collection, comScore Designed Its Surveillance Software to Continue to Operate After the Consumer Attempts to Stop It

55. comScore's Surveillance Software has no user interface from which a consumer can turn off or uninstall the software, modify the settings, or otherwise control what information the software is collecting.

56. As discussed in Section II *supra*, comScore pays third-party developers to bundle Surveillance Software with their applications.

57. Even assuming that an individual recognizes the implications of installing comScore's Surveillance Software in tandem with software such as a free screensaver, or later determines that the free screensaver was the source of the comScore software, a reasonable consumer would believe that once the screensaver was uninstalled, comScore's software would be uninstalled as well. That is not the case.

58. When a monitored consumer uninstalls bundled software, comScore's Surveillance Software remains active on that monitored consumer's computer. As a result, comScore continues to collect information about the monitored consumer, even though the individual believes comScore's Surveillance Software was uninstalled. Indeed, the only way to remove comScore's Surveillance Software is by manually locating and removing it from the system.

59. Because many consumers lack the requisite technical expertise to manually remove comScore's software, these users remain unwitting members of Defendant's monitoring

program. In many cases, consumers are forced to purchase automated spyware removal software to fully eliminate any traces of Defendant's software.

VII. comScore Endangers Consumers by Failing to Remove its Root Certificate During the Uninstall Process for of its Surveillance Software

60. If a monitored consumer manages to manually uninstall comScore's Surveillance Software, Defendant still leaves its own "root certificate" on the user's computer.

A. What is a Root Certificate?

61. In very basic terms, a root certificate is part of an intricate system that helps ensure that websites on the Internet are secure. Web browsers, such as Microsoft's Internet Explorer, come pre-packaged with a store of root certificates issued by trustworthy Certificate Authorities such as VeriSign.[11] A Certificate Authority, such as VeriSign, distributes certificates to trustworthy companies like Amazon.com. When an individual browses Amazon.com, the user's web browser identifies a certificate that was "signed" by VeriSign, and the individual is given assurance that the website is secure. Without this system, it would be extremely difficult, if not impossible, for users to verify which websites were secure and thus safe to transmit sensitive information to, *i.e*. credit card numbers and Social Security Numbers.

62. A Certificate Authority, such as VeriSign, must follow stringent regulations in order to have its root certificate included in a popular web browser. For example, Microsoft requires entities applying for root certificates to comply with rigorous guidelines delineated by the WebTrust for Certification Authorities program sponsored by the American Institute for Certified Public Accountants (AICPA).

63. To average users, the significance of a root certificate is most readily manifested by the small lock in the top left of a web browser that appears when conducting secure transactions over the Internet. This image provides the individual with peace of mind that sensitive information can be transmitted to the website without interception by nefarious actors.

[11] VeriSign is a company that specializes in, among other things, online security and digital certificates. To date, VeriSign is the largest provider of digital certificates.

B. comScore Installs its Own Root Certificate Through its Surveillance Software

64. Included in the installation of the Surveillance Software is a comScore root certificate. This root certificate allows comScore to collect information transmitted through the user's browser, regardless of whether or not the transaction is secure. In other words, because comScore has installed its own root certificate, when a monitored consumer is viewing a website—such as Amazon.com—and thinks that the transaction is free from interception by third-parties because of the image of a small lock in the top left of the browser, that information is *still* captured by Defendant.

65. If a monitored consumer uninstalls the Surveillance Software, comScore has designed its software to leave behind the root certificate.

66. The risks caused by untrusted root certificates are well documented and Defendant's actions pose serious risks to monitored consumers' computer systems.[12]

FACTS RELATING TO PLAINTIFFS

67. In or around March of 2010, Plaintiff Mike Harris downloaded and installed a free screensaver secretly bundled with comScore's Surveillance Software onto his Macintosh computer. The computer Plaintiff used was connected to a local wireless network.

68. After discovering that he had inadvertently installed this software, he searched the World Wide Web to determine how to get rid of the application. Harris attempted to uninstall the screensaver, however the Surveillance Software continued operating. Plaintiff Harris has a high level knowledge of information technology, and was still only able to uninstall the software after conducting hours of diligent research.

