SEALED

per Order #28

Alan L. Sullivan (3152)
Todd M. Shaughnessy (6651)
J. Elizabeth Haws (11667)
Snell & Wilmer L.L.P.
15 West South Temple, Suite 1200
Beneficial Tower
Salt Lake City, Utah 84101-1004
Telephone: (801) 257-1900
Facsimile: (801) 257-1800

Mark Lambert (Cal. Bar No. 197410)
Mark Weinstein (Cal Bar No. 193043)
Cooley Godward Kronish, LLP
Five Palo Alto Square
Palo Alto, California 94306-2109
Telephone: (650) 843-5003

Attorneys for Plaintiff

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF UTAH, CENTRAL DIVISION

PUBLIC ENGINES, INC., a Delaware Corporation,

Plaintiff,

vs.

REPORTSEE, INC., a Delaware Corporation,

Defendant.

REPLY MEMORANDUM IN SUPPORT OF PLAINTIFF'S MOTION FOR PRELIMINARY INJUNCTION

Case No. 2:10-cv-317

Honorable Tena Campbell

Plaintiff Public Engines, Inc. ("Public Engines") respectfully submits this reply memorandum in response to the Memorandum in Opposition to Motion for Preliminary Injunction (May 14, 2010) (the "Opposition") filed by defendant ReportSee, Inc. ("ReportSee"), and in further support of Public Engines' Motion for Preliminary Injunction.

TABLE OF CONTENTS

Page

SUMMARY

In this reply, Public Engines responds to factual statements in the Opposition and presents important new facts disclosed in discovery on this motion. Discovery has shown that ReportSee has known since June 2008 that its scraping of CrimeReports.com violated Public Engines' Terms of Use and was illegal. Last October, one of ReportSee's agents advised a law enforcement agency that ReportSee's scraping of data from CrimeReports.com "is a felony," and ReportSee has repeatedly acknowledged to others that its use of CrimeReports.com data is limited by the website's Terms of Use. The contention that ReportSee could lawfully circumvent the Terms of Use by accessing the data through a widget on the San Jose Police Department's website should be rejected: ReportSee's scraper copied CrimeReports.com's data not through a widget, but directly from Public Engines' servers, in violation of the Terms of Use. Discovery has also shown that ReportSee has systematically harassed the law enforcement agencies with which Public Engines has contracts by demanding the data feed from software that Public Engines installed at the agencies pursuant to its contracts with those agencies. In doing so, ReportSee has attempted to persuade the law enforcement agencies to violate their agreements with Public Engines.

Contrary to ReportSee's arguments, Public Engines has met each of the requirements for a preliminary injunction:

Irreparable injury—ReportSee's abuse of Public Engines' website and misappropriation of data threatens Public Engines' investment and the integrity and goodwill of its website and associated services. ReportSee has no basis to argue, as it does, that Public Engines' investment of more than $3 million to develop the content of the website from raw police data was "excessive." Mr. Drane, the source of this opinion, testified that he has no experience in software programming or law enforcement data systems. In fact, ReportSee has never developed or installed software for law enforcement agencies. Beyond that, ReportSee's

Opposition chooses to ignore the obvious differences between (1) the public's access to CrimeReports.com for personal use and (2) ReportSee's scraping of Crimereports.com for commercial purposes and unfair competitive advantage. The first constitutes the CrimeReports.com purpose of the website; the second constitutes a clear violation of the website's Terms of Use. One of the ironies of this case is that ReportSee's own Terms of Use for SpotCrime.com prohibit exactly the same conduct, namely, the scraping of website data and the commercial use of website data.

Balance of harms—Discovery has demonstrated that any injury ReportSee will suffer as the result of an injunction is pure speculation. In the first place, Mr. Drane testified that the data his company has scraped from CrimeReports.com is insignificant and that he does not intend to resume scraping even if the Court refuses to issue an injunction. We must question the truth of these statements, but they demonstrate ReportSee's public position that an injunction would be inconsequential to the company. In the second place, Mr. Drane was unable to name any law enforcement agency, media partner, or source of financing whose relationship with ReportSee would be affected as the result of this suit.

Public interest—Contrary to ReportSee's arguments, Public Engines' arrangements with law enforcement agencies are not exclusive, and CrimeReports.com does not have a monopoly on information. Public Engines' contracts with agencies do not prevent them from sharing data with the public, news reporters, or other crime mapping services. Newspapers and television stations, like all members of the public, are welcome to gather facts from CrimeReports.com for personal use or news stories. The issuance of an injunction will not adversely affect the public interest.

Success on the merits—As shown in detail in Public Engines' opening memorandum and later in this reply, Public Engines is likely to prevail on each of its claims, and nothing in the Opposition would lead to a different result. Public Engines has established a claim for violation

of the Computer Fraud and Abuse Act because, as the result of ReportSee's scraping, it has been required to expend substantial resources to protect the integrity of its website. ReportSee has unquestionably violated the Terms of Use of CrimeReports.com, establishing the basis for a breach of contract claim. The contention that these Terms of Use are "illusory" is belied by the fact that they are materially identical to ReportSee's terms of use for SpotCrime.com. ReportSee's Opposition has simply ignored the authorities that have upheld contract claims similar to the present claim. Beyond this, ReportSee does not present a serious challenge to Public Engines' entitlement to relief under the Utah Unfair Competition Act, the Lanham Act, the "hot news" misappropriation doctrine, or the rules governing the tort of intentional interference with contractual relations. For reasons explained in detail below, ReportSee's arguments based on Copyright Act preemption and the First Amendment have no support in the law.

REPLY TO STATEMENT OF FACTS

A. ReportSee's Scraping of Public Engines' Crime Report Data.

In 2008, ReportSee began scraping crime report data from CrimeReports.com. (Decl. of G. Whisenant, ¶ 38, Apr. 9, 2010.) ReportSee combined this data with other data it had collected, displayed it on SpotCrime.com, and licensed it for a fee to media outlets. (Decl. of J. Haws, Ex. 1, Dep. of C. Drane at 34:21-35:10.) ReportSee stopped scraping CrimeReports.com when Mr. Colin Drane, ReportSee's CEO, received Public Engines' June 16, 2008, cease and desist letter. (Def.'s Mem. Opp'n Pl.'s Mot. Prelim. Inj., ("Opp'n Mem."), Ex. 1, Decl. of C. Drane, ¶ 29, May 14, 2010.) At that time, he personally read and became familiar with CrimeReports.com's Terms of Use, including the provisions that prohibit scraping. (Decl. of J. Haws, Ex. 1, Dep. of C. Drane at 98:5-99:13.)

ReportSee hired a contractor to develop and operate its scraping program. (Id. at 20:15-22, 29:4-22.) In July 2009, ReportSee resumed scraping when this contractor told Mr. Drane

that the CrimeReports.com "widget" on the San Jose Police Department's webpage did not display CrimeReport's Terms of Use. (Id. at 113: 2-12; Opp'n Mem., Ex. 1, Decl. of C. Drane, ¶¶ 31-33.) A widget is a "window" or "frame" on a webpage that provides access to the content of another, different webpage. Through this widget, a user can access, search, and view all of the crime report data that appears on the CrimeReports.com webpage itself. Although Mr. Drane was fully aware that CrimeReport.com's Terms of Use prohibited scraping, he nevertheless directed the contractor to scrape data from CrimeReports.com by going through this widget. (Decl. of J. Haws, Ex. 1, Dep. of C. Drane 113:2-19, 114:13-116:13.)

Mr. Drane concedes that, at the time, he had "concerns" about whether circumventing the Terms of Use in this manner was appropriate. (Id. at 115:25-116:13.) During the time it was scraping data from CrimeReports.com, ReportSee's agents told at least one police department that it would be a "felony" for ReportSee to scrape data from CrimeReport.com, (See Decl. of J. Haws, Ex. 2, RS039142), and Mr. Drane himself acknowledged in writing that ReportSee's ability to access CrimeReports.com data was limited by Public Engines' Terms of Use. (Id. at Ex. 3, RS022769; id. at Ex. 4, RS043617.) In short, when ReportSee started scraping CrimeReports.com in 2009, it knew that doing so was illegal and was prohibited by the Terms of Use.

