In the United States District Court
for the Northern District of Illinois
Eastern Division

| | | |
|---|---|---|
| MIKE HARRIS and JEFF DUNSTAN, individually and on behalf of a class of similarly Situated individuals, | ) | |
| Plaintiffs, | ) | No. 11 C 5807 |
| v. | ) | Judge James F. Holderman |
| comScore, INC., a Delaware corporation, | ) | Magistrate Judge Nan Nolan |
| Defendant. | ) | |

**ANSWER AND JURY DEMAND**

Now comes comScore, Inc., Defendant herein ("comScore"), by its attorneys MICHAEL G. RHODES and PAUL F. STACK, and in answer to the Complaint herein, states as follows:

**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.

**ANSWER:** comScore denies the allegations contained in paragraph 1 of the Complaint and each of them. Answering further, comScore affirmatively states that it is a leading Internet market research company that designs and distributes software to measure the online activity of Internet users ("Panelists") who volunteer to join a comScore market research panel in exchange for various benefits. comScore specifically denies that its business practices are "deceptive" or are implemented "without the[] knowledge" of its Panelists, for the reasons set forth in response to Paragraph 12 of the Complaint, below.

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.

**ANSWER:** comScore admits that it measures certain online activity of its Panelists. comScore further admits that its clients have included companies like the Wall Street Journal, the New York Times, and Fox News, which use the information for their ordinary business purposes. comScore denies that any client of comScore's syndicated services, like the clients called out in this paragraph, was provided with any detailed data that comScore had collected from its Panelists, as those clients are only provided aggregated data (i.e., comScore would disclose, for example, that in December, four million people went to www.anydomain.com, and has never and would never disclose that on December 18, a specific Panelist went to www.anydomain.com). Except as expressly admitted herein, comScore denies the remaining allegations of paragraph 2 of the Complaint and each of them.

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."

**ANSWER:** comScore admits that its data provides insight into the purchasing habits, market trends, and other online behavior of Panelists. comScore further admits that in order to gather such data, comScore relies on a pool of Internet users who voluntarily install comScore's software on their computers and thereby become Panelists. comScore further admits that the quoted text within the second sentence appeared on certain comScore web pages at certain times.

Answering further, plaintiffs set forth various statements in footnotes to their Complaint contrary to Rule 10(b) of the Federal Rules of Civil Procedure which requires that "all averments of claim . . . shall be made *in* numbered paragraphs . . . ." (Emphasis added). Since the statements in the footnotes do not appear in numbered paragraphs, they are mere surplusage and should be stricken.

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.

**ANSWER:** comScore admits that the media has featured some of its reports, which are based on data gathered from Panelists that have been weighted and aggregated to form a releasable product. comScore further admits that it has developed software which has been branded with names including RelevantKnowledge, Premier Opinion, OpinionSquare, PermissionResearch, and MarketScore (although not all of these brands currently exist), each of which is designed to collect information about the online activity of Internet users who volunteer to be Panelists. comScore denies that its software has been designed to collect sensitive or personal data, as the current software has actually been designed to automatically filter out these types of data (including credit card numbers, social security numbers, account numbers, User IDs, and passwords), so that such information is not transmitted to comScore. comScore admits

that it does have subsidiaries, but denies the use of deceitful tactics to disseminate its software. Plaintiffs use the term "Surveillance Software" to describe comScore's proprietary software. comScore affirmatively states that this term is both pejorative and false and comScore denies the accuracy of the term when it appears *in passim* in the Complaint. Except as expressly admitted herein, comScore denies the allegations of paragraph 4 of the Complaint and each of them.

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.

**ANSWER:** comScore denies the allegations of paragraph 5 of the Complaint and each of them. comScore affirmatively states that its software measures certain limited information regarding the online activity of its Panelists. comScore further acknowledges that some of this limited information is sent to comScore's servers and is then aggregated for analysis. comScore admits that its syndicated clients pay for access to this aggregated data. comScore specifically denies that it monitors "every action" conducted by its Panelists.

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, modifies the consumer's firewall, and places "root certificates" on the affected computer to ensure unimpeded access.

**ANSWER:** comScore admits that when a Panelist voluntarily installs the comScore software, it works with the Panelist's web browser (e.g., Internet Explorer, Firefox) to measure certain of the Panelist's online activity. comScore admits that certain versions of its software can make modifications to the Windows Firewall that was introduced with XP Service Pack 2, and further states that any such modifications are done in accordance with publically available Windows documentation and, to comScore's knowledge, comply with the purpose of, or are consistent with, this feature as provided by the Windows operating system. comScore admits that its software, like any other Internet enabled software, connects to a port on a web server. comScore specifically denies that its software monitors "everything viewed, clicked, or inputted

online." comScore also specifically denies that its software currently installs "root certificates." Except as expressly admitted herein, comScore denies the allegations of paragraph 6 of the Complaint and each of them.

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.

**ANSWER:** Except as expressly stated herein, comScore denies the allegations of paragraph 7 of the Complaint and each of them. comScore affirmatively states that its software collects certain data from Panelists, including queries on search engines; what websites are viewed by Panelists; what goods are purchased by Panelists; what advertisements are clicked by Panelists; the length of time a Panelist is online; and how much a Panelists pays for items in online transactions. comScore specifically denies that its software "constantly collects and transmits" items like credit card numbers, social security numbers, account numbers, user IDs, or passwords; instead, comScore affirmatively states that its software is designed to identify these types of data so that it can irreversibly mask that information or otherwise prevent its transmission to comScore.

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.

**ANSWER:** comScore denies the allegations of paragraph 8 of the Complaint and each of them. comScore specifically denies that any Internet traffic from a panelist's computer is rerouted through comScore servers.

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.

**ANSWER:** Except as expressly stated herein, comScore denies the allegations of paragraph 9 of the Complaint and each of them. comScore affirmatively states that its software collects statistics on the number of files installed on a Panelist's computer (such as the number of PDF or Microsoft Word files). comScore further admits that its software collects statistics on the versions and types of installed software on a Panelist's machine (e.g., whether a Panelist's machine has Microsoft Word installed). comScore denies that it scans every file on a Panelist's computer.