---

[12] Hackers use untrusted root certificates such as comScore's to intercept personal data from users without detection. Because the consumer mistakenly believes that the transaction is secure, he or she assumes that it is safe to input sensitive financial or other information. Armed with comScore's root certificate, a hacker can create the faux appearance of a secure transaction. Accordingly, the prospect that comScore may attempt to utilize the root certificates it has intentionally left behind on monitored consumers' computers is a very real threat.

69. Plaintiff Harris did not agree to comScore's Terms of Service and did not know that he was installing Surveillance Software when he installed the free software.

70. In or around September of 2010, Plaintiff Jeff Dunstan downloaded and installed free greeting card template software secretly bundled with comScore's Surveillance Software onto his personal computer running the Microsoft Windows operating system.

71. After installation, Dunstan's firewall detected the re-routing of his Internet traffic to comScore servers, and in response, effectively disabled his computer from accessing the Internet. In fact, Plaintiff Dunstan's computer became entirely debilitated in reaction to the Surveillance Software operating on his computer.

72. Plaintiff Dunstan spent approximately ten hours investigating and researching how comScore's software became installed on his computer and how to remove it.

73. Eventually, Plaintiff Dunstan had to pay forty dollars ($40) for third-party anti-virus software to entirely remove the software from his computer and restore it to a functioning state. Plaintiff Dunstan did not agree to comScore's Terms of Service and did not know that he was installing Surveillance Software when he installed the free software.

CLASS ALLEGATIONS

74. Plaintiffs Mike Harris and Jeff Dunstan bring this action pursuant to Fed. R. Civ. P. 23(b)(2) and (3) on behalf of themselves and the following two classes:

The Surveillance Software Class: All individuals and entities in the United States that have had comScore's Surveillance Software installed on their computer(s).

The Dunstan Subclass: All individuals and entities in the United States that have incurred costs in removing the Surveillance Software.

The Surveillance Software and the Dunstan Subclass are collectively referred to throughout this Complaint as "the Classes."

75. Excluded from the Classes 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, as well as any individual who contributed to the design and deployment of Defendant's software products.

76. The Classes consist of hundreds of thousands, if not millions, of individuals and other entities, making joinder impractical. On information and belief, Defendant has deceived millions of consumers who fall into the definition set forth in the Classes.

77. Plaintiffs' claims are typical of the claims of all other members of the Classes, as Plaintiffs and other members sustained damages arising out of the wrongful conduct of Defendant, based upon the same actions of the software products which were made uniformly to Plaintiffs and the Classes.

78. Plaintiffs will fairly and adequately represent and protect the interests of the other members of the Classes. Plaintiffs have retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the members of the Classes, and have the financial resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to those of the other members of the Classes.

79. Absent a class action, most members of the Classes would find the cost of litigating their claims to be prohibitive and will have no effective remedy. The class treatment of common questions of law and fact is also 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.

80. Defendant has acted and failed to act on grounds generally applicable to Plaintiffs and the other members of the Classes, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the members of the Classes.

81. The factual and legal bases of comScore's liability to Plaintiffs and to the other members of the Classes are the same, and resulted in injury to Plaintiffs and all of the other

members of the Classes. Plaintiffs and the other members of the Classes have all suffered harm as a result of comScore's wrongful conduct.

82. There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Classes, and those questions predominate over any questions that may affect individual members of the Classes. Common questions for the Classes include but are not limited to the following:

(a) whether comScore's intentionally designed its software to scan files located on a monitored consumer's local network;

(b) whether comScore intentionally designed its software to intercept packets on wireless networks;

(c) whether comScore intentionally designed its software and/or business model with third-party application providers to avoid uninstallation when the third-party application was uninstalled, thus thwarting user attempts to remove the software;

(d) whether comScore intentionally designed its Terms of Service to exclude the true functionality of its Surveillance Software;

(e) whether comScore's conduct described herein violated the Stored Communications Act (18 U.S.C. §§ 2701, *et seq.*);

(f) whether comScore's conduct described herein violated the Electronic Communications Privacy Act (18 U.S.C. §§ 2510, *et seq*.);

(g) whether comScore's conduct described herein violated the Computer Fraud & Abuse Act (18 U.S.C. §§ 1030, *et seq*.);

(h) whether comScore's conduct described herein violated the Illinois Consumer Fraud and Deceptive Practices Act (815 ILCS 505/1 *et seq*.);

(i) whether comScore has been unjustly enriched by Plaintiffs and the Classes.