Although Mr. Drane states in his declaration that ReportSee's scraping of CrimeReport.com's data was accomplished through the San Jose Police Department widget, (Opp'n Mem., Ex. 1, Decl. of C. Drane, ¶¶ 31-34), he testified in deposition that he has no personal knowledge about how ReportSee's scraper operated or whether it accessed CrimeReports.com via the San Jose Police Department widget. (Decl. of J. Haws, Ex. 1, Dep. of C. Drane, 31:23-33:1.) In truth, ReportSee's scraper did not access Public Engines' crime report data via any widget. As explained in detail in the Supplemental Declaration of Steve Meyers, Public Engines' log files show exactly how ReportSee's scraper accessed the data, and these log

files establish unequivocally it was not done via the San Jose Police Department widget; instead, ReportSee's scraper accessed and copied the data directly from Public Engines' web servers. (Supp. Decl. of S. Meyers, ¶¶ 6-30, May 24, 2010.) Like the Terms of Use for CrimeReports.com, the Terms of Use for ReportSee's SpotCrime.com website specifically prohibit such scraping of data from the database. ReportSee's own Terms of Use provide:

> Direct Database Access prohibited. You may not directly access our database except via the standard browser/graphic user interface, and You may not use any robot, script, or other automated tool to access or use the Website, any Information, or any data or the database....

(Decl. of J. Haws, Ex. 5, SpotCrime.com Terms of Use.)

ReportSee incorrectly claims that scraping is nothing more than automated data indexing, akin to an internet search engine like Google. (Decl. of C. Drane, ¶ 27.) While search engines like Google index the content of webpages and store that information so it can be conveniently searched, they do so to assist users in finding websites and to assist website owners by directing users to them. When users type search requests in Google, they get back a list of webpages that may contain information the users are looking for and links to those webpages. To view the underlying data, the user must go to the website itself. Unlike ReportSee's scraping, Google does not take information from webpages, incorporate it into its own webpage, and then claim to own that information. (Supp. Decl. of S. Meyers, ¶¶ 31-34.)

ReportSee's own Terms of Use draw exactly this distinction. As quoted above, ReportSee prohibits users from directly accessing the SpotCrime.com database or accessing the data through means other than a standard web browser. In other words, they prohibit scraping. ReportSee's Terms of Use, however, go on to distinguish scraping from copying or indexing data on its webpage for purposes of search engines:

> .... The above shall not prohibit any act permitted by law, as by, for example, a bone fide search engine that is automatically

> *indexing the Website for its search engine database (as long as the* result of a query to such search engine returns a link back to the Website), and the search engine is not re-presenting the Information in a manner that is or would be competitive to the Website....

(Decl. of J. Haws, Ex. 5, SpotCrime.com Terms of Use.)

B. Public Engines' Customers and Competition in the Marketplace.

CrimeReports.com does not hold a monopoly on crime mapping. Rather, it competes with a number of crime mapping services in addition to SpotCrime.com and with a limited number of large police departments with their own websites. (Supp. Decl. of G. Whisenant, ¶ 4.) And contrary to ReportSee's suggestion (Opp'n Mem. at 20), Public Engines' contracts with law enforcement agencies are not exclusive arrangements. (Supp. Decl. of G. Whisenant, ¶ 5.) Police agencies that use Public Engines' Publisher software and associated services are free to contract with other software vendors to install similar programs to extract and filter crime report data from their Computer Aided Dispatch ("CAD") and Records Management Systems ("RMS"). Fort Worth, Texas, for example, operates both Public Engines' Publisher software, as well as software developed by The Omega Group which extracts crime report data from CAD and RMS systems and displays it on The Omega Group's crimemapping.com website. (Supp. Decl. of G. Whisenant, ¶ 5.)

Public Engines' contracts with its customers also do not require that the customers refrain from providing crime report data to anyone other than Public Engines. Public Engines' agreements make clear that the data contained in the law enforcement agencies' CAD and RMS systems is owned by the agency, not Public Engines, and they are free to do whatever they want with that data. The agreements only restrict the disclosure of De-Identified Data, or the output from the operation of Public Engines' proprietary Publisher software program. (Decl. of G.

Whisenant, Apr. 9, 2010, Ex. 1, ¶ 8.1 ("... all Customer Data (excluding De-Identified Data) will be considered Confidential Information of Customer.")

Public Engines does not claim, and has never claimed, that ReportSee should be prohibited from obtaining crime report data from police departments, including police departments with whom Public Engines has contracts. If these departments make crime report information available to the media or the public, ReportSee is free to obtain and use that information. According to ReportSee's Opposition, at least 212 police departments around the nation currently do this. (Opp'n Mem. at 6.) ReportSee is likewise free to ask agencies for crime report information that the agency is required to make available to the public pursuant to legitimate public records requests (but not De-Identified Data from the Publisher software), and ReportSee acknowledges that it successfully has made such requests. (Id.) ReportSee however, should be prevented from scraping information from CrimeReports.com, incorporating it into SpotCrime.com, and then selling it as its own. Nor should ReportSee be allowed to harass Public Engines' customers simply because they have installed Public Engines' software on their CAD and RMS systems, thereby creating a quick, easy, and inexpensive data feed that would allow ReportSee to piggyback on the millions of dollars Public Engines has invested in its technology and services.

C. ReportSee's Harassment of Customers and Public Engines' Response.

ReportSee's documents show that it has systematically contacted law enforcement agencies across the country via email requesting that they provide crime report information. (See, e.g., Decl. of J. Haws, Ex. 6, RS036959-61; id. at Ex. 7, RS025231-33, id. at Ex. 8, RS038913-14.) When ReportSee learns that the agency is Public Engines' customer, it sends a scripted demand that the agency provide ReportSee the same data feed being provided to Public Engines. (Id.) Many of these agencies contacted Public Engines about these demands. By fall

2009, numerous agencies had contacted Public Engines complaining about the difficulties they were having in dealing with ReportSee. (Supp. Decl. of G. Whisenant, ¶¶ 8-11.)

Based on these contacts, it appears that ReportSee chose deliberately to ignore the nature of the agencies' relationship with Public Engines and the source of the data that appeared on CrimeReports.com. Specifically, ReportSee did not simply demand that the agency provide it with crime data from the agency; rather, it demanded that the agency provide access to the ongoing data feed from Public Engines' Publisher software program. The problems with such demands are that agencies are contractually prohibited from providing this data to third parties, and that the agencies do not have access to this data feed. (See Decl. of J. Haws, Ex. 9, RS013213-14; Supp. Decl. of G. Whisenant, ¶ 8-11; Decl. of G. Whisenant, Ex. 1, ¶ 8.1.)

Public Engines first attempted to resolve the issue by discussing it directly with ReportSee. In October 2009, Greg Whisenant telephoned Mr. Drane and tried to explain that the data feed ReportSee was demanding was unique to Public Engines, was not publicly available, and was not something the agencies could provide. (Decl. of G. Whisenant, ¶ 43.) Mr. Drane advised Mr. Whisenant that ReportSee intended to continue its efforts and ultimately hung up on Mr. Whisenant. (Id. ¶ 44.) Public Engines followed up with a cease and desist letter, which ReportSee ignored. (Id.)

Public Engines therefore had no choice but to address the issue through the law enforcement agencies with which it contracted. (See Supp. Decl. of G. Whisenant, ¶¶ 8-11; Decl. of J. Haws, Ex. 10, PE000074.) Public Engines sent general information to all of its customers advising them to raise with ReportSee the same issues that Mr. Whisenant had unsuccessfully attempted to address with Mr. Drane. (See Supp. Decl. of G. Whisenant, ¶¶ 10-11; Decl. of J. Haws, Ex. 11, PE000022-23.) Public Engines did not instruct the agencies to withhold crime report information from ReportSee. Public Engines told the agencies that while they would need to make their own determinations regarding applicability of public records

access laws, Public Engines did not believe – and does not believe – that these laws require the agencies to give ReportSee access to the data feed from the Publisher software. (Supp. Decl. of G. Whisenant, ¶ 10; Decl. of J. Haws, Ex. 11, PE000022-23.) The public records access laws do not require law enforcement agencies to expend the resources necessary to create for a private party a forward-looking, ongoing electronic data feed of the agency's crime data, which is what ReportSee's employees were demanding. All of this was done to protect Public Engines' business and mitigate the damages caused by ReportSee's harassment of Public Engines' customers. (Supp. Decl. of G. Whisenant, ¶ 11.)