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.

**ANSWER:** Except as expressly stated herein, comScore denies the allegations of paragraph 10 of the Complaint and each of them. comScore affirmatively states that, for a limited period of time, it experimented with establishing a panel for Macintosh users ("Mac Panel"), and developed Macintosh-compatible software specifically for that purpose. comScore

admits that the Mac Panel software was publically available as a limited release beginning on September 29, 2009. comScore further admits that a bug in the Macintosh version of its software potentially allowed the software to count the number of specific types of files located on networks to which Panelists' Macintosh computers were connected, and that this bug was corrected in June 2010. comScore terminated the Mac Panel on or around September 25, 2010. None of the data collected through the Mac Panel was ever shared with, or sold to, a third party.

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.

**ANSWER:** comScore denies that any non-Panelist user of a local network was ever exposed to the collection of private data as any packets monitored by comScore would only have contained network address information. comScore denies the remaining allegations of paragraph 11 of the Complaint and each of them.

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.

**ANSWER:** comScore denies the allegations of paragraph 12 of the Complaint and each of them. comScore denies that it employs "covert methods for deploying its software." To the contrary, comScore's software is designed so that comScore's Terms of Service ("TOS") are presented directly to prospective Panelists prior to completion of the installation process. The TOS disclose the types of information that comScore collects and the methods by which it is collected. Prospective Panelists must click to indicate they have read and agreed to the TOS or comScore's software will not install. Moreover, in Fall 2007, comScore implemented its "Watchdog" or "RK Verify" program, a computer program that ensures the TOS is shown to users during the installation process. comScore's software will not install unless the "Watchdog"

or “RK Verify” program verifies that the TOS was shown to, and accepted by, the user. comScore further notes that, in early 2008, it introduced an icon that appears on a Panelist’s “system tray” any time that comScore software is running, which conspicuously discloses the presence of the software to Panelists. The icon is also displayed in Windows’ “All Programs” menu. In addition, comScore continually delivers messages to Panelists after they join. These messages include a Welcome message sent after installation that thanks Panelists for joining the Panel and provides a link to comScore’s Privacy Policy and to an FAQ that discusses, among other things, how to uninstall comScore’s software. These messages also include invitations to participate in surveys, clearly branded with the name of the panel of which the user is a member. Panelists may also receive benefits that remind them of their participation, including rewards programs that allow them to collect points for doing things like participating in surveys - the collected points can then be redeemed for a variety of items including gift cards or household items. Finally, comScore’s privacy policy and practices have been vetted by a number of third party auditors including TRUSTe, Grant Thornton, and Ernst and Young,. comScore has received certificates of approval for its privacy policy and practices (including for the manner in which it discloses its software) from WebTrust, Better Business Bureau, VeriSign Trusted, Trust Guard, and Network Solutions (among others).

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 screens avers 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.

**ANSWER:** comScore admits that it recruits Panelists through a variety of online methods, including through third-parties that offer comScore’s software during the installation process of their own software applications. comScore further admits that third parties may offer this third-party software at no cost to prospective Panelists. comScore further admits that it

compensates its third party partners that offer the comScore software during the installation process of their own software. Except as expressly admitted herein, comScore denies the allegations of paragraph 13 of the Complaint and each of them.

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.

**ANSWER:** comScore denies the allegations of paragraph 14 of the Complaint and each of them. comScore's software is designed so that it can be permanently and easily uninstalled using the standard Windows "Add or Remove Programs" utility. Moreover, when the software has been installed, an icon appears in the Panelist's system tray to conspicuously disclose the software's presence, thereby signaling to the user whether the software is currently installed. The icon disappears when the software has been uninstalled. comScore affirmatively states that it is inaccurate to refer to the relationship between comScore and its third party distribution partners as involving a "bundle." In fact, once installed, the comScore software is independent of the software provided by the third party, precisely so that an individual may remove the comScore software at any time and independent of the other software installed on this individuals' computer. comScore admits that to remove comScore's software, a Panelist must uninstall the comScore software, but the converse is also true: the removal of comScore's software does not also remove the third party software. In this instance, the comScore software is simply a separate offer made as part of the third party provider's installation process; it is not a "bundle."

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 "tum off' comScore's 24/7 monitoring.

**ANSWER:** comScore denies the allegations of paragraph 15 of the Complaint and each of them. comScore affirmatively states that its software can be permanently uninstalled using the Windows "Add or Remove Programs" utility. After a Panelist properly uninstalls the comScore software, the software does not automatically restart itself.

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 remonitor the consumer's computer in the future.

**ANSWER:** comScore denies that it "programmed its applications to secretly leave behind a comScore root certificate." comScore made use of root certificates with an early version of its software, but no current version of its software has employed root certificates since April 2005. comScore further denies that the installation of a root certificate exposes users to harm from hacking or that it allows comScore to "re-monitor the consumer's computer." comScore believes that installation of a root certificate in and of itself does not expose users to harm from hacking, as no alternative use may be made of this certificate without possession of a master certificate, to comScore's knowledge. comScore has strictly limited internal access to the certificate authority and is not aware of any instances in which third parties have had access to the certificate authority. A root certificate does not create "back door" access to a consumer's computer, so comScore is incapable of "re-monitoring the consumer's computer" with the existence of a root certificate by itself. Except as expressly admitted herein, comScore denies the allegations of paragraph 16 of the Complaint and each of them.

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

**ANSWER:** comScore denies the allegations of paragraph 17 of the Complaint and each of them. comScore's TOS discloses to all prospective Panelists what types of information comScore collects and how the information is collected.

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.

**ANSWER:** comScore denies the allegations of paragraph 18 of the Complaint and each of them.

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.

**ANSWER:** comScore denies the allegations of paragraph 19 of the Complaint and each of them.

**PARTIES**

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

**ANSWER:** comScore lacks knowledge or information sufficient to form a belief as to the truth of the allegations in paragraph 20, and on that basis, denies them.

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

**ANSWER:** comScore lacks knowledge or information sufficient to form a belief as to the truth of the allegations in paragraph 21, and on that basis, denies them.

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.