83. Plaintiffs reserve the right to revise these definitions based on facts learned in discovery.

FIRST CAUSE OF ACTION
Violations of the Stored Communications Act
(18 U.S.C. §§ 2701, *et seq*.)
(On Behalf of Plaintiffs and the Classes)

84. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

85. The Electronic Communications Privacy Act, 18 U.S.C. §§ 2510 *et seq.* (the "ECPA") broadly defines an "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce…" 18 U.S.C. § 2510(12). The Stored Communications Act incorporates this definition.

86. Pursuant to the ECPA and Stored Communications Act ("SCA"), "electronic storage" means any "temporary storage of a wire or electronic communication incidental to the electronic transmission thereof." 18 U.S.C. § 2510(17)(A). This type of electronic storage includes communications in intermediate electronic storage that have not yet been delivered to their intended recipient.

87. The SCA mandates, among other things, that it is unlawful for a person to obtain access to stored communications on another's computer system without authorization. 18 U.S.C. § 2701.

88. Congress expressly included provisions in the SCA to address this issue so as to prevent "unauthorized persons deliberately gaining access to, and sometimes tampering with, electronic or wire communications that are not intended to be available to the public." Senate Report No. 99–541, S. REP. 99-541, 35, 1986 U.S.C.C.A.N. 3555, 3589.

89. comScore has violated 18 U.S.C. § 2701(a)(1) because it intentionally accessed consumers' communications without authorization and obtained, altered, or prevented authorized access to a wire or electronic communication while in electronic storage by continuing to operate

after the user uninstalled bundled software. Defendant had actual knowledge of, and benefited from, this practice.

90. Additionally, Defendant has violated 18 U.S.C. § 2701(a)(2) because it intentionally exceeded authorization to access consumers' communications and obtained, altered, or prevented authorized access to a wire or electronic communication while in electronic storage by continuing to operate after the user uninstalled bundled software. Defendant had actual knowledge of, and benefited from, this practice.

91. comScore has also violated 18 U.S.C. § 2701(a)(2) because it intentionally exceeded authorization to access consumers' communications and obtained, altered, or prevented authorized access to a wire or electronic communication while in electronic storage by accessing files on the Plaintiffs' and the Classes' local networks without permission.

92. As a result of Defendant's conduct described herein and its violation of § 2701, Plaintiffs and the Classes have suffered injuries. Plaintiffs, on their own behalves and on behalf of the Classes, seeks an order enjoining Defendant's conduct described herein and awarding themselves and the Classes the maximum statutory and punitive damages available under 18 U.S.C. § 2707.

SECOND CAUSE OF ACTION
Violations of the Electronic Communications Privacy Act
(18 U.S.C. §§ 2510, *et seq.*)
(On Behalf of Plaintiffs and the Classes)

93. Plaintiffs incorporate the forgoing allegations as if fully set forth herein.

94. The Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq.* (the "ECPA") broadly defines an "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce…" 18 U.S.C. § 2510(12).

95. The ECPA defines "electronic communications system" as any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or

electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications. 18 U.S.C. § 2510(14).

96. The ECPA broadly defines the contents of a communication. Pursuant to the ECPA, "contents" of a communication, when used with respect to any wire, oral, or electronic communications, include any information concerning the substance, purport, or meaning of that communication. 18 U.S.C. § 2510(8). "Contents," when used with respect to any wire or oral communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication. The definition thus includes all aspects of the communication itself. No aspect, including the identity of the parties, the substance of the communication between them, or the fact of the communication itself, is excluded. The privacy of the communication to be protected is intended to be comprehensive.

97. Plaintiffs' and Classes Members' personal computers and computer networks constitute "electronic computer systems." Plaintiffs and Classes members transmit "electronic communications" by and through their computers and computer networks in the form of, among others, emails, sending requests to visit websites, online chats, file transfers, file uploads, and file downloads.

