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, v. COMSCORE, INC., a Delaware corporation, Defendant.	Case No. 1:11–cv–5807 Hon. James F. Holderman Magistrate Judge Young B. Kim

PLAINTIFFS' MEMORANDUM OF LAW
IN SUPPORT OF THEIR MOTION FOR PARTIAL SUMMARY JUDGMENT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

UNITED STATES CIRCUIT COURT OF APPEALS CASES:

UNITED STATES DISTRICT COURT CASES:

STATUTES:

MISCELLANEOUS:

I. INTRODUCTION

comScore, Inc.'s ("comScore") liability in this matter turns on whether it obtained consent to collect data from Class members' computers through its tracking software, OSSProxy, and if it did, whether comScore's data collection exceeded the scope of the consent obtained. The Court has recognized as much—noting that, because "consent" or "authorization"[1] is central to their claims, "[P]laintiffs need prove only one incident of OSSProxy exceeding the scope of the consent to establish violations of the ECPA, the SCA, and the CFAA." (Dkt. 186 at 11.)

In this case, both Parties agree that every issue of consent turns on the "terms and conditions" of the User License Agreement (the "ULA") that accompanies OSSProxy's installation and operation. comScore's position is that because each Class member accepted the ULA's terms and conditions during OSSProxy's installation, those terms control and show that OSSProxy's operation was authorized. (*See* Dkt. 175 at 7, 11.) As set forth in their Memorandum in Support of Class Certification (Dkt. 154 at 16), Plaintiffs Mike Harris and Jeff Dunstan ("Plaintiffs") do not dispute that they, along with each and every class member, clicked "accept" when presented with OSSProxy's "Downloading Statement"—which asked that users read and agree to the ULA's terms and conditions. That said, the issue of whether the ULA was actually binding on them (and the Class)—e.g., whether OSSProxy's "installation process uniformly fail[ed] to obtain . . . assent to the ULA"—is a question for another day and not one taken up in this motion.[2] (Dkt. 154 at 30.)

---

[1] Throughout this brief, Plaintiffs use the terms "authorization" and "consent" interchangeably, without limitation—i.e., in line with the language of the Stored Communications Act ("SCA"), Electronic Communications Privacy Act ("ECPA"), and Computer Fraud and Abuse Act ("CFAA"). Likewise, rather than repeatedly referring to comScore's "access" and/or "interception" of Plaintiffs' communications (i.e., in line with the SCA, ECPA, or both), Plaintiffs here use the broader term "collection" to reference comScore's alleged access to their computers and access and interception (or attempted access and interception) of their communications through OSSProxy.

[2] Indeed, this threshold question is particularly apt for Subclass members, who were never

Rather, Plaintiffs' motion establishes that *even if* the premise of comScore's position is correct and the ULA is binding on Plaintiffs and the Class, comScore's data collection was still unlawful. That point is demonstrated in two ways. First, if enforceable, the ULA granted limited rights to enumerated parties, but did not grant *comScore* any rights to collect data from the Class. Second, even if the ULA *did* grant comScore some right to collect data, comScore's collection still lacked authorization because the invasion comScore effectuated (i.e., through OSSProxy) was fundamentally different from the invasion supposedly authorized by the ULA's terms and conditions. All told, the ULA didn't grant comScore *any* data collection rights, but even if it did, those rights were limited to collection using means that comScore never employed. Plaintiffs are therefore entitled to summary judgment on the issues of consent and authorization.

Given the facts not in dispute, Plaintiffs seek partial summary judgment on the central issue of consent now—prior to the Parties engaging in expert discovery on the issue—so as to preserve the Court's and the Parties' resources by significantly narrowing the issues for expert testimony and discovery, future summary judgment briefing, and trial. Because Plaintiffs are entitled to summary judgment on the authorization elements and consent defenses for their claims under the SCA, ECPA, and CFAA[3], their Motion should be granted.

II. STATEMENT OF UNDISPUTED FACTS

By now, the Court is well aware of comScore's business model. comScore generates revenue by mining data from consumers across the world and then analyzing, repackaging, and selling it. (Plaintiffs' Local Rule 56.1 Statement of Undisputed Material Facts ("SOF") ¶ 11.)

---

presented with a functional hyperlink to the ULA and therefore can't be bound by it. (*See* Dkt. 31 at 4–5.)

[3] Both the CFAA and the SCA place the burden on Plaintiffs to establish that comScore's access occurred without, or in excess of, authorization. *See* 18 U.S.C. § 1030(a); 18 U.S.C. § 2701(a). The ECPA, on the other hand, puts the burden on comScore to prove the defense of consent. *See* 18 U.S.C. § 2511(2)(d); *see also Valentine v. WideOpen W. Fin., LLC*., 288 F.R.D. 407 (N.D. Ill. 2012) *reconsideration denied*, No. 09 C 7653, 2013 WL 5423846 (N.D. Ill. Sept. 27, 2013); *Doe v. Smith*, 429 F.3d 706, 709 (7th Cir. 2005).