**ANSWER:** comScore admits the allegations set forth in paragraph 22 of the Complaint.

**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.

**ANSWER:** The allegations of paragraph 23 are legal conclusions to which no response is required. To the extent a response is required, comScore denies that subject matter jurisdiction exists.

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.

**ANSWER:** The allegations of paragraph 24 are legal conclusions to which no response is required. To the extent a response is required, comScore admits that it transacts business in this District.

**FACTUAL BACKGROUND**

**Section I.**

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.

**ANSWER:** comScore admits that it measures the online activity of Internet users who volunteer to become Panelists, using proprietary software that Panelists voluntarily install on their computers, and that it provides market research data to its clients. Except as expressly admitted herein, comScore denies the allegations of paragraph 25 of the Complaint and each of them.

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.

**ANSWER:** comScore admits that the data collected from Panelists through comScore's software is transmitted to comScore's servers. comScore further admits that it provides certain syndicated clients with access to reports after the information is aggregated (e.g., comScore would disclose, for example, that in December, four million people went to www.anydomain.com, and has never and would never disclose that on December 18, a specific panelist went to www.anydomain.com). comScore admits that there are currently over two million people under measurement worldwide. Except as expressly admitted herein, comScore denies the allegations of paragraph 26 of the Complaint and each of them.

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.

**ANSWER:** comScore admits that its clients vary by industry and size, and include companies such as the New York Times, the Wall Street Journal, Proctor and Gamble, and Eli Lilly and Company, who use comScore's data as part of their ordinary business practices. Except as expressly admitted herein, comScore lacks information sufficient to form a belief as to the truth of the remaining allegations in paragraph 27 of the Complaint, and on that basis, denies them.

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."

**ANSWER:** comScore admits that its data can be used to identify certain trends and statistics. Except as expressly admitted herein, comScore lacks information sufficient to form a belief as to the truth of the remaining allegations in paragraph 28of the Complaint, and on that basis, denies them.

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.

**ANSWER:** comScore admits that its software obtains limited information about the online activity of Internet users who volunteer to become Panelists. comScore denies that it "collects, monitors, and analyzes every online move" of its Panelists, and offers as an example that comScore's software is specifically designed not to collect text messages or the text of emails, and that this is just one example of the many areas not monitored by comScore's software. comScore denies the remaining allegations of paragraph 29 of the Complaint and each of them.

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.

**ANSWER:** comScore incorporates its response to paragraph 12. Except as expressly admitted therein, comScore denies the allegations of paragraph 30 of the Complaint and each of them.

**Section II.**

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.

**ANSWER:** comScore admits that its worldwide Panel consists of around two million Internet users. comScore further admits that it has developed proprietary software that Panelists voluntarily download and install, which measures the Panelists' online activity. comScore further admits that its software is distributed through multiple methods. comScore denies that its software monitors every action conducted on an individual's computer. comScore denies the remaining allegations of paragraph 31 of the Complaint and each of them.

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." Potential members are also offered software, such as computer games, for free.

**ANSWER:** comScore admits that it recruits Panelists through a variety of online methods, which include the use of banner advertisements on third party websites. comScore admits that it pays third parties to post comScore's advertisements on their websites. comScore further admits that in exchange for volunteering to become a member of a panel, Panelists may be offered various benefits including planting of trees in their name, sweepstakes enrollments, prizes, points, or free software. Except as expressly admitted herein, comScore denies the allegations of paragraph 32 of the Complaint and each of them.

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-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.*

**ANSWER:** comScore admits that it recruits Panelists through a variety of online methods, which include partnering with third party software developers that offer comScore's software during the installation of their own software. comScore further admits that the third-party software may consist of free screensavers, games, CD burning software, greeting card templates, or other types of "freeware." comScore denies that the incorporation of its software with the third-party software is done "in an inconspicuous fashion" and incorporates by reference its response to paragraph 12 regarding comScore's various methods of disclosure. Except as expressly admitted herein, comScore denies the allegations of paragraph 33 of the Complaint and each of them.

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.

**ANSWER:** comScore admits that it compensates the third-parties who provide an offer for comScore's software as part of the third parties' software applications. Except as expressly admitted herein, comScore denies the allegations of paragraph 34 of the Complaint and each of them.

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, OpinionS quare, PermissionResearch, and MarketScore.

**ANSWER:** comScore admits that its software is marketed through subsidiaries, including but not limited to, TMRG, Inc. and VoiceFive, Inc. comScore further admits that its subsidiaries have used varying names for comScore's software over time, such as RelevantKnowledge, Premier Opinion, OpinionSquare, PermissionResearch, and MarketScore. Except as expressly admitted herein, comScore denies the allegations of paragraph 35 of the Complaint and each of them.

**Section III.**

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.

**ANSWER:** comScore denies the allegations of paragraph 36 of the Complaint and each of them.

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;

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

**ANSWER:** comScore denies the allegations of paragraph 37 of the Complaint and each of them, as well as Plaintiffs' characterization of the TOS, which is a document that speaks for itself. comScore affirmatively states that its proprietary software operates in a manner consistent with its Privacy Policy and Terms of Service. comScore also affirmatively states that it has already denied many of the so called "facts" upon which Paragraph 37 of the Complaint expressly relies.

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

**ANSWER:** Except as expressly set forth herein, comScore denies the allegations of paragraph 38 of the Complaint and each of them. comScore affirmatively states that for a limited period one third party partner failed to include a link to comScore's full Privacy Policy and User License Agreement, however, in these cases, the consumer was presented with comScore's TOS and was required to accept the terms of this TOS. However, this situation was quickly corrected and affected a very small portion of Mac Panel users only. These Mac Panel users'data was never used in any comScore reports, and thus was never provided, even in aggregate form, to anyone outside of comScore. Moreover, the full terms of the Privacy Policy and User License Agreement were available at all times to those Panelists through links installed in the Windows Start Menu, or through an icon on a Mac. In the vast majority of cases, comScore's TOS is presented directly to prospective Panelists within a dialog box that pops up during the installation process. This dialog box contains a link to comScore's full User License Agreement and Privacy Policy ("ULA"), as reflected in Exhibit A of the Complaint. comScore denies the remaining allegations of paragraph 38 of the Complaint, and each of them.