98. Defendant's conduct violated 18 U.S.C. § 2511(1)(a) because Defendant intentionally intercepted and endeavored to intercept Plaintiffs' and Classes Members' electronic communications to, from, and within their computers and computer networks.

99. Defendant's conduct violated 18 U.S.C. § 2511(1)(d) because Defendant used and endeavored to use the contents of Plaintiffs' and Classes Members' electronic communications to profit from its unauthorized collection and sale, knowing and having reason to know that the information was obtained through interception in violation of 18 U.S.C. § 2511(1).

100. Defendant intentionally obtained and/or intercepted, by device or otherwise, these electronic communications, without the knowledge, consent or authorization of Plaintiffs or the Classes.

101. Plaintiffs and the Classes suffered harm as a result of Defendant's violations of the ECPA, and therefore seek (a) preliminary, equitable and declaratory relief as may be appropriate, (b) the sum of the actual damages suffered and the profits obtained by Defendant as a result of their unlawful conduct, or statutory damages as authorized by 18 U.S.C. § 2520(2)(B), whichever is greater, (c) punitive damages, and (d) reasonable costs and attorneys' fees.

THIRD CAUSE OF ACTION
Violation of the Computer Fraud and Abuse Act ("CFAA")
(18 U.S.C. §§ 1030, *et seq*.)
(On Behalf of Plaintiffs and the Classes)

102. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

103. Defendant intentionally accessed a computer without authorization and/or exceeded any authorized access and in so doing intentionally breached its own Terms of Service and Privacy Policy.

104. Defendant illegally obtained this information from a protected computer involved in interstate or foreign communication.

105. By scanning and removing information from local and network files, monitoring internet behavior, including keystroke logging consumer input, and injecting code and data onto Plaintiffs' computers, Defendant accessed Plaintiffs' computers, in the course of interstate commerce and/or communication, in excess of the authorization provided by Plaintiffs as descried in 18 U.S.C. § 1030(a)(2)(C).

106. Defendant violated 18 U.S.C. § 1030(a)(2)(C) by intentionally accessing Plaintiffs' and Classes Members' computers and computer networks without authorization and/or by exceeding the scope of that authorization.

107. Plaintiffs' computer, and those belonging to Class Members, are protected computers pursuant to 18 U.S.C. § 1030(e)(2)(B) because they are used in interstate commerce

and/or communication. Specifically, Plaintiff Dunstan spent $40 to purchase a spyware removal program to fully remove the program and restore his computer to a functioning state.

108. By accessing, collecting, and transmitting Plaintiffs and Classes Members' computer data without authorization, Defendant intentionally caused damage to those computers by impairing the integrity of information and/or data.

109. Through the conduct described herein, Defendant has violated 18 U.S.C. § 1030(a)(5)(A)(iii).

110. As a result, 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.

111. Plaintiffs and the Classes expended time, money and resources to investigate and remove comScore's tracking software from his computer.

112. Plaintiffs and Classes members have additionally suffered loss by reason of these violations, including, without limitation, violation of the right of privacy.

113. Defendant's actions were knowing and/or reckless and caused harm to Plaintiffs and members of the Classes.

FOURTH CAUSE OF ACTION
Violation of the Illinois Consumer Fraud and Deceptive Practices Act
(815 ILCS 505/1 *et seq*.)
(On Behalf of Plaintiff Dunstan and the Dunstan Subclass)

114. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

115. The Illinois Consumer Fraud and Deceptive Practices Act, 815 ILCS 505/1 *et seq*. ("ICFA"), protects both consumers and competitors by promoting fair competition in commercial markets for goods and services.

116. The ICFA prohibits any unlawful, unfair or fraudulent business acts or practices including the employment of any deception, fraud, false pretense, false promise,

misrepresentation, or the concealment, suppression, or omission of any material fact. 815 ILCS 505/2.

117. Defendant has engaged in deceptive and fraudulent business practices, as defined by the ICFA, by intentionally concealing the fact that its software was included in supposed "freeware." comScore has further violated the ICFA by fraudulently designing its software to be highly resistant to uninstallation by the user. In addition, comScore has omitted material facts about the true nature of its software products in its Terms of Service. Defendant's practice of profiting from information deceptively gathered from unwitting consumers also constitutes a violation of the ICFA.

