UNITED STATES DISTRICT COURT
DISTRICT OF CONNECTICUT

ROBERT DOGGA and JOSE BERMUDEZ, Individually and on Behalf of All Others Similarly Situated,

Plaintiffs,

vs.

GOOGLE, INC.,

Defendant.

JURY TRIAL DEMANDED

COMPLAINT

Plaintiffs Robert Dogga and Jose Bermudez ("Plaintiffs"), by and through undersigned counsel, as and for their Complaint, allege the following based upon personal knowledge as to allegations regarding the Plaintiffs and on information and belief as to all other allegations.

NATURE OF THE ACTION

1. Plaintiffs bring this action on behalf of themselves and a proposed class of similarly situated individuals ("Class Members"), who were victims of unfair, deceptive, and unlawful business practices.

2. Plaintiffs' and the Class Members' privacy, financial interests, and security rights were violated by Defendant Google ("Google" or "Defendant"), that acted individually, and in concert with entities involved in whole, or part, with advertising networks, data exchanges, traffic measurement service providers, and marketing and analytic service providers that develop and service websites (hereinafter "Google Affiliates"), to gain unauthorized access to, and use and retention of, Plaintiffs' and Class Members' data contained within their computing devices, which includes computers and mobile electronic devices used for communication, Internet, and multimedia capabilities ("Computing Devices").

3. Without disclosure to consumers, and without their permission, Defendant inserted code into its Google Ads that deactivated the security protections built into the Apple Safari Internet web browser ("Safari") and enabled tracking cookies (described below) to be installed on Safari-using consumers' Computing Devices.

4. Defendant used Plaintiffs' and Class Members' Computing Devices to access, retain, and disclose personal information, personally identifiable information, and/or sensitive identifiable information derived from Plaintiffs' and Class Members' Computing Devices while they browsed online or wirelessly. Defendant accomplished this covertly, without actual notice, awareness, or consent and choice, and which information Defendant obtained deceptively, for purposes which included Defendant's commercial gain.

5. Defendant individually, and in concert with Google Affiliates, has been systematically engaged in and facilitated a covert operation of surveillance of Class Members and the following:

1) Violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030;

2) Violations of the Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq.*;

3) Violations of the Connecticut Computer Crime Recovery Law, Connecticut General Statutes § 53-452 *et seq.*;

4) Violations of the Connecticut Computer-Related Offenses Law, Connecticut General Statutes § 52-570b *et seq.*;

5) Violations of the Connecticut Unfair Trade Practices Act, Connecticut General Statutes §§ 42-110a *et seq.*;

6) Conversion; and

7) Unjust Enrichment.

JURISDICTION AND VENUE

6. This Court has diversity jurisdiction over this matter under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). This Complaint states claims on behalf of a national class of consumers who are minimally diverse from Defendant. The amount in controversy exceeds $5 million, exclusive of interest and costs. The class consists of more than one hundred members.

7. This Court also has federal question jurisdiction under 28 U.S.C. § 1331 as this action arises, in part, under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and the Electronic Communications Privacy Act, 18 U.S.C. § 2510.

8. This Court has supplemental jurisdiction with respect to the pendent state law claims under 28 U.S.C. § 1367.

9. This Court has personal jurisdiction over Defendant because some of the acts alleged herein were committed in the State of Connecticut and because Defendant systematically and continuously conducts business here.

10. Venue is proper in this district pursuant to 28 U.S.C. §1391(a), in that, *inter alia*, a substantial part of the events giving rise to the claims herein occurred in the State of Connecticut. Plaintiffs reside, and at all relevant times resided, in Connecticut.

PARTIES

11. Plaintiff Robert Dogga is a resident of Fairfield County, Connecticut.

12. At all relevant times, Plaintiff Dogga owned an Apple iPhone and MacBook that use the Safari web browser.

13. Within the past year, Plaintiff Dogga has used his iPhone and MacBook to visit the Google website and has viewed ads on various websites, including, among others, youtube.com, gmail.com, googlemaps.com, and blogger.com. On information and belief, visiting these websites allowed Google's tracking cookies to be placed on Plaintiff Dogga's iPhone and MacBook without

appropriate authorization and, as a result, Google obtained, again without appropriate authorization, from Plaintiff Dogga's iPhone and MacBook, information pertaining to the websites that he visited.