D. ReportSee's Terms of Use Mirror Public Engines' Terms of Use.

Mr. Drane states that "ReportSee considers all of its crime data to be public data" (Decl. of C. Drane, ¶ 23) and suggests that ReportSee, unlike Public Engines, allows third parties to use ReportSee's crime report data for whatever purposes they wish. ReportSee's own Terms of Use, however, say exactly the opposite. As quoted above, ReportSee's Terms of Use (like Public Engines' Terms of Use) prohibit scraping, require that website use be for personal purposes only, and prohibit business or commercial use of the website's data. Specifically, ReportSee's Terms of Use provide:

> We grant You a limited, royalty-free, non-exclusive revocable license to make use of the Information [defined as "[a]ll words, pictures, content, graphs, charts, data and other matters presented or made available on the Website...."] for Your own personal purposes only, and You are specifically not authorized to access, and not authorized to use, any Information on the Website, for any business purpose. All other rights are expressly reserved. For the avoidance of doubt, and including by way of example and not limitation, You are not authorized to use, and You specifically covenant that that [sic] You will not use, the Information on the Website to: (i) provide access to the Information to any third person, or to otherwise distribute, make available, transmit or other disseminate the Information to anyone else or to use the Information on the Website; (ii) download any Information on this Website; (iii) sell the Information downloaded (or copied in another form) for money, exchange or other consideration; (iv)

> redistribute the Information for free to anyone; (v) make any more than one print copy of the Information for your personal use; (vi) republish the Information; (vii) make any alterations, additions or other modifications to the Information.

(Decl. of J. Haws, Ex. 5, SpotCrime.com Terms of Use.) In short, ReportSee's Terms of Use are substantially similar to Public Engines' Terms of Use, and prohibit precisely what ReportSee has done.

ARGUMENT

Public Engines has established that (a) it will suffer irreparable harm if the injunction does not issue; (b) the threatened injury to Public Engines if the injunction does not issue outweighs any potential damage to ReportSee; (c) the injunction would not be adverse to the public interest; and (d) Public Engines has a substantial likelihood of success on the merits of its claims. Arguments to the contrary in ReportSee's Opposition should be rejected.

A. Public Engines Will Suffer Irreparable Harm If the Injunction Does Not Issue.

In its opening memorandum and in the First Declaration of Greg Whisenant, Public Engines showed that if ReportSee is allowed to continue to scrape and sell data from CrimeReports, Public Engines' investment will be lost, and the integrity of its website will be compromised. (G. Whisenant Decl. ¶¶ 46-48.) Mr. Drane challenges the more than $3 million Public Engines has invested in its technology, stating the figure is "excessively high." (Decl. of C. Drane, ¶ 45.) According to Mr. Drane:

> [i]t is not a particularly advanced or difficult process to create software that queries databases and pull [sic] out specific information ("de-identified data" for example). ReportSee creates software to scrub identifying information from police database reports that are sent to [sic], and it takes about 4-hours to create that software for each brand of CAD or RMS system."

(Id.) But in deposition, Mr. Drane admitted that he has no basis for making any of these statements. (Decl. of J. Haws, Ex. 1, Dep. of C. Drane at 142:2-143:2.) He acknowledged that

he has no background or experience in computer programming or software development, and he does not claim to be an expert in databases generally, or in the particular CAD and RMS systems that are used by police agencies. (Id. at 9:3-12:5). Most important, he admitted that ReportSee has never developed or installed a program designed to extract or filter data from a CAD or RMS system. (Id. at 142:20-143:1.)

Public Engines' revenue comes from its contracts with over 800 law enforcement agencies, which pay Public Engines a small fee to license Public Engines' software and associated services. (Decl. of G. Whisenant, ¶ 11-16.) If ReportSee is permitted to misappropriate data from Public Engines and then sell the data to third parties in competition with Public Engines, Public Engines' investment in technology and general goodwill will be diminished. (Id., ¶ 47(b).) Moreover, as Public Engines is forced to take increasingly aggressive technical measures to stop ReportSee, the likelihood increases that the public generally will not be able to use CrimeReports.com as easily and both law enforcement agencies and the public in general will suffer. (Id., ¶ 47(a).) Finally, law enforcement agencies are under no obligation to contract with Public Engines or make their crime report information available through CrimeReports.com. If ReportSee's harassment and threats of litigation cause a law enforcement agency to conclude that it is simply too much trouble, they will simply terminate their contracts. (Id. ¶ 48(b).)

ReportSee's only response is to claim that, to date, only one law enforcement agency has terminated its contract and this agency had reasons in addition to ReportSee's harassment. (Opp'n Mem. at 57.) But Public Engines need not lose customers in droves before being entitled to an injunction. Injunctive relief is "an anticipatory remedy proposed to prevent the perpetration of a threatened wrong or to compel the cessation of a continuing one" Sys. Concepts, Inc. v. Dixon, 669 P.2d 421, 428 (Utah 1983), and injunctive relief is particularly appropriate to prevent the misappropriation of intellectual property rights. See, e.g., Lorillard

Tobacco Co. v. Engida, 213 Fed. Appx. 654, 656-67 (10th Cir. 2007); New Pro Publ'ns v. Links Media Group, LLC, 2007 WL 4115995, at *4 (D. Colo. Nov. 16, 2007); Harris Research, Inc. v. Lydon, 505 F. Supp. 2d 1161, 1168 (D. Utah 2007). Moreover, the contract ReportSee entered with Public Engines through the Terms of Use specifically authorizes injunctive relief. (Decl. of G. Whisenant, Ex. 3, ¶ 11.)

Finally, ReportSee argues that because Public Engines provides access to its crime report data to millions of people for free on CrimeReports.com, it "strains common sense" to argue that ReportSee's "same use" of that data devalues Public Engines' technology. (Opp'n Mem. at 58.) To state the obvious, ReportSee is not making the "same use" of Public Engines' data as the millions of individuals who regularly access CrimeReports.com. Instead, ReportSee scrapes the data, puts ReportSee's name on it, earns advertising revenue from its republication, and then sells it in direct competition with Public Engines to third parties. It is clear that such conduct causes irreparable harm.

B. The Threatened Injury to Public Engines if the Injunction Does Not Issue Outweighs Any Potential Damage to ReportSee.

ReportSee fails to identify any harm it would suffer from the issuance of an injunction, and it is now clear that an injunction would have no impact on ReportSee's business. ReportSee claims that the data taken from CrimeReports.com was insignificant; that it was removed from SpotCrime.com after this lawsuit was filed; and that ReportSee stopped scraping data from CrimeReports.com shortly before the lawsuit was filed. (Decl. of C. Drane, ¶¶ 36-38.) Furthermore, Mr. Drane testified that he does not intend to resume scraping CrimeReports.com, even if this Court does not enjoin him from doing so. (Decl. of J. Haws, Ex. 1, Dep. of C. Drane at 157:2-9.)[1] Although we have reason to question the truth of these statements, ReportSee

[1] In June 2008, when Public Engines first confronted Mr. Drane about scraping and demanded that he stop, he agreed in writing to do so. (Decl. of G. Whisenant, ¶¶ 35-38.) That promise lasted a year, until ReportSee resumed scraping in July 2009. (Decl. of C. Drane, ¶ 31.) Public Engines therefore has little confidence that, this time, he will stand by his word and stop scraping.

appears to concede that it does not need data from CrimeReports.com to operate its website, and that an injunction will not interfere with its business. (Id. at 139:10-140:1.)

Although Mr. Drane's declaration states that issuance of an injunction "could have serious implications to SpotCrime's ability to secure financing to operate its business – particularly in today's economic climate" (Decl. of C. Drane, ¶ 41), he testified that he personally has provided all financing for ReportSee's business and has never spoken with possible outside investors. (Decl. of J. Haws, Ex. 1, Dep. of C. Drane at 12:9-15:2.) Mr. Drane also speculates in his declaration that ReportSee's relationships with its media customers might be adversely affected by the issuance of an injunction (Decl. of C. Drane, ¶ 41). But he testified in deposition that no media customer with whom he had spoken about this lawsuit has changed or threatened to change its business relationship with ReportSee. (Decl. of J. Haws, Ex. 1, Dep. of C. Drane at 200:9-13, 201:17-21; 202:24-203:6.)[2]

Finally, ReportSee claims that if police departments or other government officials learn that an injunction has been issued, they may be less likely to consider ReportSee's requests for crime data, and less likely to trust ReportSee with that data. (Decl. of C. Drane, ¶ 41.) Aside from being speculative, this harm is not the product of issuing an injunction but the product of ReportSee's deliberate decision to misappropriate data from CrimeReports.com, knowing that doing so violated the Terms of Use for CrimeReports.com. ReportSee can hardly complain about the consequences that flow from that decision.