118. Plaintiff Dunstan and the Subclass have suffered harm as a proximate result of the violations of law and wrongful conduct of Defendant in the form of actual monetary damages and violations of their privacy rights. Specifically, Plaintiff's computer was debilitated by the surreptitiously installed Surveillance Software and he was forced to spend $40 on third party software to remove comScore's Surveillance Software.

119. Plaintiff seeks an order (1) permanently enjoining Defendants from continuing to engage in unfair and unlawful conduct; (2) requiring Defendants to pay actual and compensatory damages; (3) requiring Defendants to make full restitution of all funds wrongfully obtained; and (4) requiring Defendants to pay interest, attorneys' fees, and costs pursuant to 815 ILCS 505/10a(c).

FIFTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiffs and the Classes)

120. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

121. Plaintiffs and members of the Classes conferred a monetary benefit on Defendant. Defendant received and retained money by selling data to its clients that was collected about

Plaintiffs and the Classes through its Surveillance Software. Much of this information was collected from Plaintiffs and the Classes without authorization and through deceptive business practices.

122. Defendant appreciates or has knowledge of such benefit

123. Under principles of equity and good conscience, Defendant should not be permitted to retain the money obtained by selling information about Plaintiffs and members of the Classes, which Defendant has unjustly received as a result of its unlawful actions.

124. Accordingly, Plaintiffs and the Classes seek full disgorgement and restitution of any amounts comScore has retained as a result of the unlawful and/or wrongful conduct alleged herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Classes, pray for the following relief:

A. Certify this case as a class action on behalf of the Classes defined above, appoint Mike Harris and Jeff Dunstan as class representatives, and appoint their counsel as class counsel;

B. Declare that comScore's actions, as described herein, violate the Stored Communications Act (18 U.S.C. §§ 2701, *et seq.*), the Electronic Communications Privacy Act (18 U.S.C. §§ 2510, *et seq.*), the Computer Fraud and Abuse Act (18 U.S.C. §§ 2510, *et seq.*), and Illinois Consumer Fraud and Deceptive Practices Act (815 ILCS 505/1 *et seq*.);

C. Award injunctive and other equitable relief as is necessary to protect the interests of the Plaintiffs and the Classes, including, *inter alia*: (i) an order prohibiting comScore from engaging in the wrongful and unlawful acts described herein; and (ii) requiring comScore to refrain from accessing files attached to consumers' local networks; and (iii) requiring comScore to delete its root certificate when the Surveillance Software is removed; and (iv) requiring comScore to conspicuously and truthfully display the manner in which it collects data about monitored consumers in its Terms of Service; and (v) requiring comScore to uninstall its

Surveillance Software when bundled software is uninstalled; and (vi) requiring comScore to refrain from intercepting wireless network traffic without authorization.

D. Award damages, including statutory damages of $1,000 per violation under the Stored Communications Act, 18 U.S.C. § 2707(c), and the Electronic Communications Privacy Act, 18 U.S.C. § 2520, and punitive damages where applicable, to Plaintiffs and the Classes in an amount to be determined at trial;

E. Award Plaintiffs and the Classes their reasonable litigation expenses and attorneys' fees;

F. Award Plaintiffs and the Classes pre- and post-judgment interest, to the extent allowable; and

G. Award such other and further relief as equity and justice may require.

JURY TRIAL

Plaintiffs demand a trial by jury for all issues so triable.

Dated: August 23, 2011

RESPECTFULLY SUBMITTED,

MIKE HARRIS AND JEFF DUNSTAN,
INDIVIDUALLY AND ON BEHALF OF A CLASS OF SIMILARLY SITUATED INDIVIDUALS,

By: /s/ Ari J. Scharg
One of Plaintiffs' Attorneys

Jay Edelson
William C. Gray
Ari J. Scharg
Christopher L. Dore
EDELSON MCGUIRE, LLC
350 North LaSalle, Suite 1300
Chicago, Illinois 60654
Telephone: (312) 589-6370
jedelson@edelson.com
wgray@edelson.com
ascharg@edelson.com
cdore@edelson.com