While it acquires consumer data from a number of sources, comScore's reputation stems mainly from its online panel of consumers that—thanks to OSSProxy's constant monitoring—continually feeds comScore with data about consumers' online activity (e.g., who is shopping where, what credit cards they are using, what is being purchased, what online ads are being clicked on, etc.). (*Id.* ¶¶ 6, 44–46.) comScore isn't shy about the size and scope of its panel—it boasts that OSSProxy captures "over 1.5 Trillion [online] interactions . . . monthly; equal to almost 40% of the monthly page views of the entire internet." (*Id.* ¶ 12.)

A. Class Members Downloaded and Installed Bundled Versions of OSSProxy as Part of comScore's TAP Recruitment Scheme.

The entire Class was recruited to comScore's online panel via comScore's "third party application provider" program (the "TAP program"). (*Id.* ¶¶ 15, 20–21, 76–77.) Rather than recruiting consumers to voluntarily sign up for its panel directly—as it does for its "affiliate network" recruitment program[4]—comScore's TAP program requires that consumers download free applications (generally termed "freeware," such as screensavers, music programs, games, etc.) that have been "bundled" with OSSProxy.[5] (*Id.* ¶¶ 13–15, 22, 25.) comScore does not

---

[4] Unlike its TAP recruitment model, comScore's affiliate program is far less likley to result in unitentional installations of OSSProxy. Through the affiliate model, comScore pays partners to post Internet advertisements to increase traffic to comScore's panel websites (such as www.permissionresearch.com), where consumers can sign up for a panel directly. (SOF ¶¶ 13–14.) There, consumers are required to provide substantial personal information up front (such as their name, address, age, gender, and email address) *before* downloading and installing OSSProxy. (*Id.* ¶ 14.) And even though the sites are still "branded" and utilize program sponsors (similar to the TAP program), there's no element of surprise attendant to the downloading process.

[5] Many authorities take issue with the practice of "bundling"—i.e. offering bundled software along with free/trial programs—as a threshold matter because it (i) is not detected by most antivirus vendors, (ii) operates in the same manner as recognized "malicious" programs, and is, as such, (iii) fundamentally "based on deception." *See* Vyacheslav Zakorzhevsky, *Bundled software – grey market with dirty rules*, Kaspersky Lab: Security Analyst Summit 2013, *available at* http://media.kaspersky.com/en/Events/Presentations/Vyacheslav%20Zakorzhevsky_Bundled%20software%20-%20grey%20market%20with%20dirty%20rules.pdf (last accessed Feb. 20, 2014). How these issues operate with respect to bundled versions of OSSProxy will be a specific focus of expert discovery, and—should this motion be denied—will be a key issue at trial in determining the existence and scope of any consent given.

require its TAP partners to warn or otherwise disclose that OSSProxy is bundled with freeware before a consumer downloads it—indeed, comScore's own expert witness stated that he'd be "surprised" if such disclosures were ever made. (*Id.* ¶ 23.)

To install OSSProxy through comScore's TAP program, a user must initialize a bundled freeware's installation process and then click past the installation window for OSSProxy. (*Id.* ¶¶ 21–22, 24–25.) This process [redacted] (*Id.* ¶ 18.) To ensure the rapid and continuous installation of OSSProxy by consumers, [redacted] *Id.* ¶ 16.) Historically, "TAP panelists" [redacted] of comScore's panel. (*Id.* ¶ 17.) [redacted] (*Id.* ¶ 19.) Looking forward, many aspects of comScore's TAP recruitment model have drawn criticism among privacy experts and will be a key focus of expert testimony.[6] For the purposes of this motion, two aspects of the process are especially relevant:

The Downloading Statement. Over the course of a TAP bundle's installation, every TAP panelist (and every Class member) was presented with the Downloading Statement. (*Id.* ¶¶ 20–

[6] Likewise, expert testimony will show that several aspects of the TAP installation process were designed to—as one antivirus vendor described to comScore [redacted] S0082285_Confidential--Attorney's Eyes Only.docx, attached to the Declaration of Benjamin S. Thomassen ("Thomassen Decl.") as Exhibit 29.) Expert evaluation of the overall process will demonstrate the deceptive nature of comScore's TAP recruitment scheme and support Plaintiffs' view that—in light of that deceit—any consent obtained from Class members was vitiated. *See Theofel v. Farey-Jones*, 359 F.3d 1066, 1073–75 (9th Cir. 2003); *see also Desnick v. Am. Broad. Cos.*, 44 F.3d 1345, 1351–53 (7th Cir. 1995).

21, 24, 25.) The Downloading Statement contained (i) an abbreviated summary of the terms and conditions attendant to the download and use of OSSProxy and (ii) a hyperlink to the ULA containing the full terms and conditions.[7] (*Id.* ¶¶ 21, 24, 29.) The Downloading Statement also stated that a "branded" version of OSSProxy ("RelevantKnowledge" for most Class members) was presented "in order to provide" the freeware, and that OSSProxy was "provided by" a named program "Sponsor" ("TMRG, Inc." sponsored RelevantKnowledge). (*Id.* ¶¶ 9, 27, 36.)