---

[2] Additionally, to the extent his relationships with media customers may be affected, it would not be as a result of an injunction but a result of his own conduct. If media customers – who themselves display the content of SpotCrime.com on their own websites – learn that unlawfully scraped data appears on SpotCrime.com, they would, in all likelihood, demand that ReportSee immediately remove it because failing to do so could subject them to liability. This likely explains why ReportSee removed the data from SpotCrime.com right after this lawsuit was filed.

The harm that would be caused to Public Engines by not issuing an injunction, as outlined above and in our moving papers, certainly outweighs the speculative and non-existent harm identified by ReportSee.

C. The Injunction Would Not Be Adverse to the Public Interest.

ReportSee argues that it is not in the public interest to permit Public Engines "to exert a monopoly over the publication, comment, criticism and other use of crime data...." (Opp'n Mem. at 60.) But Public Engines is not a monopoly. It competes with ReportSee and other crime mapping services. (See Supp. Decl. of G. Whisenant, ¶ 4.) ReportSee's hyperbole also is undermined by ReportSee's contention that what it took from CrimeReports.com was trivial, has been removed, and is not necessary to the operation of SpotCrime.com. (See Decl. of C. Drane, ¶¶ 36-38.)

ReportSee next claims that "if NBC Nightly News decided to produce a special report on a rash of crimes in downtown Salt Lake City and needed a large amount of 'de-identified' basic crime data regarding the area, according to Public Engines, the Salt Lake City Police Department would be prohibited from providing it." (Opp'n Mem. at 61.) This argument fails for at least three reasons. First, Public Engines' agreement with the Salt Lake City Police Department makes clear that the department, not Public Engines, owns the data contained in its CAD and RMS systems. The police department is free to use that data however it wants, including providing it to NBC Nightly News. Second, reporters have and may use copyright-able material, like the De-Identified Data on CrimeReports.com, to gather facts for a legitimate news story under the fair use doctrine. See 17 U.S.C. § 107; Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 579 (1994). But gathering facts for a news story is far different from scraping data from someone else and commercializing it as your own. See, e.g., Los Angeles News Service v. Reuters Television Intern., Ltd., 149 F.3d 987, 993 (9th Cir. 1998). Third, to the extent NBC Nightly News wishes to publish for itself the content of CrimeReports.com or SpotCrime.com,

nothing would prevent it from negotiating an agreement with either Public Engines or SpotCrime.com for the rights to do so, as many media outlets already have.

The only public interest implicated by the requested injunction is the strong public interest in ensuring parties' performance of their contractual arrangements, Mountain Am. Credit Union v. Godfrey, 2006 WL 2129465, at *4 (D. Utah, July 28, 2006), and the interests of Public Engines' law enforcement customers and the general public in making crime report data freely available for citizens in communities across the country.

D. Public Engines Has A Substantial Likelihood of Success on the Merits.

Because Public Engines satisfies the first three requirements for injunctive relief, it is only required to show that "there are 'questions going to the merits so serious, substantial, difficult and doubtful, as to make the issues fair ground for litigation and deserving of more deliberate investigation.'" Waste Connections of Kansas, Inc. v. City of Bel Aire, Kan., 191 F.Supp.2d 1238, 1241 (D. Kan. 2002) (citing Buca, Inc. v. Gambucci's Inc., 18 F. Supp. 2d 1193, 1201 (D. Kan. 1998)); accord Tri-State Generation and Transmission Ass'n, Inc. v. Shoshone River Power, Inc., 805 F.2d 351, 355 (10th Cir. 1986). In other words, Public Engines need not prove it will win. Instead, it must only show that at least one of its claims supporting injunctive relief raises "a genuinely debatable issue." Tri-State Generation, 805 F.2d at 355.[3] Public Engines has met its burden on this issue.

[3] ReportSee incorrectly argues that the injunction Public Engines seeks is disfavored and therefore requires a stronger showing. That contention is wrong. Public Engines' proposed injunction is not a disfavored injunction because it seeks to preserve the status quo, is not mandatory, and does not grant Public Engines all the relief it could recover at the conclusion of a trial on the merits. The status quo, or "the last peaceable uncontested status existing between the parties before the dispute developed," Doubleclick Inc. v. Paikin, 402 F. Supp. 2d 1251, 1255 (D. Colo. 2005), was ReportSee not scraping CrimeReports.com or harassing Public Engines' customers. An injunction would restore that status quo. The proposed injunction is prohibitory not mandatory: ReportSee must stop misappropriating and making commercial use of Public Engines' data and interfering with Public Engines' contracts. Requiring ReportSee to delete Public Engines' data from its website (which ReportSee claims it already has done) does not make the injunction mandatory but simply reestablishes the status quo. See Evans v. Fogarty, 44

1. Computer Fraud and Abuse Act ("CFAA").

ReportSee argues that Public Engines' CFAA claim is likely to fail because: (a) Public Engines has not stated a claim for relief, (b) Public Engines should be estopped from asserting a CFAA violation, (c) the CFAA does not prohibit unauthorized use of data, (d) the CFAA is unconstitutional, and (e) the CFAA claim is preempted by the federal Copyright Act. (Opp'n Mem. at 25.) As explained below, however, each of these contentions should be rejected.[4]

(a) Public Engines states a claim for relief.

ReportSee first contends that Public Engine has not shown that its computers or servers were physically damaged and thus does not state a claim for relief. (Op. Mem. at 26.) ReportSee's reading of the CFAA improperly limits the reach of the statute. Damage under the CFAA includes "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § (e)(8). Under this section, Public Engines must show either "damage or loss by reason of a violation" of the CFAA. 18 U.S.C. § 1030(g); Southwest Airlines Co. v. Farechase, Inc., 318 F. Supp. 2d 435, 439 (N.D. Tex. 2004). Our opening papers showed that Public Engines has suffered both because ReportSee has compromised the integrity of Public Engines' database and misappropriated its information, requiring Public Engines to expend resources to remediate these problems. (Decl. of S. Meyers, ¶¶ 4-21.)

Second, Public Engines is not required to plead a CFAA claim with particularity, as ReportSee contends. Patrick Patterson Custom Homes, Inc. v. Bach, 586 F. Supp. 2d 1026, 1031 (N.D. Ill. 2008) ("Plaintiffs need only allege the required elements pursuant to Rule 8(a)(2)'s notice pleading standard, not the heightened pleading standard of Rule 9(b).") (citing P.C. of

---

Fed. Appx. 924, 928 (10th Cir., Aug. 21, 2002); Dominion Video Satellite, Inc. v. EchoStar Satellite Corp., 269 F.3d 1149, 1155 (10th Cir. 2001). Finally, damages are a significant part of the relief sought by Public Engines and would not be resolved with the issuance of a preliminary injunction.

[4] Because ReportSee makes its copyright argument concerning multiple causes of action, Public Engines' response to that argument is set forth in subsection D(7) below.

Yonkers, Inc. v. Celebrations! The Party and Seasonal Superstore, LLC, 2007 WL 708978, at *6 (D. N.J. Mar. 5, 2007)). Clearly, Public Engines has adequately stated a claim for relief under the CFAA.

(b) ReportSee's estoppel argument should be rejected.

ReportSee argues that because Public Engines has communicated with its customers about how they should respond to demands from ReportSee, Public Engines should be estopped from asserting various causes of action, including a claim under the CFAA. (Opp'n Mem. at 27-28.) ReportSee provides no legal support for this argument, and it fails to describe anything that was improper about these communications. As explained above and in the Supplemental Declaration of Greg Whisenant, Public Engines took this step only after ReportSee began systematically harassing its customers, and only after ReportSee refused to discuss the issue directly with Public Engines. Faced with confused and disgruntled law enforcement customers, Public Engines had no choice but to help educate its customers in order to allow them to raise with ReportSee the very issues that ReportSee would not discuss with Public Engines. Public Engines was preserving its business and mitigating its damages. This does not give rise to estoppel.

(c) ReportSee violated the CFAA.

ReportSee was not authorized to access Public Engines' database for business use, nor was ReportSee's scraper authorized to access the database at all. The CFAA prohibits not only unauthorized access to a protected computer, but also access that exceeds any authorization given. 18 U.S.C. 1030(a)(4). Even when it involves publicly-available internet content, courts have held the owners of that information may limit or deny access. The federal courts have specifically held that unauthorized scraping violates the CFAA.