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 resented seamlessly with the rest of the installation.

**ANSWER:** comScore admits that, when a prospective Panelist installs a free screensaver that includes an offer for comScore's RelevantKnowledge software, a dialog box appears during the installation process containing comScore's TOS, which discloses what type of information will be collected and references comScore's full ULA. Except as expressly admitted herein, comScore denies the allegations of paragraph 39 of the Complaint and each of them.

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.

**ANSWER:** comScore denies the allegations of paragraph 40 of the Complaint and each of them.

**Section IV**.

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.

**ANSWER:** comScore admits that, once installed, its software collects and transmits certain aspects of a Panelist's online activity back to comScore's servers. comScore denies that any Internet traffic from a Panelist's computer is sent through comScore's servers before

reaching a destination website. Except as expressly admitted herein, comScore denies the allegations of paragraph 41 of the Complaint and each of them.

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.

**ANSWER:** comScore admits that when a Panelist downloads the comScore software, computer code is installed that works with the Panelist's web browser (e.g., Internet Explorer, Chrome, Firefox) *to measure* the Panelist's online activity. Except as expressly admitted herein, comScore denies the allegations of paragraph 42 of the Complaint and each of them.

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.

**ANSWER:** comScore admits that certain versions of its software make modifications to the Windows Firewall that was introduced with XP Service Pack 2, and incorporates its response to paragraph 6 of the Answer, as though fully set forth herein. comScore lacks knowledge and information sufficient to form a belief as to the truth of the remaining allegations in paragraph 43 of the Complaint, and on that basis, denies them.

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, 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.

**ANSWER:** comScore admits that its software is able to identify the web pages that a Panelist is viewing, and the length of time a Panelist is online. comScore denies that it has ever measured the location or movement of the mouse. Except as expressly admitted herein, comScore denies the remaining allegations of paragraph 44 of the Complaint.

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.

**ANSWER:** comScore denies the allegations of paragraph 45 of the Complaint and each of them, and incorporates its response to paragraphs 4 and 7 of the Answer, as though fully set forth herein.

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.

**ANSWER:** comScore admits that it developed “User Demographic Reporting” (“UDR”), a proprietary technology designed to identify a particular Panelist in a household.

Except as expressly admitted herein, comScore denies the allegations of paragraph 46 of the Complaint and each of them.

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

**ANSWER:** comScore denies the allegations of paragraph 47 of Complaint and each of them. comScore's software is designed so that it can be permanently uninstalled using the standard Windows "Add or Remove Programs" utility and so it is not "impossible" to "turn off" the software. For those Panelists who do not uninstall the software, comScore admits that its software runs in the background during a Panelist's computer activities.

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.

**ANSWER:** comScore denies that its software constitutes "spyware," or that it is designed to gather data from a consumer's computer without consent. comScore affirmatively states that anti-virus offerings from companies including Microsoft, AVG and McAfee categorize comScore's software as clean, and do not classify it as spyware. comScore lacks knowledge and information sufficient to form a belief as to the truth of the remaining allegations in paragraph 48 of the Complaint, and on that basis, denies each of them.

**Section V.**

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).

**ANSWER:** comScore denies the characterization in Paragraph 49 of the Complaint of comScore's TOS, which speaks for itself. Moreover, Paragraph 49 references, and relies on, an exhibit to the Complaint ("Exhibit B") that does not exist. On that basis, comScore lacks knowledge and information sufficient to form a belief as to the truth of the remaining allegations in paragraph 49 of the Complaint, and on that basis, denies them.

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.

**ANSWER:** comScore denies the characterization in Paragraph 50 of comScore's Terms of Service, which is a document that speaks for itself. comScore notes that its TOS informs users that its software monitors and collects "certain hardware, software, computer configuration and application usage information," as depicted in Exhibit A to the Complaint. Further, comScore denies the premise upon which paragraph 50 is based – that comScore's software causes "all files on that individual's computer [to] be scanned."

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.

**ANSWER:** comScore incorporates its response to paragraph 10 of the Answer. Except as expressly admitted herein, comScore denies the allegations of paragraph 51 of the Complaint.

52. Put another way, if a monitored consumer uses a local network to store and access files-a nearly ubiquitous practice among modem 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.

**ANSWER:** comScore incorporates its response to paragraph 51 of the Complaint. Except as expressly admitted therein, comScore denies the allegations of paragraph 52 of Complaint and each of them.

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

**ANSWER:** comScore admits that its software measures certain types of packets. Except as expressly admitted herein, comScore denies the allegations of paragraph 53 of the Complaint and each of them.

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.

**ANSWER:** comScore admits that its software measures certain types of packets, but because these packets can only be used to identify the type of other devices on a network, comScore denies that any non-Panelist computer is subject to data collection. Except as expressly admitted therein, comScore denies the allegations of paragraph 54 of the Complaint and each of them.

**Section VI.**

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.

**ANSWER:** comScore denies the allegations of paragraph 55 of the Complaint and each of them. comScore’s software is designed so that it can be uninstalled using a Windows user’s “Add or Remove Programs” utility.

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

**ANSWER:** comScore admits that it pays third-party developers to offer comScore's software with their applications. Except as expressly admitted herein, comScore denies the allegations of paragraph 56 of Complaint and each of them.

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.

**ANSWER:** comScore denies Plaintiffs' characterizations regarding what a "reasonable consumer would believe," and on that basis denies the allegations of paragraph 57 of the Complaint and each of them. comScore's software is designed so that it can be permanently uninstalled using the standard Windows "Add or Remove Programs" utility. Any time comScore software is running, an icon appears in the Panelists' system tray to conspicuously disclose the software's presence, thereby signaling to the user whether or not the software has been uninstalled. Moreover, the presence of comScore's software is made known to Panelists in numerous other ways, as described in comScore's response in paragraph 12 of the Answer.

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.