The ULA. Following a short preamble, the hyperlinked-to ULA explained that "[b]efore joining [the panel] . . . and installing our application, you must review and agree to the terms and conditions below and provide and obtain consent to this agreement from anyone who will be using the computers on which you install the application." (*Id.* ¶ 37; Dkt. 156-9, attached to the Thomassen Decl. and cited herein as Ex. 4.) The ULA's terms and conditions set out that "[the] Agreement constitutes the entire agreement between sponsor and you with respect to the subject matter contained in the Agreement" and explained that "[the] agreement shall not create any rights or remedies in any parties other than the parties to the agreement and no person shall assert any rights as a third party beneficiary under this agreement." (SOF ¶ 43, Ex. 4 at 7.) Consistent with those restrictions, the terms and conditions encouraged users to contact the Sponsor's "Privacy Office" at specific postal and/or email addresses (e.g., privacy@tmrginc.com or support@tmrginc.com) with questions about OSSProxy or its terms and conditions. (SOF ¶ 42.)

B. If Enforceable, the ULA's Terms and Conditions Define the Nature and Scope of Any Class Member's Consent to Collection by OSSProxy.

Assuming *arguendo* that the Class members validly consented to the ULA, then every issue regarding their consent flows from the ULA's "terms and conditions." That's because:

(i) Every Class member was presented with a Downloading Statement prior

[7] As the Court knows, members of the Subclass did not receive a functional hyperlink. (SOF ¶ 32.)

to the installation of OSSProxy, (*Id.* ¶ 24);

(ii) Each Downloading Statement explained that "[b]y clicking Accept you acknowledge that . . . you have read, agreed to . . . the ***terms and conditions*** of the Privacy Statement and User License Agreement," (*Id.* ¶¶ 29, 31 (emphasis added));

(iii) Each Downloading Statement provided an active hyperlink labeled Privacy Statement and User License Agreement that, once clicked on, directed Class members to the ULA, (*Id.* ¶¶ 29–30);[8]

(iv) The linked-to ULA contained a section header containing the words "PRIVACY POLICY & USER LICENSE AGREEMENT," under which the ULA explained that "Before joining our program, enjoying the benefits of this program, and installing our application, you must review and agree to the ***terms and conditions below*** and provide and obtain consent to this agreement from anyone who will be using the computers on which you install this application," (*Id.* ¶ 37 (emphasis added)); and

(v) The "terms and conditions" section of the ULA explained, *inter alia*:

a. "What information [would be] collected," (e.g., what data would be collected wholesale versus data that was subject to "automatic[] filter[ing]") (Ex. 4 at 2–3; SOF ¶¶ 39–40;);

b. "How . . . the information [would be] collected," (e.g., the methods through which data was collected by OSSProxy, what collected data would be transmitted, and to whom that data would be sent) (Ex. 4 at 3–4; SOF ¶ 40);

c. "How . . . the collected information [would be] used," (e.g., how the collected data would be used to create "Market Research Reports" after "automatically filter[ing]" certain data) (Ex. 4 at 4; SOF ¶ 40); and

d. "How . . . the information [would be] secured," (e.g., how employees exposed to collected data would be "contractually restricted on their use and access to personally identifiable information," and how panelists could "access, modify, and/or request deletion" of certain data") (Ex. 4 at 4–5; SOF ¶ 40).

Per its own express and limiting language, the ULA's terms and conditions were the *only* place where panelists could have authorized OSSProxy's data collection. (SOF ¶ 43.) And per that

[8] Excepting, as explained above, members of the Subclass, who did not receive a link. (SOF ¶ 32.)

same language, the agreed-to data collection (i.e., what was consented to) extended *only to specific parties* and permitted *only* the conduct described. (*Id.*)

1. The ULA's terms and conditions limited who (if anyone) had rights to collect data from panelists, while its preamble named possible downstream users of the collected and anonymized data.

The ULA's terms and conditions were unequivocal about the parties authorized to collect data from panelists. The terms and conditions made clear that "[t]his Agreement constitutes the entire agreement between *sponsor and you*" and identified the program Sponsor by name (e.g., TMRG, Inc., for RelevantKnowledge). (Ex. 4 at 7–8; SOF ¶¶ 36, 43 (emphasis added).) Throughout, the terms and conditions made consistent use of personal pronouns to reference the program Sponsor—stating, for example, "[o]nce you install *our* application," "[*w*]*e* may use the information *we* monitor," and that if users had "any questions . . . [about] *our* practices" the Sponsor's "Privacy Office" should be contacted. (Ex. 4 at 7–8; SOF ¶ 42.) Indeed, the *Sponsor* is the only entity named in the ULA's terms and conditions, which additionally limited any rights granted to the named parties: "[t]his agreement shall not create any rights or remedies in any parties other than the parties to the agreement and no person shall assert any rights as a third party beneficiary under this agreement." (Ex. 4 at 7; SOF ¶¶ 38, 43.)