In Southwest Airlines Co. v. FareChase, Inc., 318 F. Supp. 2d 435, 437 (N.D. Tex. 2004), for example, the court held the defendants use of a scraper to obtain data from Southwest's

website violated the CFAA's prohibitions on unauthorized access because (1) Southwest.com's Use Agreement prohibited "any deep-link, page-scrape, robot, spider or other automatic devise, program, algorithm or methodology which does the same things," and (2) Southwest had provided "direct 'repeated warnings and requests to stop scraping.'" See id. at 439. According to the court, the defendant knew, by virtue of the Use Agreement, that scraping was not allowed. Id. Moreover, even if the defendant had not read the Use Agreement, Southwest represented that it had explicitly informed the defendant that their access was not authorized. Id. at 439-40. According to the court, the facts supported a claim under the CFAA. Id.

The First Circuit addressed website scraping in EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 585 (1st Cir. 2001), holding that an injunction was properly entered where a competitor deployed a scraper that accessed the plaintiff's website in order to extract pricing data. Id. at 579-80. Injunctive relief was appropriate because "copyright, contractual and technical restraints sufficiently notified [the defendant] that its use of a scraper would be unauthorized." Id. at 580. According to the court, the defendant's likely abuse of proprietary information to facilitate the scraping of information from a website would not be an authorized use of that website. Id. at 584.[5]

ReportSee contends there can be "no liability when a defendant's access to a computer was authorized but its use of data obtained from the computer was not." (Opp'n Mem. at 28.) But ReportSee's access to CrimeReports.com's database was not authorized, and the cases

[5] In United States v. Drew, another CFAA case, the court recognized "the vast majority of the courts (that have considered the issue) have held that a website's terms of service/use can define what is (and/or is not) authorized vis-à-vis that website." 259 F.R.D. 449, 462 (C.D. Cal. 2009). "It cannot be considered a stretch of the law to hold that an owner of an Internet website has the right to establish the extent to (and the conditions under) which members of the public will be allowed access to information, services and/or applications which are available on the website." Id. at 461. The court in Drew also recognizes that "[w]ithin the breach of contract approach, most courts that have considered the issue have held that a conscious violation of a website's terms of service/use will render the access unauthorized and/or cause it to exceed authorization." Drew, 259 F.R.D. at 460 (summarizing cases).

ReportSee cites are not applicable. ReportSee primarily relies on LVRC Holdings, LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009), but misstates the nature of Public Engines' claims and the result under Brekka that flows from them.

Brekka held that where a grantor gives another unqualified access to a computer or database, the grantor cannot later claim a violation of CFAA if the grantee uses data in an unexpected or undesired manner. Id. at 1132-35. There, an employee was given unlimited access to certain databases belonging to the employer and thereafter appropriated the data to start a competing business. Id. The Ninth Circuit held that because the employer had given the defendant permission to access its computer, and that the documents were made available by virtue of his employment, the employee did not access the computer "without authorization." Id.

ReportSee's conduct is very different. ReportSee never had authority to access Public Engines' servers for the purpose of scraping data. Its access was at all times limited by the website's Terms of Use, which specifically prohibit scraping. Access to CrimeReports.com was at all times qualified. As such Brekka is distinguishable, if not wholly inapposite.[6] In fact, the court in Brekka recognized that by including the phrase "exceeds authorized access," Congress recognized that "an individual who is authorized to use a computer for certain purposes but goes

[6] ReportSee argues at length that the Court should impose the rule of lenity and narrowly construe the CFAA in its favor. The rule of lenity, however, should not be applied in this case. The court recognized in Brekka that lenity finds its bases in considerations of notice. Brekka, 581 F.3d at 1135. The rule recognizes that interpreting criminal statutes in unexpected and novel ways is therefore improper. Id. at 1134-35. Notice concerns, however, are not present here. ReportSee was given notice–through both the Terms of Use of Public Engines' site and the cease and desist letter served upon them–that its actions were without authorization. As applied in this case, there is no ambiguity in the CFAA. As the United States Supreme Court has stated, "the rule of lenity applies only when an ambiguity is present; 'it is not used to beget one . . . . The rule comes into operation at the end of the process of construing what Congress has expressed, not at the beginning as an overriding consideration of being lenient to wrongdoers.'" National Organization for Women, Inc., v. Scheidler, 510 U.S. 249, 262 (1994). And simply because a statute is applied in a context not anticipated by Congress does not necessarily demonstrate ambiguity–it can also demonstrate breadth. Id.

beyond those limitations is considered by the CFAA as someone who has 'exceeded authorized access.'" Id. at 1133.

(d) The CFAA is not unconstitutional.

ReportSee next challenges the constitutionality of the CFAA, claiming that imposing liability for a breach of a website's terms of use would render the Act void for vagueness. It is true that the court's decision in United States v. Drew, supports the proposition that some provisions of the CFAA could be void for vagueness where criminal liability is to be imposed for nothing more than consciously breaching a website's terms of use. Id. at 467. ReportSee, however, misstates the breadth of the holding.

Drew involved a challenge only to 18 U.S.C. § 1030(a)(2)(C), which states that the CFAA is violated where a person "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer." Id. Drew recognized that "scienter requirements alleviate vagueness concerns." Id. at 464 (quoting Gonzales v. Carhart, 550 U.S. 124, 149 (2007)). And although the court held that the "intentional" element was not sufficiently limiting to contravene void for vagueness principles, id. at 467, it recognized the result could be different under other sections of the CFAA, and distinguished another Ninth Circuit case in part because it was brought under § 1030(a)(5). Id. Thus, even if this Court adopted the Drew reasoning, it would apply only to the § 1030(a)(2)(C) claim and not Public Engines' other CFAA claims.[7]

[7] Furthermore, the void-for-vagueness doctrine "must be examined in light of the facts of the case at hand." United States v. Mazurie, 419 U.S. 544, 550 (1975). In this case, ReportSee knew the exact limits of its authorization to access to CrimeReports.com. This is not a case where there is a notice issue concerning whether a defendant knew or should have known his actions were prohibited. ReportSee knew it was not allowed to access CrimeReports.com and take its data for commercial uses. ReportSee knew, in no uncertain terms, that Public Engines did not allow scrapers to access CrimeReports.com. ReportSee consciously violated the terms of Public Engines' site.

2. *Breach of Contract.*

ReportSee admits to scraping, and it also admits that scraping is prohibited by Public Engines' Terms of Use. (Decl. of J. Haws, Ex. 1, Dep. of C. Drane at 98:19-99:18.) To avoid the breach of contract claim, ReportSee argues (a) that Public Engines' Terms of Use do not apply because it scraped via the San Jose Police Department website (which, for a time, did not display the Terms of Use); (b) that the Terms of Use are "illusory;" and (c) that Public Engines' does not own its De-Identified data under the Terms of Use. (Opp'n Mem. at 36.) Each contention should be rejected.

ReportSee's arguments concerning access via the San Jose Police Department widget fail for at least three independent reasons. First, ReportSee admits the Terms of Use are now posted on the widget and therefore its arguments are irrelevant. (Decl. of C. Drane, ¶ 36.) Going forward, ReportSee cannot access the data via the San Jose widget without violating the Terms of Use. Second, regardless of whether the Terms of Use were posted, ReportSee knew it was violating them. Public Engines sent a cease-and-desist letter in June 2008, and Mr. Drane testified that from that point forward he was aware scraping was prohibited. (Decl. of J. Haws, Ex. 1, Dep. of C. Drane at 98:19-99:18.) In fact, ReportSee's own Terms of Use specifically prohibit scraping. Thus, regardless of whether the Terms of Use were displayed on the widget, Mr. Drane knew what they were and knew ReportSee was violating them. Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 403-04 (2d Cir. 2004) (granting preliminary injunction in scraping case because notwithstanding how or when terms of use were placed on the website at issue, defendant had actual knowledge that scraping was prohibited). Third, ReportSee is wrong as a factual matter. ReportSee did not scrape the data via the San Jose widget. The evidence conclusively shows that ReportSee's contractor programmed the scraper to access Public Engines' computers without going through any other website. (Supp. Decl. of S. Meyers, ¶¶ 4-30.)