**ANSWER:** comScore admits that, to remove comScore's software, a Panelist must uninstall comScore's software and not the separate third-party freeware program, and incorporates its response in paragraph 14 of the Answer as if fully set forth herein. comScore lacks knowledge and information sufficient to form a belief as to the truth of the remaining allegations in paragraph 58 regarding the purported beliefs of consumers as characterized by

Plaintiffs, and on that basis, denies them. comScore notes, however, that its software can be uninstalled using a Windows user's "Add or Remove Programs" utility. Moreover, any time comScore software is running, an icon appears in the Panelists' system tray to conspicuously disclose the software's presence, thereby signaling to the user whether or not the software has been uninstalled.

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.

**ANSWER:** comScore lacks knowledge and information sufficient to form a belief as to the truth of the allegations in paragraph 59 of the Complaint and each of them, which reflects Plaintiffs' characterizations of the "technical expertise" of consumers, and on that basis, denies them.

**Section VII.**

60. If a monitored consumer manages to manually uninstall comScore's Surveillance Software, Defendant sti11leaves its own "root certificate" on the user's computer.

**ANSWER:** comScore denies the allegations of paragraph 60 of Complaint and each of them. comScore's software stopped installing "root certificates" in April 2005.

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. 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.

**ANSWER:** Paragraph 61 reflects Plaintiffs' characterizations of general industry information and does not require a response. To the extent a response is required, comScore lacks information sufficient to form a belief as to the truth of the allegations in paragraph 61 of the Complaint, and on that basis, denies them.

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).

**ANSWER:** Paragraph 62 reflects Plaintiffs' characterizations of general industry information and does not require a response. To the extent a response is required, comScore lacks information sufficient to form a belief as to the truth of the allegations in paragraph 62 of the Complaint, and on that basis, denies them. comScore notes, however, its Panels are certified by WebTrust, the very "certification authority" identified in this paragraph of the Complaint. comScore's Panels are also certified by, among others, the Better Business Bureau, VeriSign Trusted, Trust Guard, and Network Solutions.

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.

**ANSWER:** Paragraph 63 reflects Plaintiffs' characterizations of the expectations of "average users" and does not require a response. To the extent a response is required, comScore lacks information sufficient to form a belief as to the truth of the allegations in paragraph 63 of the Complaint, and on that basis, denies them.

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.

**ANSWER:** comScore denies the allegations of paragraph 64 of the Complaint and each of them. comScore's software stopped installing "root certificates" in April 2005. comScore further denies Plaintiffs' characterizations of what "a monitored consumer" might believe with respect to the monitoring of online activity.

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

**ANSWER:** comScore denies the allegations of paragraph 65 of the Complaint and each of them. comScore's software stopped installing "root certificates" in April 2005.

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

**ANSWER:** comScore is not aware of any instances in which any consumers have been harmed by the presence of a root certificate installed by the comScore software and, on that basis, denies the allegations of paragraph 66 of the Complaint. Moreover, comScore stopped installing "root certificates" in April 2005.

**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.

**ANSWER:** comScore lacks information sufficient to form a belief as to the truth of the allegations in paragraph 67 of the Complaint, and on that basis, denies them.

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.

**ANSWER:** comScore lacks information sufficient to form a belief as to the truth of the allegations in paragraph 68 of the Complaint, and on that basis, denies them.

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.

**ANSWER:** comScore lacks information sufficient to form a belief as to the truth of the allegations in paragraph 69 of the Complaint, and on that basis, denies them. comScore notes, however, that Plaintiff Harris would not have been able to install comScore's software unless he affirmatively clicked to agree to comScore's Terms of Service, which expressly informs users of the presence of comScore's software. Assuming Plaintiff Harris installed comScore's software, he would have also been presented with a "welcome" pop up, after installation, thanking him for joining the Panel and providing a link to comScore's Privacy Policy and to an FAQ that discusses, among other things, how to uninstall comScore's 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.

**ANSWER:** comScore lacks information sufficient to form a belief as to the truth of the allegations in paragraph 70 of the Complaint, and on that basis, denies them.

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.

**ANSWER:** comScore lacks information sufficient to form a belief as to the truth of the allegations in paragraph 71 of the Complaint, and on that basis, denies them.

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

**ANSWER:** comScore lacks information sufficient to form a belief as to the truth of the allegations in paragraph 72 of the Complaint, and on that basis, denies them.

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.

**ANSWER:** comScore lacks information sufficient to form a belief as to the truth of the allegations in paragraph 73 of the Complaint, and on that basis, denies them. comScore notes, however, that Plaintiff Dunstan would not have been able to install comScore's software unless he affirmatively clicked to agree to comScore's Terms of Service, which expressly informs users of the presence of comScore's software. Assuming Plaintiff Dunstan installed comScore's software, he would have also been presented with a "welcome" pop up, after installation, thanking him for joining the Panel and providing a link to comScore's Privacy Policy and to an FAQ that discusses, among other things, how to uninstall comScore's software. comScore further denies that Dunstan "had to" purchase third-party anti-virus software to remove the comScore software, since the software can be removed using a standard Windows utility.

**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."

**ANSWER:** Paragraph 74 of the Complaint reflects Plaintiffs' characterization of their own complaint and proposed classes and does not require a response. To the extent a response is required, this allegation is denied.

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.

**ANSWER:** Paragraph 75 of the Complaint reflects Plaintiffs' characterization of their own complaint and proposed classes and does not require a response, and denies that this action can be maintained as a class action. To the extent a response is required, this allegation is denied.

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.

**ANSWER:** comScore lacks information sufficient to form a belief as to the truth of the allegations in paragraph 76 of the Complaint, and on that basis, denies them. comScore denies

that it has "deceived millions of consumers," and denies that this action can be maintained as a class action.

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.

**ANSWER:** The allegations set forth in paragraph 77 of the Complaint assert conclusions of law to which no response is required. To the extent paragraph 77 may purport to assert allegations of fact to which a response may be required, comScore denies each and every allegation contained in this paragraph, and denies that this action can be maintained as a class action.

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.

**ANSWER:** The allegations set forth in paragraph 78 of the Complaint assert conclusions of law to which no response is required. To the extent paragraph 78 may purport to assert allegations of fact to which a response may be required, comScore denies those allegations and denies that this action can be maintained as a class action. comScore lacks knowledge or information sufficient to form a belief as to the truth of the allegations in paragraph 78 regarding the motivations of Plaintiffs and their counsel, or their financial wherewithal, and on that basis, denies them.