It's true that other parties were mentioned in the ULA's preamble (i.e., the short portion appearing before the identified "terms and conditions" that panelists were asked to review and assent to). (SOF ¶ 38.) There, and after explaining that panelists' data would be "passively collected and used as a part of anonymous research reports," the preamble mentioned downstream users of panelists' then-anonymized data. (Ex. 4 at 2; SOF ¶ 38.) comScore was mentioned as a user "of the information you contribute." (SOF ¶ 38.) Further downstream from comScore, the New York Times, the Wall Street Journal, and CNN were also identified as users of the data. (*Id*.) The preamble flagged that "the data [would also be] extensively used by the

largest Internet services companies and scores of Fortune 500 companies[.]" (*Id*.) Throughout the preamble, none of these "users" of collected data were referenced by a personal pronoun; instead, each was always identified by name and none appeared in the ULA's terms and conditions. (*Id.*)

2. The ULA's terms and conditions limited any authorized collection to collection performed by specific means.

In addition to explaining *who* would collect data through OSSProxy, the ULA's terms and conditions described *how* collection would occur. (Ex. 4 at 3–4; SOF ¶ 40.) Specifically, and rather than providing for unlimited monitoring by OSSProxy, the terms and conditions sought authorization for particular data collection practices. The most significant restriction on OSSProxy's collection was the promise of "commercially viable efforts to ***automatically filter confidential personally identifiable information*** [from collection,] such as UserID, password, credit card numbers, and account numbers." (Ex. 4 at 4; SOF ¶ 39 (emphasis added.)). With respect to the data that the ULA identified for collection, the commitment to collect data subject to automatic filtering of confidential personally identifiable information ("CPII") was the ULA's *only* commitment to safeguard panelists' privacy that was programmed into OSSProxy itself. (*See* Ex. 4.) All other privacy protections came from post-collection promises, such as the Sponsor's commitment to (i) "purge our database of [inadvertently collected CPII] information;" (ii) give panelists the ability to "access, modify, and/or request deletion of the personally identifiable profile information submitted by [panelists] as a part of this program;" and (iii) ensure that all data collected was anonymized before being used in "Market Research Reports" and distributed/sold to downstream users of that data.[9] (*Id.* at 3–4.)

[9] Though these post-collection protections are not the subject of the instant motion, it is not at all clear that comScore's data practices conformed to these provisions of the ULA either. Regarding the promise to "purge our database" of [inadvertently collected CPII] [redacted]

All told, the ULA's terms and conditions established that the panelists consented to be monitored (if at all) *only* through a specific type of data collection—by software programmed to automatically filter CPII.

C. OSSProxy's Design and Actual Data Collection Practices Differ Fundamentally From the Data Collection Guaranteed by the ULA.

Although not disclosed to consumers before (or even after) the ULA's terms and conditions were presented to them, the Sponsors had no role in the actual collection of data through OSSProxy. And the software itself—while programmed with the ability to automatically "filter" data before collecting it—was not programmed to automatically filter *any* CPII, but was designed instead to target and collect all of it. (SOF ¶¶ 47–53.)

1. comScore—rather than any program Sponsor—collected data from panelists via OSSProxy, packaged it, and generated revenue from it.

comScore—not any program Sponsor—is the only entity that collected panelist data through OSSProxy. (*Id.* ¶¶ 70–71.) comScore alone designed OSSProxy. (*Id.* ¶ 67.) comScore alone distributed OSSProxy to panelists, caused it to be installed and configured on panelists' computers, and actively maintained the software (e.g., by facilitating communications between its own servers and all installed iterations of OSSProxy). (*Id.* ¶¶ 68–69.) And of course, all data collected from panelists through OSSProxy went directly to comScore, after which comScore analyzed, packaged, and sold it through its various commercial products. (*Id.* ¶¶ 11, 70–71.)

2. Although it could have, comScore did not program OSSProxy to automatically filter CPII.

The undisputed facts also show that comScore did not program OSSProxy to

[redacted] (*Id.* ¶ 63.)

automatically filter *any* CPII—even though, by its design, OSSProxy was programmed to automatically filter other data from collection. (SOF ¶¶ 47–53.) As a result, and assuming *arguendo* that comScore had some authority to collect data, its undisclosed collection practices—where CPII was in fact targeted for collection—were inconsistent with the collection practices authorized by the ULA's terms and conditions. That OSSProxy did not automatically filter CPII is demonstrated in at least two ways.

a. Even comScore agrees that "fuzzification" is not filtering.