14. Plaintiff Jose Bermudez is a resident of New Haven County, Connecticut.

15. At all relevant times, Plaintiff Bermudez owned an Apple iPod Touch that uses the Safari web browser.

16. Within the past year, Plaintiff Bermudez has used his iPod Touch to visit the Google website and has viewed ads on various websites, including, among others, drugstore.com, amazon.com, and expedia.com. On information and belief, visiting these websites allowed Google's tracking cookies to be placed on Plaintiff Bermudez's iPod Touch without appropriate authorization and, as a result, Google obtained, again without appropriate authorization, from Plaintiff Bermudez's iPod Touch, information pertaining to the websites that he visited.

17. Defendant Google, Inc. is a publicly traded Delaware corporation headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. Google does business throughout the United States and worldwide.

FACTS COMMON TO ALL CLAIMS

18. A cookie is a small text file that a website sends to a user's computer, where it is stored on the hard drive of a Computing Device. Web page servers generate cookies, and the information the cookie contains is set by the server and can be used by that server whenever the user visits the site. Cookies enable web sites to monitor their users' web surfing habits and profile them for marketing purposes. More specifically, cookies can be described as follows:

> Cookies are pieces of information generated by a web server and stored in the user's computer, ready for future access. Cookies are embedded in the HTML [*i.e.*, Hypertext Markup Language] information flowing back and forth between the user's computer and the servers. Cookies were implemented to allow user-side customization of Web information. For example, cookies are used to personalize Web search engines, to allow users to participate in WWW-wide contests (but only once!), and to store shopping lists of items a user has selected while browsing through a virtual shopping mall.

> Essentially, cookies make use of user-specific information transmitted by the Web server onto the user's computer so that the information might be available for later access by itself or other servers. In most cases, not only does the storage of personal information into a cookie go unnoticed, so does access to it. Web servers automatically gain access to relevant cookies whenever the user establishes a connection to them, usually in the form of Web requests.
>
> Cookies are based on a two-stage process. First the cookie is stored in the user's computer without their consent or knowledge. For example, with customizable Web search engines like My Yahoo!, a user selects categories of interest from the Web page. The Web server then creates a specific cookie, which is essentially a tagged string of text containing the user's preferences, and it transmits this cookie to the user's computer. The user's Web browser, if cookie-savvy, receives the cookie and stores it in a special file called a cookie list. This happens without any notification or user consent. As a result, personal information (in this case the user's category preferences) is formatted by the Web server, transmitted, and saved by the user's computer.
>
> During the second stage, the cookie is clandestinely and automatically transferred from the user's machine to a Web server. Whenever a user directs her Web browser to display a certain Web page from the server, the browser will, without the user's knowledge, transmit the cookie containing personal information to the Web server (hosted with any web hosting provider).

http://www.cookiecentral.com/c_concept.htm.

19. Google is the owner and operator of the website located at http://www. Google.com, and is a provider of advertising services through doubleclick.net. Google describes itself as "a global technology leader focused on improving the ways people connect with information." *See* http://investor.google.com/corporate/faq.html#toc-located. Further, according to Google: "Google primarily generates revenue by delivering relevant, cost-effective online advertising. Businesses use our AdWords program to promote their products and services with targeted advertising. In addition, third-parties that comprise our Google network use our Google AdSense program to deliver relevant ads that generate revenue and enhance the user experience." *Id.*

20. Safari is an Internet web browser offered by Apple, Inc., that is pre-installed on Computing Devices – including computers (such as the Mac) and mobile electronic devices (such as the iPhone, iPad, and iPod Touch) – used for communication, Internet, and multimedia capabilities.

To protect consumers' privacy, Safari's default settings block tracking the behavior of its users, which includes blocking third-party cookies.

21. On February 17, 2012, Jonathan Mayer, a Stanford researcher, published a study, "Web Policy- Do Not Track, Measurement, Privacy," that revealed the Defendant was intentionally circumventing and exploiting the Safari privacy features:

> Apple's Safari web browser is configured to block third-party cookies by default. We identified four advertising companies that unexpectedly place trackable cookies in Safari. Google and Vibrant Media intentionally circumvent Safari's privacy feature. Media Innovation Group and PointRoll serve scripts that appear to be derived from circumvention example code. . . .
>
> Some companies track the cookies generated by the websites you visit, so they can gather and sell information about your web activity. Safari is the first browser that blocks these tracking cookies by default, better protecting your privacy. Safari accepts cookies only from the current domain. . . .
>
> These allowances in the Safari cookie blocking policy enable three potentially undesirable behaviors by advertising networks, analytics services, social widgets, and other 'third-party websites.' If a company operates both a first-party website and a third-party website from the same domain, visitors to the first-party website will be open to cookie-based tracking by the third-party service. . . .
>
> Separating first-party websites from third-party services improves security: interactions between google.com content and other websites could introduce vulnerabilities. The domain separation also benefits user privacy: Google associates user account information with google.com cookies. By serving its third-party services from other domains, Google ensures it will not receive google.com cookies, and therefore will not be able to trivially identify user activities on other websites.