ReportSee's one-paragraph argument that the Terms of Use are "illusory" is equally flawed. As support, ReportSee cites nothing more than a case involving the enforceability of employee handbook disclaimers under the law of New Mexico. Dumais v. American Golf Co., 299 F.3d 1216, 1219-20 (10th Cir. 2002). ReportSee does not cite, let alone address, the numerous cases cited in our opening papers that specifically enforce terms of use, or "browsewrap," contracts – including cases applying the law of California, the law that governs Public Engines' Terms of Use. See e.g., Ticketmaster L.L.C. v. RMG Techs., Inc., 507 F. Supp. 2d 1096, 1107 (C.D. Cal. 2007); McMillan v. Wells Fargo Bank, N.A., 2009 WL 1686431 (N.D. Cal. June 12, 2009); Southwest Airlines Co. v. Boardfirst, LLC, 2007 WL 4823761, at *12 (N.D. Tex. Sept. 12, 2007). These courts all have held that even though a website owner can modify its terms of use, and even though a user has no means of negotiating or formally accepting those terms, they are nevertheless enforceable against anyone who chooses to visit the site.

Finally, ReportSee's argument that Public Engines does not own its De-Identified Data is based on a selective misreading of the Terms of Use. Section 1 of the terms, titled "Permitted Use," explicitly states that "[t]he content and software on the Public Engines Sites are the proprietary property of Public Engines . . .." (See Compl., Ex. 2, ¶ 2.) The raw data provided by law enforcement agencies remains owned by those agencies, but the de-identified data belongs to Public Engines. This is clear from the Terms of Use themselves, and both the declaration of Greg Whisenant and the Terms of Service by which agencies agree to be bound in their dealings with Public Engines. (See Decl. of G. Whisenant, ¶ 14; id. at Ex. 1, ¶ 2 (defining de-identified data as the blockized data created by Public Engines).)

3. Utah Unfair Competition Act.

ReportSee does not dispute that it intentionally deployed an automated scraper specifically designed to obtain access to Public Engines' computer systems; and that it copied that data and treated it as its own. ReportSee cannot plausibly dispute this conduct led to the

"material diminution in value" of Public Engines' data. Utah Code Ann. § 13-5a-102(4). Based on these facts, it is clear that ReportSee has violated the Utah Unfair Competition Act.

ReportSee, however, challenges the way in which Public Engines has pled its claim under the Utah Unfair Competition Act. On this score, ReportSee argues that Public Engines has not identified any intellectual property rights it holds in the crime data shown on CrimeReports.com, even though five pages earlier in its opposition, ReportSee argued that the compilation of crime data on CrimeReports.com is subject to copyright protection. (Opp'n Mem. at 34-35). Beyond this, ReportSee's only argument is that according to its Terms of Use, Public Engines does not own its De-Identified Data. (Opp'n Mem. at 40). As explained above, this is based on a selective misreading of the Terms of Use and should be rejected.

4. False Advertising Under the Lanham Act.

ReportSee only argument on the Lanham Act claim concerns whether ReportSee "made material false or misleading representations of fact in connection with the commercial advertising or promotion of its product." Folkers v. Am. Massage Therapy Ass'n, Inc., 2004 WL 306913, at *9 (D. Kan. Feb. 10, 2004). (See Opp'n Mem. at 40-42.) ReportSee contends that it did not misrepresent the facts because it really does obtain data either directly from police agencies or from news reports and third party sources. (Id.)

But scraping data from others, including CrimeReports.com, is a substantial part of ReportSee's business, and it has misrepresented this fact to the public in promoting SpotCrime.com. ReportSee states that it maps crime for approximately 300 cities and counties around the nation. (Decl. of C. Drane, ¶ 8.) Approximately "212 police departments around the nation . . . either supply ReportSee directly with crime data" or provide a public feed. (Id., ¶ 9.) And although Mr. Drane states in his declaration that only 2% of the data on SpotCrime.com was scraped from CrimeReports.com, (Dec. of C. Drane ¶ 9), he acknowledged in his deposition that

he has no personal knowledge of the scraping because it was done by an outside vendor. (Decl. of J. Haws, Ex. 1, Dep. of C. Drane, 31:23-33:1.)

In contrast to this, Public Engines' records show that during the first few months of 2010, ReportSee scraped from CrimeReports.com data for at least 160 separate police agencies or geographic areas. (Supp. Decl. of S. Meyers, ¶ 39, Ex. B.) When asked about this list, Mr. Drane could not identify a single agency that was incorrectly listed or from which ReportSee did not scrape data. (Decl. of J. Haws, Ex. 1, Dep. of C. Drane at 105:3-110:10.) Based on this alone, data scraped from CrimeReports.com would constitute a significant proportion of the communities covered by SpotCrime.com. ReportSee does not acknowledge the source of its data to the public in advertising its product. (Decl. of J. Haws, Ex. 12, RS009270-71.) These material misrepresentations give rise to liability under the Lanham Act.

5. Hot News Misappropriation.

Public Engines' opening memorandum explained the elements of hot news misappropriation and facts showing ReportSee's liability. (Mem. in Supp. of Pl.'s Mot. for Prelim. Inj. at 28-29 (hereinafter "Prelim. Inj. Mem.").)[8] In response, ReportSee cites no contrary authority and argues only that timeliness is not critical to Public Engines business model, so that the claim is ill-suited to the allegations of the Complaint. (Opp'n Mem. at 43.) Timeliness, however, is the essence of Public Engines' business. Public Engines has invested millions of dollars in a system that gathers crime data in near real time, and a system for displaying that data to the public. (Decl. of G. Whisenant, ¶ 11.) Public Engines' product is designed to provide "up to the minute information to the public" to "assist law enforcement

[8] To establish "hot news" misappropriation, Public Engines must show: "(i) the plaintiff generates or collects information at some cost or expense; (ii) the value of the information is highly time-sensitive; (iii) the defendant's use of information is in direct competition with a product or service offered by plaintiff; (v) the ability of the other party to free-ride on the efforts of the plaintiff would so reduce the incentive to produce the product or service that its existence or quality would be substantially threatened." Nat'l Basketball Ass'n v. Motorola, Inc., 105 F.3d 841, 845, 852 (2d Cir. 1997).

efforts in both solving and preventing criminal activity." (Id. at 7.) Allowing ReportSee to intercept and copy that data, and publish it as its own, would substantially diminish the value of Public Engines' investment and allow ReportSee to free-ride on Public Engines' efforts. (Decl. of G. Whisenant, ¶¶ 10-14, 46-48.) Based on this, Public Engines has shown hot news misappropriation.

6. Interference with Contract.

ReportSee first asserts that Public Engines has not provided complete copies of its contracts with law enforcement agencies that are the basis for its interference with contract claim and therefore cannot show it is likely to succeed. (Opp'n Mem. at 44.) This is incorrect. Public Engines attached to its Complaint the standard form contract it enters with each law enforcement agency, which contains all terms relevant to the interference claim. (See Compl., Ex. 1.) Any amendments law enforcement customers have made to the standard form contract, the Terms of Service, were produced in discovery. The "Order Form" referenced in this standard contract, the Terms of Service, is available on the Crimereports.com website, but is not directly relevant to this claim. (Supp. Decl. of G. Whisenant, ¶ 7.) Thus, ReportSee has complete copies of entire contracts with Public Engines' customers, has had them since long before filing its opposition, and the fact that ReportSee does not cite or reference them in its opposition demonstrates they are irrelevant to the present motion.

ReportSee interferes with Public Engines contracts and relationships with its customers by demanding that they provide ReportSee with the De-Identified Data shown on CrimeReports.com. As just one recent example, on March 23, 2010, ReportSee through legal counsel wrote to the St. Petersburg Police Department requesting the agency's "assistance in retrieving public data from, CrimeReports.com ("CrimeReports") that is currently inaccessible to SpotCrime." (See Decl. of J. Haws, Ex. 9, RS013213-14). The letter continues that "as of March 19, 2010, CrimeReports has cut off access by SpotCrime to the SPPD's data by requiring

special access." (Id.) The "access" to which Mr. Drane refers was a change to Public Engines' computer systems that successfully, albeit temporarily, defeated ReportSee's scraper. (Decl. of S. Meyers, ¶¶ 15-18).

ReportSee argues that "SpotCrime simply seeks equal treatment under the public records laws and requests that it receive the requested crime data twice a day . . . whether that access is directly through SPDD or through CrimeReports as SPPD's agent." Id. In other words, ReportSee demands that this police department either find a way to provide ReportSee with Public Engines' De-Identified Data, directly or through Public Engines, and in violation of its contract with Public Engines,[9] or face a lawsuit. When ReportSee did this, Mr. Drane knew that Public Engines' contracts with its law enforcement customers limited the use or disclosure of De-Identified Data. (Decl. of J. Haws, Ex. 3, RS022769.) Public Engines' customers should not be faced with demands that they either reverse engineer Public Engines' software products or be sued.