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.

**ANSWER:** The allegations set forth in paragraph 79 of the Complaint assert conclusions of law to which no response is required. To the extent paragraph 79 may purport to assert allegations of fact to which a response may be required, comScore denies those allegations, and denies that this action can be maintained as a class action.

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.

**ANSWER:** The allegations set forth in paragraph 80 of the Complaint assert conclusions of law to which no response is required. To the extent paragraph 80 may purport to assert allegations of fact to which a response may be required, comScore denies those allegations, and denies that this action can be maintained as a class action.

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.

**ANSWER:** The allegations set forth in paragraph 81 of the Complaint assert conclusions of law to which no response is required. To the extent paragraph 81 may purport to assert allegations of fact to which a response may be required, comScore denies those allegations, and denies that this action can be maintained as a class action

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.

**ANSWER:** The allegations set forth in paragraph 82 of the Complaint assert conclusions of law to which no response is required. To the extent paragraph 82 may purport to assert allegations of fact to which a response may be required, comScore denies those allegations, and denies that this action can be maintained as a class action.

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

**ANSWER:** Paragraph 83 of the Complaint reflects Plaintiffs effort to reserve certain rights and does not require a response.

**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.

**ANSWER:** comScore hereby incorporates as though fully set forth herein its answers to paragraphs 1 through 83.

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.

**ANSWER:** The allegations set forth in paragraph 85 assert conclusions of law to which no response is required. To the extent paragraph 85 may purport to assert allegations of fact to which a response may be required, comScore states that the statutes cited by Plaintiffs speak for themselves, and comScore denies any characterization of the laws applicable to this case that is inconsistent with their language. Except as specifically admitted, comScore denies each and every allegation contained in this paragraph.

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.

**ANSWER:** The allegations set forth in paragraph 86 assert conclusions of law to which no response is required. To the extent paragraph 86 may purport to assert allegations of fact to which a response may be required, comScore states that the statutes cited by Plaintiffs speak for themselves, and comScore denies any characterization of the laws applicable to this case that is

inconsistent with their language. Except as specifically admitted, comScore denies each and every allegation contained in this paragraph.

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.

**ANSWER:** The allegations set forth in paragraph 87 assert conclusions of law to which no response is required. To the extent paragraph 87 may purport to assert allegations of fact to which a response may be required, comScore states that the statutes cited by Plaintiffs speak for themselves, and comScore denies any characterization of the laws applicable to this case that is inconsistent with their language. Except as specifically admitted, comScore denies each and every allegation contained in this paragraph.

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.

**ANSWER:** The allegations set forth in paragraph 88 assert conclusions of law to which no response is required. To the extent paragraph 88 may purport to assert allegations of fact to which a response may be required, comScore states that the statutes cited by Plaintiffs speak for themselves, and comScore denies any characterization of the laws applicable to this case that is inconsistent with their language. Except as specifically admitted, comScore denies each and every allegation contained in this paragraph.

89. comScore has violated 18 U.S.C. § 270 1 (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.

**ANSWER:** The allegations set forth in paragraph 89 assert conclusions of law to which no response is required. To the extent paragraph 89 may purport to assert allegations of fact to which a response may be required, comScore states that the statutes cited by Plaintiffs speak for themselves, and comScore denies any characterization of the laws applicable to this case that is inconsistent with their language. Except as specifically admitted, comScore denies each and every allegation contained in this paragraph.

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.

**ANSWER:** The allegations set forth in paragraph 90 assert conclusions of law to which no response is required. To the extent paragraph 90 may purport to assert allegations of fact to which a response may be required, comScore states that the statutes cited by Plaintiffs speak for themselves, and comScore denies any characterization of the laws applicable to this case that is inconsistent with their language. Except as specifically admitted, comScore denies each and every allegation contained in this paragraph.

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.

**ANSWER:** The allegations set forth in paragraph 91 assert conclusions of law to which no response is required. To the extent paragraph 91 may purport to assert allegations of fact to which a response may be required, comScore states that the statutes cited by Plaintiffs speak for themselves, and comScore denies any characterization of the laws applicable to this case that is

inconsistent with their language. Except as specifically admitted, comScore denies each and every allegation contained in this paragraph.

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.

**ANSWER:** comScore admits that Plaintiffs purport seek the relief requested in paragraph 92. Except as otherwise expressly admitted herein, comScore denies the allegations of paragraph 92.

**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.

**ANSWER:** comScore hereby incorporates as though fully set forth herein its answers to paragraphs 1 through 92.

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).

**ANSWER:** The allegations set forth in paragraph 94 assert conclusions of law to which no response is required. To the extent paragraph 94 may purport to assert allegations of fact to which a response may be required, comScore states that the statutes cited by Plaintiffs speak for themselves, and comScore denies any characterization of the laws applicable to this case that is inconsistent with their language. Except as specifically admitted, comScore denies each and every allegation contained in this paragraph.

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).

**ANSWER:** The allegations set forth in paragraph 95 assert conclusions of law to which no response is required. To the extent paragraph 95 may purport to assert allegations of fact to which a response may be required, comScore states that the statutes cited by Plaintiffs speak for themselves, and comScore denies any characterization of the laws applicable to this case that is inconsistent with their language. Except as specifically admitted, comScore denies each and every allegation contained in this paragraph.

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.

**ANSWER:** The allegations set forth in paragraph 96 assert conclusions of law to which no response is required. To the extent paragraph 96 may purport to assert allegations of fact to which a response may be required, comScore states that the statutes cited by Plaintiffs speak for themselves, and comScore denies any characterization of the laws applicable to this case that is inconsistent with their language. Except as specifically admitted, comScore denies each and every allegation contained in this paragraph.

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.

**ANSWER:** The allegations set forth in paragraph 97 assert conclusions of law to which no response is required. To the extent paragraph 97 may purport to assert allegations of fact to which a response may be required, comScore states that the statutes cited by Plaintiffs speak for themselves, and comScore denies any characterization of the laws applicable to this case that is inconsistent with their language. Except as specifically admitted, comScore denies each and every allegation contained in this paragraph.