"Web Policy" (last accessed on: February 21, 2012), available online at: http://webpolicy.org/2012/02/17/safari-trackers/.

22. Prior to the publication of Mayer's research, Defendant provided browser instructions for Safari users: "Safari is set by default to block all third-party cookies. If you have not changed those settings, this option effectively accomplishes the same thing as setting the [Google advertising cookie opt-out plugin]."

23. This representation was false, as Defendant actively circumvented Safari privacy settings.

24. Defendant has since removed the foregoing language from its webpage.

25. Plaintiffs and Class Members demand that Defendant return their Computing Devices to the state that in which they existed prior to any and all activity implemented by Defendant and Google Affiliates. Such a demand is premised on the fact that, even if Defendant has ceased setting the cookies, Defendant may still continue its tracking practices using such tracking mechanisms. Plaintiffs' and Class Members' Computing Devices are at risk, and Plaintiffs and Class Members do not desire to accept such a risk.

26. Plaintiffs and Class Members use their Computing Devices' cache to store and use data, including, but not limited to, files of interest, website passwords, and bookmarks. Plaintiffs and Class Members do not want to use the Computing Devices' software to delete their entire cache but only that data within their hardware associated with Defendant and Google Affiliates.

CLASS ACTION ALLEGATIONS

27. Plaintiffs bring this action pursuant to Fed. R. Civ. P. 23(a), and (b)(1), (b)(2) and/or (b)(3) on behalf of themselves and the following class:

> All persons in the United States who purchased or owned a Computing Device with a Safari web browser installed on it, which was subjected to the Google code that circumvented Safari's third-party cookie blocking feature and placed tracking cookies on their Computing Devices.

28. The Class Period is defined as the time period applicable under the claims to be certified.

29. Excluded from the Class are Defendant, its assigns, and successors, legal representatives, and any entity in which Defendant has a controlling interest.

30. Plaintiffs reserve the right to revise this definition of the Class based on facts learned as litigation progresses.

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

32. The claims of Plaintiffs are typical of the claims of all other Class Members.

33. Plaintiffs will fairly and adequately represent the interests of the Class. 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 Class and have the resources to do so. Neither Plaintiffs nor their counsel has any interests adverse to those of the Class.

34. Absent a class action, most Class Members would find the cost of litigating their claims to be prohibitive and would 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.

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

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

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

a. What was the extent of Defendant's business practice of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and

remotely store users' data?

b. What information did Defendant collect from its business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data, and what did it do with that information?

c. Whether users, by virtue of visiting websites with Defendant's tracking mechanisms, had pre-consented to the operation of Defendant's business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data;

d. Was there adequate notice, or any notice, of the operation of Defendant's business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data provided to Plaintiffs and Class Members?

e. Was there reasonable opportunity to decline the operation of Defendant's business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data provided to Plaintiffs and Class Members?

f. Did Defendant's business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data disclose, intercept, and transmit personal information?

g. Whether Defendant devised and deployed a scheme or artifice to defraud or conceal from Plaintiffs and the Class Members Defendant's ability to, and practice of, circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data, for its own benefit, personal information, and tracking data from Plaintiffs' and the Class Members' Computing Devices via the ability to track their data on their Computing Devices;

h. Whether Defendant engaged in deceptive acts and practices in connection with its undisclosed and systemic practice of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data on Plaintiffs' and the Class Members' Computing Devices and using that data to track and profile Plaintiffs' and the Class Members' Internet activities and personal habits, proclivities, tendencies, and preferences for Defendant's use and benefit;

i. Did the implementation of Defendant's business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data violate the Computer Fraud and Abuse Act, 18 U.S.C. §

1030?

j. Did the implementation of Defendant's business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data violate the Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq.*?

k. Did the implementation of Defendant's business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data violate the Connecticut Computer-Related Offenses Law, Connecticut General Statutes § 52-570b and 53a-251 *et seq.*?

l. Did the implementation of Defendant's business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data violate the Connecticut Computer Crime Recovery Law, Connecticut General Statutes § 53-452 *et seq.*?