Rather than automatically filter CPII from its targeted collection, comScore collected it all (while attempting to "fuzzify" some) of it. (*Id.*) The Court will recall comScore's "fuzzification" process—through it, comScore programmed OSSProxy (using both programming hard-coded into the software itself, and external, regularly-updated "rule files") to (i) capture all CPII inputted by panelists (e.g., credit card numbers or passwords inputted into webpages during secure browsing sessions); (ii) identify it as CPII (e.g., by recognizing certain field names or patterns of data); (iii) obfuscate some of it; and (iv) transmit the "fuzzified" CPII to comScore's servers for processing, analysis, and eventual sale. (*Id.* ¶¶ 50, 53; Dkt. 154 at 13–14.) No one at comScore—not even its own proffered expert, Dr. Tamassia—describes the "fuzzification" process as "filtering." (SOF ¶¶ 51–53.) And comScore first pointed out this difference during class discovery when its Chief Technology Officer and Rule 30(b)(6) designee admitted that "filtering and fuzzifying are two different things." (*Id.* ¶ 51.)

The distinction makes sense, because OSSProxy *is* in fact programmed to automatically "filter" some data from its collection processes—it just isn't programmed to filter CPII. For example, comScore [redacted] (*Id.* ¶ 48.) Likewise, comScore programmed OSSProxy to automatically filter (i.e.,

exclude or exempt from collection) certain web content ("page data") accessed and viewed by panelists through web browsers—including, for example, page data from "dot-edu" (.edu) sites. (*Id.* ¶ 49). comScore took this action not because the ULA's terms and conditions represented that such data would be filtered from collection, but because it doesn't "want to collect" that data, has "no need for" it, and it is "not part of [comScore's] business model." (*Id.* ¶ 52.)

CPII, on the other hand—and far from being filtered, excluded, or exempted—is explicitly targeted for OSSProxy's collection. Indeed, analysis of CPII collected from panelists (e.g., social security numbers, credit card numbers, etc.) is key to the utility and value of comScore's data analytics products. (*Id.* at ¶ 53.)

b. comScore [redacted]

Even though it first identified the difference between filtering and fuzzifying, and even though [redacted] comScore still believes that its (publicly undisclosed) fuzzification logic is a suitable analogue to "filtering." But even if that were true, comScore doesn't even fuzzify as promised. That fact is demonstrated in at least three ways.

First, comScore uses (but does not publicly disclose) [redacted] *Id.* ¶¶ 54–56.)[10] [redacted]

[10] From a technical [redacted] (CS0096108_Confidential--Attorney's Eyes Only.docx, attached to the Thomassen Declaration as Exhibit 30.)

[redacted] *Id.* ¶¶ 55–57.)

Second, comScore [redacted] (*Id.* ¶¶ 39; 54–57.) For example [redacted] (*Id.* ¶¶ 39, 57–59.)

Third, comScore [redacted] (*Id.* ¶¶ 58–59.) With this information, [redacted] (*Id.* ¶¶ 58–62.) [redacted] a known minor, [redacted] Facebook.com "About" page [redacted] she set that webpage's security settings to

[11] Given these collection practices, it's unsurprising that comScore's Director of Software Engineering, Steven Chase, testified that, to his knowledge, [redacted] though "UserID" is the ULA's *first* enumerated example of CPII. (*Id.* ¶¶ 39, 64.)

"private," so as to hide certain information—including her birth year—from the public's view.[12] (*Id.* ¶ 61–62.) [redacted] (*Id.* ¶¶ 59, 61.)

All told, comScore's fuzzification of CPII is less of an automatic process triggered whenever CPII is detected, and more of a conditional one that comScore employs when CPII is detected [redacted] Given that functionality, fuzzification differs sharply from the ULA's promised "automatic CPII filtering."

Ultimately, the ULA's terms and conditions, which comScore insists are binding, provide for a very specific type of data collection: collection by the Sponsors using software that would make commercially viable efforts to automatically filter CPII from collection. In reality, the collection that took place was nothing like that described in the ULA. Instead, *comScore* did the collecting, and it did so using software that made no effort to filter CPII (though it did filter information less useful and valuable to comScore), and in some cases [redacted] As such, Plaintiffs never consented to the collection that actually occurred.

III. ARGUMENT

Because the undisputed facts show that comScore had no right to collect data from Class members' computers, Plaintiffs and the Class are entitled to partial summary judgment on the

[12] A user's Facebook_ID or Facebook Username, when added after the "www.facebook.com/" prefix, leads to that user's personal Facebook page (e.g., entering "www.facebook [redacted]

"authorization" element of their SCA and CFAA claims, and comScore's "consent" defense under the ECPA.[13] *See* 18 U.S.C. §§ 2701(a), 1030(a), 2511(2)(d). "A party claiming relief may move, with or without supporting affidavits, for summary judgment on all or part of the claim . . . at any time after . . . 20 days have passed from commencement of the action." Fed. R. Civ. P. 56(a)(1). Summary judgment is proper "if the pleadings, the discovery and disclosure materials on file, and any affidavits show that there is no genuine issue as to any material fact and that the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(c)(2).