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.

**ANSWER:** The allegations set forth in paragraph 98 assert conclusions of law to which no response is required. To the extent paragraph 98 may purport to assert allegations of fact to which a response may be required, comScore states that the statutes cited by Plaintiffs speak for themselves, and comScore denies any characterization of the laws applicable to this case that is inconsistent with their language. Except as specifically admitted, comScore denies each and every allegation contained in this paragraph.

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).

**ANSWER:** The allegations set forth in paragraph 99 assert conclusions of law to which no response is required. To the extent paragraph 99 may purport to assert allegations of fact to

which a response may be required, comScore states that the statutes cited by Plaintiffs speak for themselves, and comScore denies any characterization of the laws applicable to this case that is inconsistent with their language. Except as specifically admitted, comScore denies each and every allegation contained in this paragraph.

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.

**ANSWER:** The allegations set forth in paragraph 100 assert conclusions of law to which no response is required. To the extent paragraph 100 may purport to assert allegations of fact to which a response may be required, comScore states that the statutes cited by Plaintiffs speak for themselves, and comScore denies any characterization of the laws applicable to this case that is inconsistent with their language. Except as specifically admitted, comScore denies each and every allegation contained in this paragraph.

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.

**ANSWER:** comScore admits that Plaintiffs purport seek the relief requested in paragraph 101. Except as otherwise expressly admitted herein, comScore denies the allegations of paragraph 101.

**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.

**ANSWER:** comScore hereby incorporates as though fully set forth herein its answers to paragraphs 1 through 101.

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.

**ANSWER:** The allegations set forth in paragraph 103 assert conclusions of law to which no response is required. To the extent paragraph 103 may purport to assert allegations of fact to which a response may be required, comScore states that the statutes cited by Plaintiffs speak for themselves, and comScore denies any characterization of the laws applicable to this case that is inconsistent with their language. Except as specifically admitted, comScore denies each and every allegation contained in this paragraph.

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

**ANSWER:** The allegations set forth in paragraph 104 assert conclusions of law to which no response is required. To the extent paragraph 104 may purport to assert allegations of fact to which a response may be required, comScore states that the statutes cited by Plaintiffs speak for themselves, and comScore denies any characterization of the laws applicable to this case that is inconsistent with their language. Except as specifically admitted, comScore denies each and every allegation contained in this paragraph.

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).

**ANSWER:** The allegations set forth in paragraph 105 assert conclusions of law to which no response is required. To the extent paragraph 105 may purport to assert allegations of

fact to which a response may be required, comScore states that the statutes cited by Plaintiffs speak for themselves, and comScore denies any characterization of the laws applicable to this case that is inconsistent with their language. Except as specifically admitted, comScore denies each and every allegation contained in this paragraph.

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.

**ANSWER:** The allegations set forth in paragraph 106 assert conclusions of law to which no response is required. To the extent paragraph 106 may purport to assert allegations of fact to which a response may be required, comScore states that the statutes cited by Plaintiffs speak for themselves, and comScore denies any characterization of the laws applicable to this case that is inconsistent with their language. Except as specifically admitted, comScore denies each and every allegation contained in this paragraph.

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.

**ANSWER:** The allegations set forth in paragraph 107 assert conclusions of law to which no response is required. To the extent paragraph 107 may purport to assert allegations of fact to which a response may be required, comScore states that the statutes cited by Plaintiffs speak for themselves, and comScore denies any characterization of the laws applicable to this case that is inconsistent with their language. Except as specifically admitted, comScore denies each and every allegation contained in this paragraph.

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.

**ANSWER:** The allegations set forth in paragraph 108 assert conclusions of law to which no response is required. To the extent paragraph 108 may purport to assert allegations of fact to which a response may be required, comScore states that the statutes cited by Plaintiffs speak for themselves, and comScore denies any characterization of the laws applicable to this case that is inconsistent with their language. Except as specifically admitted, comScore denies each and every allegation contained in this paragraph.

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

**ANSWER:** The allegations set forth in paragraph 109 assert conclusions of law to which no response is required. To the extent paragraph 109 may purport to assert allegations of fact to which a response may be required, comScore states that the statutes cited by Plaintiffs speak for themselves, and comScore denies any characterization of the laws applicable to this case that is inconsistent with their language. Except as specifically admitted, comScore denies each and every allegation contained in this paragraph.

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.

**ANSWER:** The allegations set forth in paragraph 110 assert conclusions of law to which no response is required. To the extent paragraph 110 may purport to assert allegations of fact to which a response may be required, comScore states that it lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 110, and on that basis, denies them.

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

**ANSWER:** comScore lacks information sufficient to form a belief as to the truth of the allegations in paragraph 111, and on that basis, denies them.

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

**ANSWER:** The allegations set forth in paragraph 112 assert conclusions of law to which no response is required. To the extent paragraph 112 may purport to assert allegations of fact to which a response may be required, comScore states that it lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 112, and on that basis, denies them.

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

**ANSWER:** The allegations set forth in paragraph 113 assert conclusions of law to which no response is required. To the extent paragraph 113 may purport to assert allegations of fact to which a response may be required, comScore denies those allegations.

**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.

**ANSWER:** comScore hereby incorporates as though fully set forth herein its answers to paragraphs 1 through 113.

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.

**ANSWER:** The allegations set forth in paragraph 115 assert conclusions of law to which no response is required. To the extent paragraph 115 may purport to assert allegations of fact to which a response may be required, comScore states that it lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 115, and on that basis, denies them.

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.

**ANSWER:** The allegations set forth in paragraph 116 assert conclusions of law to which no response is required. To the extent paragraph 116 may purport to assert allegations of fact to which a response may be required, comScore states that the statutes cited by Plaintiffs speak for themselves, and comScore denies any characterization of the laws applicable to this case that is inconsistent with their language. Except as specifically admitted, comScore denies each and every allegation contained in this paragraph.

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.

**ANSWER:** The allegations set forth in paragraph 117 assert conclusions of law to which no response is required. To the extent paragraph 117 may purport to assert allegations of fact to which a response may be required, comScore states that the statutes cited by Plaintiffs speak for themselves, and comScore denies any characterization of the laws applicable to this case that is inconsistent with their language. Except as specifically admitted, comScore denies each and every allegation contained in this paragraph.