ReportSee makes these threats to Public Engines' customers under the auspices of state public disclosure laws, with Mr. Drane boasting that when Public Engines' law enforcement customers do not provide their data to SpotCrime.com, ReportSee "hire[s] a local law firm to press the issue . . . It's time consuming, but our success rate is close to 100%." (Id.) And although he pressures Public Engines' customers about their obligations to produce De-Identified Data under public records laws, he himself has no idea whether such laws require disclosure, and has not sought legal counsel on the subject. (Decl. of J. Haws, Ex. 1, Dep. of C. Drane at 186:9-

[9] Under Section 3.3 of the Terms of Service, law enforcement agencies acknowledge that "the Services, the structure, organization and source code of the foregoing, and the selection, compilation, and analysis of all data in the Licensed Products constitute valuable Intellectual Property of Public Engines." (See Compl., Ex. 1.) Public Engines' law enforcement clients further agree not to "reverse engineer, decompile, disassemble, or otherwise derive or determine or attempt to derive or determine the source code (or the underlying ideas, algorithms, structure or organization) of the Services," or otherwise use Public Engines' proprietary data in an unauthorized way. Id.

24, 190:25-191:6; 193:10-194:6.) These communications are improper and interfere with Public Engines' contracts and its relationships with its customers.

7. Public Engines' Claims are Not Preempted by the Copyright Act.

ReportSee wrongly claims that Public Engines' CFAA and breach of contract claims are preempted by federal copyright law. (Opp'n Mem. at 34-36, 38.)

As a preliminary matter, the doctrine of preemption only applies to state law claims, not other federal claims, like the CFAA. See Lacour v. Time Warner, Inc., 2000 WL 688946, at *3 (N.D. Ill. 2000) ("the question whether one federal law takes precedence over another does not implicate the Supremacy Clause; therefore, preemption is not the applicable doctrine in these circumstances.").[10]

With regard to Public Engines' state law breach of contract claim, it would only be preempted if "(1) the work is within the scope of the 'subject matter of copyright' as specified in 17 U.S.C. §§ 102, 103; and (2) the rights granted under state law are equivalent to any exclusive rights within the scope of the federal copyright as set out in 17 U.S.C. § 106."[11] Ehat v. Tanner, 780 F.2d 876, 878 (10th Cir. 1985), cert. denied, 479 U.S. 820, 107 S. Ct. 86 (1986). "If a state cause of action requires an extra element, beyond mere copying, preparation of derivative works, performance, distribution or display, then the state cause of action is qualitatively different from,

[10] ReportSee's reliance on Dastar Corp. v. Twentieth Century Fox Film Corp., 539 U.S. 23 (2003) is inapposite; Dastar was not a preemption case. In Dastar, the Court considered how to limit causes of action under the Lanham Act so that it could be read in harmony with federal copyright law. Id. at 33-38. As discussed in more detail above, the CFAA addresses different harms than those addressed by federal copyright law. Beyond copying and distributing, Public Engines' claim under the CFAA alleges extra elements such as accessing a computer, without authorization or exceeding authorized access, knowing transmission of a program, code, or command, and intent to defraud or otherwise commit wrongdoing.

[11] 17 U.S.C. § 301(a) itself provides that "On and after January 1, 1978, all legal or equitable rights that are equivalent to any of the exclusive rights within the general scope of copyright as specified by section 106 in works of authorship that are fixed in a tangible medium of expression and come within the subject matter of copyright as specified by sections 102 and 103, whether created before or after that date and whether published or unpublished, are governed exclusively by this title. Thereafter, no person is entitled to any such right or equivalent right in any such work under the common law or statutes of any State."

and not subsumed within, a copyright infringement claim and federal law will not preempt the state action." Gates Rubber Co. v. Bando Chem. Indus., Ltd., 9 F.3d 823, 847 (10th Cir. 1993).

The fact that a legal dispute involves copyrighted or copyrightable material will not itself render a dispute subject to copyright law, let alone preempt it. For example, in Image Software, Inc. v. Reynolds and Reynolds Co., 459 F.3d 1044, 1048 (10th Cir. 2006), the Tenth Circuit recognized that not all contract disputes that "just happen[] to involve copyrighted material" are sufficient to grant a federal court jurisdiction. The court went on to quote Nimmer on Copyright which states that for federal jurisdictional purposes, some of the most difficult procedural problems arise in the context of "factually related copyright and contract claims." Image, 459 F.3d at 1049 (quoting Melville B. Nimmer & David Nimmer, Nimmer on Copyright § 12.01[A], at 12-4 (1999)). Furthermore, "[s]uch claims characteristically arise where the defendant held a license to exploit the plaintiff's copyright, but is alleged to have forfeited the license by breaching the terms of the licensing contract." Id. (quoting Nimmer on Copyright § 12.01[A], at 12-4 (1999)). These statements implicitly recognize that causes of action for breach of contract, among others, are not preempted merely because copyrighted or copyrightable material is present in the underlying facts.

Public Engines' claims for breach of contract each involve an extra element beyond mere copying. Public Engines' breach of contract claim has very little to do with the fact that the suit involves material that may be copyrightable. Beyond copying or using Public Engines' data, Public Engines must prove extra elements such as an agreement or contract between ReportSee and Public Engines and that Public Engines breached that agreement—for example by deploying an automated scraper to harvest data from the CrimeReports.com website.[12]

[12] ReportSee states, with no analysis, that Public Engines' other state law claims are preempted. (Opp'n Mem. at 38.) Each additional state law claim requires proof of an extra element beyond mere copying and consequently is not preempted.

E. An Injunction Does Not Raise Any First Amendment Concerns.

1. Public Engines is Not a State Actor.

The overriding consideration in determining whether a private entity is functioning as a state actor is whether "'the conduct allegedly causing the deprivation of a federal right'" is "'fairly attributable to the State.'" See Gallagher v. Neil Young Freedom Concert, 49 F.3d 1442, 1447 (10th Cir. 1995) (citing Lugar v. Edmondson Oil Co., 457 U.S. 922, 937 (1982)). The purported deprivation of a federal right at issue here is Pubic Engines' enforcement of its Terms of Use, which prohibit ReportSee from misappropriating data from CrimeReports.com and republishing it for ReportSee's commercial use and profit. (See Opp'n Mem. at 53 ("Public Engines' conduct and its present attempt to enforce its TOU violates the First Amendment . . .").) Merely forming a contractual relationship with a governmental agency does not make Public Engines a state actor. See e.g., Gallagher v. Neil Young Freedom Concert, 49 F.3d 1442, 1453 (10th Cir. 1995); Simescu v. Emmet County Dept. of Social Services, 942 F.2d 372 (6th Cir. 1991); Atkinson v. B.C.C. Associates, Inc., 829 F.Supp. 637 (S.D.N.Y. 1993) (same). In fact, ReportSee does not cite a single Tenth Circuit case in which the court found the private entity at issue was a state actor.[13] Instead, ReportSee cobbles together principles from disparate and remote areas of law to support the novel proposition that a defendant, like ReportSee, can misappropriate the data of a private competitor to sell at a profit, under the guise of the First Amendment.

Public Engines is not a state actor under the public function test, the state compulsion test, the nexus test, or the joint actor test. Gallagher v. Neil Young Freedom Concert, 49 F.3d 1442 (10th Cir. 1995). First, because the dissemination of information about crimes is not the

[13] See Johnson v. Rodrigues, 293 F.3d 1196, 1206 (10th Cir. 2002) (holding that an adoption center and adoptive parents did not act under color of state law); Gallagher v. Neil Young Freedom Concert, 49 F.3d 1442, 1458 (10th Cir. 1995) (holding that the "pat-down searches conducted at the Huntsman Center . . . cannot be fairly attributable to the State of Utah under any of the tests for state action").

exclusive province of the government, the Court cannot find that Public Engines is a state actor under the public functions test. See Johnson v. Rodrigues, 293 F.3d 1196, 1203 (10th Cir. 2002).[14] Second, the fact that law enforcement agencies have the ability to correct inaccurate entries on CrimeReports.com does not transform Public Engines into a state actor under the "nexus test." (Opp'n Mem. at 50.)[15] Third, the minimal involvement a law enforcement agency has in making corrections to inaccurate entries on CrimeReports.com does not begin to meet the "symbiotic relationship test." (Opp'n Mem. at 51.) Courts interpret this test narrowly, and regularly reject state actor claims even in the face of "extensive state regulation, the receipt of substantial state funds, and the performance of important public functions." Gallagher, 49 F.3d

[14] ReportSee admits proving a function is "exclusively reserved" to the state is "an arduous standard to satisfy." Id. (cited in Opp'n Mem. at 48). Even assuming the doubtful proposition that receiving 911 and other police reports is the exclusive prerogative of law enforcement agencies, Opp'n Mem. at 49, Public Engines has not taken over this role. Public Engines takes crime report data already amassed by law enforcement agencies and then de-identifies that data for distribution to the public via its own website. There are numerous private entities that take on the function of distributing crime data to the public, including ReportSee and its competitors, Raidsonline.com and Omega. (See Decl. of G. Whisenant, ¶ 4.); Johnson, 293 F.3d at 1203 (noting that "four and a half pages of adoption agencies are listed in the Salt lake City Yellow Pages," empirically showing that adoption centers are not the "exclusive prerogative of the state").