Plaintiffs are entitled to partial summary judgment on the central issue in this case—whether they consented to *comScore's* collection of their data through OSSProxy. For each of their claims, the issues of consent and authorization are interpreted in light of the common law, especially the common law of trespass. *Theofel*, 359 F.3d at 1072–33. "Consent may be explicit or implied, but it must be actual consent rather than constructive consent . . . and should not be casually inferred." *In re Pharmatrak, Inc.*, 329 F.3d 9, 20 (1st Cir. 2003) (citing *Williams v. Poulos*, 11 F.3d 271, 281–82 (1st Cir. 1993); *United States v. Footman*, 215 F.3d 145, 155 (1st Cir. 2000); and quoting *Griggs-Ryan v. Smith*, 904 F.2d 112, 117 (1st Cir. 1990)) (internal quotations omitted).

Here, the undisputed facts show that comScore lacked consent for two reasons. First, *comScore* had no authorization to collect data from Plaintiffs' computers. The ULA's terms and conditions granted collection rights to, if anyone at all, *only* the Sponsors, while comScore had *no* such rights. Second, any collection rights granted by the ULA's terms and conditions authorized only a *specific* type of collection performed by software that automatically filtered CPII—a practice that was different from what comScore actually utilized. From either

[13] comScore did not raise "consent" as a defense in its Answer to the Second Amended Complaint. Thus, to the extent it has not waived it outright, Plaintiffs are still entitled to summary judgment on it.

perspective, comScore had no consent to collect data from Plaintiffs' computers using OSSProxy, and Plaintiffs are entitled to summary judgment on the issues of consent and authorization for each of their claims.

A. Under the ULA comScore Relies Upon to Establish Consent, It Had No Right to Access Plaintiffs' Computers or Communications.

comScore has repeatedly asserted that the ULA governs OSSProxy's operation, and that Plaintiffs consented to the collection provided under the ULA. (*See* Dkts. 15, 42-1, 175, 243, 302-1.) By its own text, however, the ULA gave comScore no right to access Plaintiffs' computers and communications, and instead limited any such right exclusively to the Sponsors.

It is hornbook law that consent may be limited to particular activities performed by particular individuals. *See* Restatement (Second) of Torts (hereinafter "Restatement") §§ 52, 892A. Thus, when an individual grants license to another to invade his interests or property, and an unauthorized individual invades instead, the invading individual has acted without consent and may be held liable as the law sees fit. *See* Restatement §§ 892A, 892B; *Thrasher-Lyon v. CCS Commercial, LLC*, No. 11-cv-04473, 2012 WL 3835089, at *5 (N.D. Ill. Sept. 4, 2012) (consent to receive calls from one person did not constitute consent to receive telemarketing calls from another); *Easterling v. Kopp*, No. 04-cv-615, 2005 WL 1630006, at *3 (E.D. Wis. July 7, 2005) *aff'd*, 168 F. App'x 100 (7th Cir. 2006) (holding that in fourth amendment context, an individual could limit consent to search to a particular person). And in cases like this, where a contract defines the scope of access, its terms define and limit the consent conferred. (*See* Dkt. 186 at 10.)

Here, the ULA, through its specifically identified "terms and conditions," defined any consent granted by Plaintiffs. (*See* Dkt. 186 at 10.) The ULA strictly limited any collection rights to *the Sponsors* by enumerating the types of collection the Sponsors could undertake. (*See* Ex. 4.)

In contrast, the ULA never identified comScore as a party that would monitor or collect panelists' data. (Ex. 4; SOF ¶ 38.) In fact, the ULA's "terms and conditions" didn't mention comScore at all. (Ex. 4; SOF ¶ 38.) Rather, comScore was *only* referenced in the ULA's non-binding preamble. (SOF ¶ 38); *see Atl. Mut. Ins. Co. v. Metron Eng'g and Const. Co.*, 83 F.3d 897, 900 (7th Cir. 1996) ("[I]ntroductory language or recitals are not binding obligations unless so referred to in the operative portion of the instrument as to show a design that they should form a part of it."). In the preamble, comScore was identified as one of several downstream users of the data "contribute[d]" by panelists—i.e., along with other entities described as "extensive[] use[rs]" of that same data. (SOF ¶ 38.) These clearly drawn distinctions between the Sponsors and comScore, along with the ULA's express limitation of collection rights to those parties specifically enumerated, (*see* Ex. 4 at 7 ("Third Party Rights" and "ENTIRE AGREEMENT" clauses limiting rights to panelists and Sponsors)), confirmed that Plaintiffs consented to, *at most*, the *Sponsors*' collection, and never agreed to any such activity by comScore.[14]

In reality, however, it was comScore who operated OSSProxy. (SOF ¶¶ 69–71.) The Sponsors had no role in accessing panelists' computers and communications, profiting from it, or deploying, updating, or maintaining OSSProxy. (*Id.* ¶¶ 67–71.) Thus, while Plaintiffs consented to one type of conduct (access and interception by the Sponsors), another (access and interception by comScore), occurred—undermining Plaintiffs' rights in their computers and private communications. (*See* Section II.B.1, *supra*.) *See Desnick*, 44 F.3d at 1352 (explaining that a party's misrepresentation regarding its identity to enter private property vitiates consent).