m. Did the implementation of Defendant's business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data violate the Connecticut Unfair Trade Practices Act, Connecticut General Statutes § §§ 42-110a *et seq.*?

n. Did the implementation of Defendant's business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data constitute unlawful Conversion?

o. Did the implementation of Defendant's business practices of circumventing users' Computing Device security settings to transmit, access, collect, monitor, and remotely store users' data result in Unjust Enrichment?

p. Whether Defendant participated in and/or committed or is responsible for violation of law(s) complained of herein;

q. Are Class Members entitled to damages as a result of the implementation of Defendant's conduct, and, if so, what is the measure of those damages?

r. Whether Plaintiffs and Class Members have sustained damages as a result of Defendant's conduct, and, if so, what is the appropriate measure of damages;

s. Whether Plaintiffs and Class Members are entitled to declaratory and/or injunctive relief to enjoin the unlawful conduct alleged herein; and

t. Whether Plaintiffs and Class Members are entitled to punitive damages, and, if so, in what amount?

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

39. Based on the foregoing allegations, Plaintiffs' legal theories for relief include those set forth below.

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

40. Plaintiffs repeat and reallege each and every allegation contained above as if fully set forth herein.

41. Plaintiffs' and the Class Members' Computing Devices are computers used in and affecting interstate commerce and communication and are therefore "protected computers" as defined in the Computer Fraud and Abuse Act (the "CFAA"), 18 U.S.C. § 1030(e)(2).

42. Defendant violated the CFAA, 18 U.S.C. § 1030(a)(4) in that it knowingly and with intent to defraud, accessed the protected Computing Devices of Plaintiffs and the Class Members without authorization, or exceeding authorized access, and by means of such conduct, furthered the intended fraud and obtained things of value.

43. As described above, Defendant surreptitiously gained access to, and placed persistent cookies onto, Plaintiffs' and Class Members' Computing Devices.

44. Defendant acted without authorization or exceeding authorization in that the Plaintiffs and the Class Members did not give Defendant permission or consent to place persistent cookies on their Computing Devices. In fact, they reasonably believed that Safari would block such cookies from being placed on their Computing Devices or downgrade such cookies to the status of session cookies.

45. Defendant's conduct was done knowingly and with intent to defraud and for the purpose of circumventing the cookie-filtering functions of Plaintiffs' and the Class Members' browsers.

46. Through Defendant's conduct it was able to further its intended fraud of placing persistent cookies on Plaintiffs' and Class Members' Computing Devices and using such cookies to collect and maintain Plaintiffs' and Class Members' personal information, and to share that information with third parties without the knowledge, consent, or authorization of Plaintiffs and Class Members.

47. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered harms and losses that include those described above.

48. Defendant's unlawful access to Plaintiffs' and Class Members' Computing Devices constituted a single act that resulted in an aggregated loss to the Plaintiffs and the Class Members of at least $5,000 within a one-year period.

49. Therefore, Plaintiffs and the Class Members are entitled to compensatory damages.

50. In addition, Defendant's unlawful access to Plaintiffs' and Class Members' Computing Devices has caused Plaintiffs and Class Members irreparable injury.

51. Unless restrained and enjoined, Defendant will continue to commit such acts. Plaintiffs' and Class Members' remedy at law is not adequate to compensate them for these inflicted, imminent, threatened, and continuing injuries, entitling Plaintiffs and the Class Members to remedies including injunctive relief as provided by 18 U.S.C. § 1030(g).

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

52. Plaintiffs repeat and reallege each and every allegation contained above as if fully set forth herein.

53. The Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510 *et seq.*, ("ECPA"), regulates wire and electronic communications interception and interception of oral communications, and makes it unlawful for a person to "willfully intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication," within the meaning of 18 U.S.C. § 2511(1).

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

55. At all relevant times, Defendant engaged in business practices of intercepting the Plaintiffs' and Class Members' electronic communications, which included endeavoring to intercept the transmission of a user's Computing Devices' activities and interactions between the user and its contact online from within their Computing Devices. Once Defendant obtained the data, it used such to aggregate Computing Device data of the Plaintiffs and Class Members as they used their Computing Devices.

56. The contents of data transmissions from and to Plaintiffs' and Class Members' Computing Devices constitute "electronic communications" within the meaning of 18 U.S.C. § 2510.

57. Plaintiffs and Class Members are "person[s] whose … electronic communication is intercepted … or intentionally used in violation of this chapter" within the meaning of 18 U.S.C. § 2520.