[15] The existence of a contract between a private entity and a governmental agency does not "transform the conduct of that entity into state action." See Gallagher v. Neil Young Freedom Concert, 49 F.3d 1442, 1448 (10th Cir. 1995). "Private corporations whose business depends primarily on contracts to build roads, bridges, dams, ships, or submarines for the government" do not become state actors by virtue of their "total engagement in performing public contracts." Rendell-Baker v. Kohn, 457 U.S. 830, 840-41 (1982). Furthermore, a governmental entity can approve or provide minimal supervision over the initiatives of a private entity without rendering that private entity a state actor. Gallagher, 49 F.3d at 1448. Any action by the Public Engines to enforce its Terms of Use is independent of the state's minimal regulation of the CrimeReports.com website through the use of the "Admin Tool." (Supp. Decl. of G. Whisenant, ¶¶ 13-15.) There is not a sufficient nexus between the state and Public Engines to conclude that its choices are "in law . . . that of the State." Rendell-Baker, 457 U.S. at 840.

at 1451.[16] Fourth, Public Engines does not satisfy the "joint action" test because there is no evidence that it has "acted in concert in effecting a particular deprivation of constitutional rights" and "substituted the judgment of a private party for that of the [governmental official] or allowed a private party to exercise state power." Gallagher, 49 F.3d at 1454.

In short, ReportSee faces a heavy burden in showing that Public Engines is a state actor. It has not begun to meet that burden in this case. The First Amendment therefore has no application whatsoever.

2. An Injunction that Prohibits ReportSee from Misappropriating Public Engines' Data and Interfering with its Business Would Not Violate the First Amendment.

Even assuming ReportSee could clear the state actor hurdle, ReportSee's First Amendment argument still fails. ReportSee cites no persuasive authority for the proposition that Public Engines must provide ReportSee free access to its crime report data to comply with the First Amendment. ReportSee's reliance on Legi-Tech v. Keiper, 766 F.2d 728 (2d Cir. 1985), is misplaced. In Legi-Tech, the Second Circuit considered the First Amendment implications of a statute which prohibited companies from subscribing to a state-run database, LRS, and republishing its database information for profit. Id. at 731-32. The Court did not hold the statute unconstitutional; it lacked enough facts to determine whether Legi-Tech had other ways of accessing the proposed legislation contained in the database. Id. at 733. The fact of "central importance" was whether the statute created a monopoly over legislative information, or whether Legi-Tech could obtain the legislative information on "substantially the same terms as LRS." Id. at 733. If access was comparable, there was no First Amendment violation.[17] As explained

[16] To meet the "symbiotic relationship test," the law enforcement agencies with whom Public Engines' contracts must have "insinuated itself into a position of long-term interdependence" with Public Engines. Johnson v. Rodrigues, 293 F.3d 1196, 1204 (10th Cir. 2002). ReportSee cannot begin to show this, and use of a software editing tool does not come close. (Supp. Decl. of G. Whisenant, ¶¶ 13-15.)

[17] The Court also remanded the case to consider whether Legi-Tech had to pay an additional amount in subscription fees as a competitor. Id. at 736.

further below, ReportSee has comparable access to crime report data as the general public and consequently there is not a First Amendment issue here.

Consistent with the analysis in Legi-Tech, the First Amendment does not allow the press to receive special access to governmental information; it only has a right of access consistent with that provided to the public. Houchins v. KQED, Inc., 438 U.S. 1, 11 ("the First Amendment does not guarantee the press a constitutional right of special access to information not available to the public generally") (citing Branzburg v. Hayes, 408 U.S. 665, 684 (1972)); Legi-Tech, 766 F.2d at 734 ("The Supreme Court has squarely held that the government may not single out the press to bear special burdens, even if evenhanded imposition of the identical burdens would be constitutionally permissible."). ReportSee's own allegations prevent it from arguing that its access is more limited than the public's access. While remaining in full compliance with CrimeReports' Terms of Use, ReportSee can access crime data from law enforcement agencies through multiple means: from law enforcement agencies with public feeds; by creating software and services comparable to those provided by CrimeReports.com and offering them as a vendor; by making public disclosure requests; by going to the police station and reviewing documents; or even by viewing (but not appropriating for commercial use) the data from Crimereports.com. (See Opp'n Mem. at 6-7.) This is the same use provided to the public.

There is nothing in Public Engines' Terms of Use which would prevent a law enforcement agency from contracting with Public Engines and providing ReportSee with access to its raw data. (Decl. of G. Whisenant, ¶ 5.) With this preliminary injunction motion, Public Engines asks the Court to require ReportSee, as a member of the press, to comply with the Terms of Use also imposed on the public. The First Amendment does not require that the press have the easiest or most convenient access to public information, just access to information. See 16A Am. Jur. 2d Constitutional Law § 497 ("The First Amendment does not guarantee to the press a

constitutional right of special access to information or places not available to the general public."). ReportSee is asking the Court to allow full-scale misappropriation of data under the guise of the First Amendment; a position for which there is no constitutional basis.

CONCLUSION

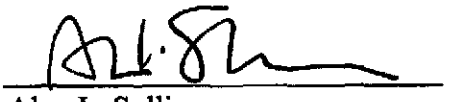
Public Engines respectfully requests that the Court grant its motion for preliminary injunction enjoining defendant, its officers, directors, employees, agents, and affiliates from (a) accessing or making any commercial use of the De-Identified Data generated from Public Engines' Publisher software; (b) making any commercial use whatsoever of any information from CrimeReports.com including, without limitation, crime report data that appears on the website; and (c) contacting or communicating with any of Public Engines' law enforcement customers to obtain, or to suggest that ReportSee has a right to obtain, any data or other output from Public Engines' Publisher software. Public Engines also requests that the Court direct ReportSee to 1) permanently delete from its collection of websites, including the SpotCrime.com website, all information that was previously misappropriated from Public Engines; and 2) contact all third parties to whom it has distributed information that was misappropriated from Public Engines and direct them to delete the information.[18]

Public Engines has met each of the required elements for issuance of this preliminary injunction.

[18] ReportSee has not responded to Public Engines' argument that no bond should be necessary, because (i) the Terms of Use state that security is not required, (ii) ReportSee is unlikely to incur or suffer any costs associated with the injunction, and (iii) any costs ReportSee might suffer was brought about by its own conduct. (Supp. Mem. at 30). ReportSee certainly has not identified or quantified any such costs. On this basis, no bond should be required.

DATED this 25th day of May, 2010.

Snell & Wilmer L.L.P.



Alan L. Sullivan
Todd M. Shaughnessy
J. Elizabeth Haws
Attorneys for Plaintiff

CERTIFICATE OF SERVICE

I certify that on the 25th day of May, 2010, a true and correct copy of the Reply Memorandum in Support of Plaintiff's Motion for Preliminary Injunction has been served by United States mail and by email on the following:

Joshua A. Glikin
29 W. Susquehanna Ave.
Suite 600
Towson, MD 21204
glikin@bowie-jensen.com

Jeffrey J. Hunt
David C. Reymann
Parr Brown Gee & Loveless
185 South State Street
Suite 800
Salt Lake City, UT 84111
jjh@pwlaw.com
dreymann@parrbrown.com

Walter Diercks
Rubin, Winston, Diercks, Harris & Cooke, L.L.P.
1201 Connecticut Ave., NW
Suite 200
Washington, DC 20036
wdiercks@rwdhc.com