Accordingly, Plaintiffs never entered into *any* agreement with comScore, much less an

14 [redacted]

agreement to authorize its highly invasive tracking. And, therefore, comScore's access to and interception of Plaintiffs' communications occurred without authorization. *See* Restatement § 52, cmt. a, Ill. 1 ("A consents to an operation to be performed by B, a surgeon, whom A knows and in whom he has great confidence. After A is under a general anesthetic, the hospital substitutes C, another surgeon of equal skill. C performs the operation. C is subject to liability to A."); Restatement § 892A, cmt. e ("[O]ne who consents that another may walk across his land does not, without more, consent that . . . a third person may walk across it along with the other.").

Since Plaintiffs never authorized comScore to access their computers, their communications, or their personal information, they are entitled to summary judgment on the consent and authorization elements of their claims.

B. To the Extent They Agreed to be Bound by the ULA's Terms and Conditions, Plaintiffs *Only* Authorized Collection Performed by Software that Included and Employed Automatic CPII-Filtering Functionality.

Even if the ULA had given *comScore* some form of collection rights, its terms and conditions established that Plaintiffs *only* authorized collection using automatic CPII-filtering. Plaintiffs never consented to the collection that actually occurred, which comScore performed without *any* CPII-filtering mechanisms.

For consent to be effective, it "must be to the actor's conduct or to substantially the same conduct, rather than to the invasion that results from it." Restatement § 892A, cmt. e.; *accord* *Lloyd v. Kull*, 329 F.2d 168, 170 (7th Cir. 1964) (holding that physician's removal of non-threatening mole exceeded plaintiff's consent to "such operations as may be deemed necessary or advisable in [her] diagnosis or treatment"). Thus, where the conduct performed is not substantially the same as the conduct consented to, there is no consent. *See Desnick*, 44 F.3d at 1345; *see also* Restatement § 892A, cmt. e ("Consent to an invasion by particular conduct is not

consent to the same invasion by entirely different conduct."). As the Seventh Circuit has explained, "[i]f a homeowner opens his door to a purported meter reader who is in fact nothing of the sort—just a busybody curious about the interior of the home—the homeowner's consent to his entry is not a defense to a suit for trespass." *Desnick*, 44 F.3d at 1352.

Accordingly, in cases involving the invasion of property interests, like this one, the key question is whether the specific conduct that occurred was of the nature agreed to. *See id.* at 1352–53 (Defendants who posed as clinic patients for investigative purposes did not trespass, because their entry was not "an invasion . . . of any of the specific interests that the tort of trespass seeks to protect."); *see also* Restatement §§ 892A, 892B. Here, the ULA's terms and conditions, if enforceable at all, defined the conduct Plaintiffs authorized: data collection using software programmed to automatically filter CPII—nothing more and nothing else. (SOF ¶ 39; *see also* Dkt. 186 at 10 ("The scope of plaintiffs' consent here is determined by that identical [installation] process, the ULA, and the Downloading Statement.").) In its actual invasion of Plaintiffs' computers and communications, however, comScore lacked consent for two reasons.

First, as shown *supra*, Section II.C.2.a., fuzzifying is substantially different from filtering, and Plaintiffs never consented to—indeed, never even knew about—collection by software that merely fuzzified (rather than filtered) their CPII. Even though the ULA's terms and conditions said that the collection software would "make commercially viable efforts to automatically filter [CPII]," OSSProxy didn't filter CPII at all. Instead, OSSProxy collected all CPII, attempted to obfuscate some of it, and transmitted it to comScore's servers (in both fuzzified and plaintext form). (SOF ¶¶ 44, 50–53.)

Any commonsense understanding of the term "filter" is irreconcilable with OSSProxy's "collect everything, sort it out later" fuzzification programming. In the online and software

contexts, Merriam-Webster defines "filter" as "software for sorting or *blocking access to* certain online material."[15] Common usages of "filter"—both online and off—are in line with Merriam-Webster's "blocking" definition. Major antivirus companies (Norton, McAfee, etc.) sell "web filtering" software that allows administrators (or parents) to permit or deny access to selected websites, or categories of websites.[16] Internet-based email applications commonly let users "filter" emails from pre-identified senders or that contain certain textual content, which prevents such emails from ever reaching a user's inbox. Spam filters work the same way. In the non-software context, vacuum filters block dust and debris from escaping into the air, and coffee filters block grounds from dripping into freshly brewed coffee. The list goes on. OSSProxy's fuzzification mechanism, by contrast, didn't block or exclude *any* CPII from collection. Instead, OSSProxy was programmed to *target* CPII for collection before trying to obfuscate some of it.