58. Defendant violated 18 U.S.C. § 2511(1)(a) by intentionally intercepting, endeavoring to intercept, or procuring any other person to intercept or endeavor to intercept Plaintiffs' and Class Members' electronic communications.

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

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

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

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

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

64. ECPA, 18 U.S.C. § 2520(a) provides a civil cause of action to "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used" in violation of the ECPA.

65. Defendant is liable directly and/or vicariously for this cause of action. Plaintiffs and Class Members therefore seek remedy as provided for by 18 U.S.C. § 2520, including such preliminary and other equitable or declaratory relief as may be appropriate, damages consistent with

subsection (c) of that section to be proven at trial, punitive damages to be proven at trial, and a reasonable attorney's fee and other litigation costs reasonably incurred.

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

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

COUNT III
Violations of Connecticut General Statutes § 53-452(a)
Computer Crime Recovery

68. Plaintiffs repeat and reallege each and every allegation contained above as if fully set forth herein.

69. Connecticut General Statute § 53-452(a) creates a private right of action in favor of any person aggrieved or injured by the commission of a computer crime. C.G.S.A. § 53- 452(a).

70. Under Connecticut law, the computer crime of unauthorized use of a computer or computer network occurs when "any person . . . use[s] a computer or computer network without authority and with the intent to . . . (6) [m]ake or cause to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data . . . residing in, communicated by or produced by a computer or computer network . . . ." C.G.S.A. § 53- 451(b).

71. As described herein, Defendant has repeatedly, knowingly, intentionally, and without permission, used Plaintiffs' and the Class Members' Computing Devices located in Connecticut and

has transmitted, accessed, collected, monitored, and remotely stored Plaintiffs' and the Class Members' data, in violation of § 53-451(b).

72. Plaintiffs and the Class Members have been injured as a result of Defendant's violation of § 53-451(b).

73. Pursuant to Conn. Gen. Stat. § 53-452, Plaintiffs are entitled to a Court Order enjoining further violations and awarding damages sustained by reason of Defendant's actions, plus costs, as well as an Order awarding any other remedies Plaintiffs may have available under applicable law.

COUNT IV
Violations of Connecticut General Statutes § 52-570b
Computer-Related Offenses

74. Plaintiffs repeat and reallege each and every allegation contained above as if fully set forth herein.

75. Connecticut General Statute § 52-570b creates a private right of action in favor of any person aggrieved or injured by the commission of a computer-related offense. C.G.S.A. § 52-570b(a), (c).

76. Under Connecticut law, the computer-related offense of unauthorized access to a computer system occurs when, "knowing that he is not authorized to do so, [a person] accesses or causes to be accessed any computer system without authorization." C.G.S.A. § 53a-251(b). The computer-related offense of misuse of computer system information occurs when, "(1) [a]s a result of his accessing or causing to be accessed a computer system . . . [a person] intentionally makes or causes to be made an unauthorized display, use, disclosure or copy, in any form, of data residing in, communicated by or produced by a computer system; or (2) he intentionally or recklessly and without authorization . . . takes data intended for use by a computer system, whether residing within or external to a computer system, or . . . intercepts . . . data residing within a computer system; or (3)

he knowingly receives or retains data obtained in violation of subdivision (1) or (2) of this subsection; or (4) he uses or discloses any data he knows or believes was obtained in violation of subdivision (1) or (2) of this subsection." C.G.S.A. § 53a-251(e).

77. Defendant has repeatedly, knowingly, intentionally, and without permission, used Plaintiffs' and the Class Members' Computing Devices located in Connecticut and has transmitted, accessed, collected, monitored, and remotely stored Plaintiffs' and the Class Members' data, in violation of Section 53a-251(b) and (e).

78. Defendant's actions were willful and malicious.

79. Plaintiffs and the Class Members have been injured as a result of Defendant's violation of Section 53a-251(b) and (e).

80. Pursuant to Conn. Gen. Stat. § 52-570b, Plaintiffs are entitled to an Order temporarily and permanently restraining and enjoining the continuance of such violation, restitution, actual damages, damages for unjust enrichment, statutory damages, treble damages, costs and attorneys' fees.

COUNT V
Violations of Connecticut General Statutes §§ 42-110a, *et seq.*
The Connecticut Unfair Trade Practices Act ("CUTPA")

81. Plaintiffs repeat and reallege each and every allegation contained above as if fully set forth herein.

82. The actions of the Defendant alleged herein were carried out in the conduct of its primary business described above.

83. The actions of the Defendant alleged herein violated CUTPA in that they constituted unfair acts and/or deceptive practices prohibited by CUTPA.