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, Plaintiffs 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.

**ANSWER:** The allegations set forth in paragraph 118 assert conclusions of law to which no response is required. To the extent paragraph 118 may purport to assert allegations of fact to which a response may be required, comScore states that it lacks knowledge or information sufficient to form a belief as to the truth of the allegations of paragraph 118, and on that basis, denies them

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).

**ANSWER:** comScore admits that Plaintiffs purport seek the relief requested in paragraph 119. Except as otherwise expressly admitted herein, comScore denies the allegations of paragraph 119.

**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.

**ANSWER:** comScore hereby incorporates as though fully set forth herein its answers to paragraphs 1 through 119.

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.

**ANSWER:** comScore denies the allegations of paragraph 121.

122. Defendant appreciates or has knowledge of such benefit

**ANSWER:** comScore denies the allegations of paragraph 122.

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.

**ANSWER:** The allegations set forth in paragraph 123 assert conclusions of law to which no response is required. To the extent paragraph 123 may purport to assert allegations of fact to which a response may be required, comScore states that the legal principles cited by Plaintiffs speak for themselves, and comScore denies any characterization of the laws applicable to this case that is inconsistent with those principles. Except as specifically admitted, comScore denies each and every allegation contained in this paragraph.

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.

**ANSWER:** comScore admits that Plaintiffs purport to seek the relief requested in paragraph 124. Except as otherwise expressly admitted herein, comScore denies the allegations of paragraph 124.

**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.

**ANSWER:** comScore denies that Plaintiffs are entitled to a judgment or to any other relief as requested in their "PRAYER FOR RELIEF."

**SEPARATE AND ADDITIONAL DEFENSES**

comScore asserts the following separate and additional defenses to Plaintiffs' Complaint, without assuming the burden of proof on such defenses that would otherwise fall on Plaintiffs. comScore reserves the right to supplement or amend these defenses as discovery is conducted, and does not knowingly or intentionally waive any applicable separate and additional defense. comScore reserves all other affirmative defenses pursuant to Rule 8(c) of the Federal Rules of Civil Procedure, the Patent Laws of the United States, and any other defenses, at law or in equity, that now exist or in the future may be available based on discovery and further factual investigation in this case.

**First Separate and Additional Defense**
**(Venue)**

1. Plaintiff entered into an agreement with comScore that contains a binding forum selection clause providing for exclusive venue in Virginia state court or the Eastern District of Virginia.

**Second Separate and Additional Defense**
**(Waiver)**

2. The Complaint and the claims asserted therein are barred by the doctrine of waiver.

**Third Separate and Additional Defense**
**(Failure to Mitigate Damages)**

3. Plaintiffs failed to properly mitigate their alleged damages by, among other things: (1) failing to remove comScore's software through the Windows Add/Remove programs utility, which is the industry standard, rather than purchasing unnecessary antivirus software; (2) failing to review comScore's FAQ and Privacy Policy, which would have quickly and expressly informed them how to remove comScore's software; and (3) objectively manifesting their assent to the installation of comScore's software, and to comScore's TOS and Privacy Policy, when that was apparently not their intention.

**Fourth Separate and Additional Defense**
**(Statute of Limitations and Laches)**

4. Plaintiffs define the putative class to include individuals that fall outside the applicable statute of limitations and/or whose claims are barred by the doctrine of laches

**PRAYER FOR RELIEF**

Wherefore, comScore prays for relief and judgment as follows:

1. That the Court deny Plaintiffs' prayer for relief in its entirety and that the Court dismiss the Complaint with prejudice and enter judgment in comScore's favor and against Plaintiffs;

2. That the Court award comScore its costs and expenses that it incurs in this action

and attorneys' fees as permitted by law; and

3. That the Court award comScore such other and further relief that it deems appropriate.

**Jury Demand**

Defendant demands a jury trial of all issues so triable.

Dated: December 13, 2011

Respectfully submitted,

By: /s/ Whitty Somvichian
Michael G. Rhodes (*admitted pro hac vice*)
Whitty Somvichian (*admitted pro hac vice*)
Ray Sardo (*admitted pro hac vice*)
COOLEY LLP
101 California Street, 5th Floor
San Francisco, CA 94111
Telephone: (415) 693-2000
rhodesmg@cooley.com
wsomvichian@cooley.com
rsardo@cooley.com

By: /s/ Paul F. Stack
Paul F. Stack
Mark W. Wallin
STACK & O'CONNOR CHARTERED
140 South Dearborn Street, Suite 411
Chicago, IL 60603
Telephone: (312) 782-0690
Facsimile: (312) 782-0936

Attorneys for Defendant comScore, Inc.

**Certificate of Service**

I hereby certify that on December 13, 2011, I electronically filed the foregoing document with the Clerk of Court using the CM/ECF system, which will send notifications of such filings to the following:

**Attorneys for Plaintiffs**
Jay Edelson
William Charles Gray
Steven W. Teppler
Ari Jonathan Scharg
EDELSON McGUIRE, LLC
350 North LaSalle, Suite 1300
Chicago, Illinois 60654
Telephone : (312)589-6370
jedelson@edelson.com
wgray@edelson.com
ascharg@edelson.com
steppler@edelson.com

Respectfully submitted,

By: /s/ Whitty Somvichian
Michael G. Rhodes,(*admitted pro hac vice*)
Whitty Somvichian, (*admitted pro hac vice*)
Ray Sardo,(*admitted pro hac vice*)
COOLEY LLP
101 California Street, 5th Floor
San Francisco, CA 94111
Telephone: (415) 693-2000
mrhodesmg@cooley.com
wsomvichian@cooley.com
rsardo@cooley.com

By: /s/ Paul F. Stack
Paul F. Stack
Mark W. Wallin
STACK & O'CONNOR CHARTERED
140 South Dearborn Street, Suite 411
Chicago, IL 60603
Telephone: (312) 782-0690
Facsimile: (312) 782-0936

Attorneys for Defendant comScore, Inc.