While comScore writes the difference off as "lawyers' semantic quibbles," (*see* comScore's Petition for Leave to Appeal Class Certification Order Pursuant to Fed. R. Civ. P. 23(f), *Harris v. comScore, Inc.*, No. 13-8007, Dkt. 1 at 15 n.11 (7th Cir. Apr. 16, 2013)), it forgets that its *own* (non-lawyer) witness first identified the difference between filtering and fuzzification. (SOF ¶ 51.) Not only that, OSSProxy *does* employ filtering mechanisms [redacted] (*Id.* ¶¶ 47–49, 52 (emphasis added.)) comScore simply didn't program OSSProxy to apply those mechanisms to prevent collection of CPII (and thereby protect panelists' privacy and conform with the ULA). Instead, the filters only operated to exclude data comScore couldn't monetize, while allowing OSSProxy to collect *all* CPII and monetize as much as possible.

---

[15] *Filter Definition*, Merriam-Webster, http://www.merriam-webster.com/dictionary/filter (last visited Feb. 20, 2014).

[16] *See*, *e.g.*, *McAfee Web Protection*, McAfee, http://www.mcafee.com/us/resources/data-sheets/ds-web-protection.pdf (last visited Feb. 20, 2014).

These substantial differences explain the admission by comScore's Chief Technology Officer and Rule 30(b)(6) designee, that "filtering and fuzzifying are two different things." (*Id.* ¶ 51.) Plaintiffs and the Class consented the to the former, not the latter.

Second, and as shown *supra*, Section II.C.2.b., even if fuzzifying were substantially the same as filtering, comScore programmed OSSProxy to [redacted] The ULA's promise of "automatic CPII filtering" was given with only one qualification: that "commercially viable efforts" would be made to do it.[17] (*Id.* ¶ 39.) The ULA did not explain, however, that filtering (or fuzzification, as it turned out) would be additionally limited by [redacted] (Ex. 4; SOF ¶¶ 55–57.) Worse still, not only did comScore know [redacted] (SOF at ¶¶ 57–58.) As a result of this departure from the ULA's terms, comScore [redacted]

All told, the difference between what was promised and what occurred goes to the nature of comScore's invasion itself, and what was consented to (if anything) was "entirely different" from what took place. Like the "busybody" in Judge Posner's *Desnick* opinion, comScore's entry

---

[17] comScore cannot plausibly assert that automatic filtering of CPII would not have been "commercially viable," as it demonstrated the capacity to employ filtering technology in a commercially viable manner with regard to other types of data. (SOF ¶¶ 47–49.)

[18] It is irrelevant whether or not [redacted] comScore's *conduct* was different from any consented to, thereby creating liability, regardless of the conduct's effects. *See* Restatement § 892A, cmt. e.

into Plaintiffs' computers (via software programmed *not* to automatically filter CPII) is a trespass, even if Plaintiffs consented to *an entry* pursuant to the ULA (which only permitted software programmed to automatically filter CPII). *See Desnick*, 44 F.3d at 1352–53; *see also United States v. Blas*, No. 90-CR-162, 1990 WL 265179, at *21–22 (E.D. Wis. Dec. 4, 1990) (consent to "look at" pager did not constitute consent to activate it). Here, the difference between the actual conduct and the conduct assented to was significant—the ULA provided for collection by software that did one thing (collect certain data, while filtering CPII) but comScore did something substantially different (collect *all* data, while [redacted] In essence, comScore was permitted to take "a few stones," and instead hoped to make off with "large boulders." *See* Restatement § 892A, ill. 1; *see also id.* at cmt. e ("Consent to an invasion by particular conduct is not consent to the same invasion by entirely different conduct.").

Plaintiffs cannot be said to have consented to comScore's conduct, and therefore, Plaintiffs are entitled to partial summary judgment on the issues of consent and authorization.

IV. CONCLUSION

For the foregoing reasons, Plaintiffs Mike Harris and Jeff Dunstan respectfully request that the Court grant their Motion for Partial Summary Judgment, and award such other and further relief as it deems equitable and just.

Respectfully submitted,

MIKE HARRIS and **JEFF DUNSTAN**, individually and on behalf of a class of similarly situated individuals,

Dated: February 20, 2014

By: s/ Rafey S. Balabanian
One of Plaintiffs' Attorneys

Jay Edelson
jedelson@edelson.com
Rafey S. Balabanian

rbalabanian@edelson.com
Chandler R. Givens
cgivens@edelson.com
Benjamin S. Thomassen
bthomassen@edelson.com
EDELSON PC
350 North LaSalle Street, Suite 1300
Chicago, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378

Attorneys for Plaintiffs, the Class, and the Subclass

CERTIFICATE OF SERVICE

I, Rafey S. Balabanian, an attorney, hereby certify that on February 20, 2014, I served the above and foregoing ***Plaintiffs' Memorandum of Law in Support of their Motion for Partial Summary Judgment***, by causing true and accurate copies of such paper to be filed and transmitted to all counsel of record via the Court's CM/ECF electronic filing system.

s/ Rafey S. Balabanian