84. Defendant's acts and/or practices were unfair and/or deceptive, in part, because they violate Connecticut Regulation 42-110b-18, which prohibits false advertising, in that they were

untrue and misleading statements relating to Defendant's performance of services, made with the intent to induce consumers to enter into obligations relating to such services, and regarding which statements Defendant knew, or which by the exercise of reasonable care Defendant should have known, to be untrue and misleading. Defendant's acts and practices are also unfair and/or deceptive in that they violate Connecticut General Statutes §§ 53-452(a) and 52-570b.

85. The actions of the Defendant alleged herein were unfair in that they offended public policy or within at least the penumbra of common laws or statutes and/or other established concepts of unfairness, were immoral, unethical, oppressive, or unscrupulous.

86. The actions of the Defendant alleged herein were done with a reckless indifference to the rights of Plaintiffs or were an intentional and wanton violation of those rights.

87. Plaintiffs and the Class Members suffered ascertainable loss of money or property as a result of Defendant's unfair acts and/or deceptive practices – specifically, personal information, cleanup costs, and/or bandwidth costs.

COUNT VI
Conversion

88. Plaintiffs repeat and reallege each and every allegation contained above as if fully set forth herein.

89. Plaintiffs' and Class Members' Computing Device data, including, but not limited to, their Computing Devices' online usage data, is being used by Defendant to obtain personal information derived from Plaintiffs' and Class Members' Computing Device browsing activities. Such property, owned by the Plaintiffs and Class Members, is valuable to the Plaintiffs and Class Members.

90. Plaintiffs' and Class Members' Computing Devices use bandwidth. Defendant's activities, made the basis of this action, used without notice or authorization such bandwidth for purposes not contemplated nor agreed to by Plaintiffs and Class Members when they visited

websites containing Defendant's tracking mechanisms. Such property, owned by the Plaintiffs and Class Members, is valuable to the Plaintiffs and Class Members.

91. Defendant unlawfully assumed and exercised ownership over said property to the exclusion of the Plaintiffs' and Class Members' rights, and thereby converted Plaintiffs' and Class Members' property, by providing personal information to third parties and by using Plaintiffs' and Class Members' bandwidth for data mining, in violation of collective class allegations, made the basis of this action.

92. Plaintiffs and Class Members were damaged thereby.

COUNT VII
Unjust Enrichment

93. Plaintiffs repeat and reallege each and every allegation contained above as if fully set forth herein.

94. Defendant received a benefit from the Plaintiffs and the Class Members for which they did not pay to the detriment of the Plaintiffs and the Class Members. On information and belief, Defendant, directly or indirectly, has received and retained information regarding Plaintiffs and Class Members that is otherwise private, confidential, and not of public record, and/or has received revenue from the use and provision of such information.

95. Defendant appreciates or has knowledge of said benefit.

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, pray for an Order:

A. Certifying this matter as a class action under Rule 23 of the Federal Rules of Civil Procedure, and certifying Plaintiffs Robert Dogga and Jose Bermudez as Class Representatives, and designating their counsel as counsel for the Class;

B. Entering judgment in favor of Plaintiffs and the Class;

C. Awarding Plaintiffs and Class Members damages, in amounts to be proved at trial;

D. Awarding Plaintiffs and Class Members statutory damages;

E. Awarding Plaintiffs and Class Members treble damages under the applicable statutes;

F. Awarding Plaintiffs and Class Members exemplary or punitive damages;

G. Awarding disgorgement of monies obtained through and as a result of unfair and/or deceptive acts and/or practices, in amounts to be proved at trial;

H. Awarding Plaintiffs and Class Members pre- and post-judgment interest;

I. Awarding Plaintiffs and Class Members reasonable expenses and attorneys' fees; and

J. Awarding such other and further relief as equity and justice may require.

JURY DEMAND

Plaintiffs demand a trial by jury.

Dated: July 17, 2012
Greenwich, Connecticut

COHEN LAW GROUP, P.C.

By: **___/s/ Brian S. Cohen_____**

Brian S, Cohen, Esq.
Federal Juris No.: CT18878
2 Greenwich Office Park - Suite 300
Greenwich, CT 06831
Phone: 203-485-7525
Fax: 203-485-7526
E-Mail: brian@cohenlg.com

Attorneys for Plaintiffs