Jeffrey J. Hunt (5855)
David C. Reymann (8495)
PARR BROWN GEE & LOVELESS
185 South State Street, Suite 800
Salt Lake City, Utah 84111
Telephone: (801) 532-7840
Facsimile: (801) 532-7750
Email: jhunt@parrbrown.com
dreymann@parrbrown.com

Joshua A. Glikin (*pro hac vice*)
BOWIE & JENSEN, LLC
29 West Susquehanna Avenue
Suite 600
Towson, Maryland 21204
Telephone: (410) 583-2400
Facsimile: (410) 583-2437
Email: glikin@bowie-jensen.com

Walter E. Diercks (*pro hac vice*)
RUBIN, WINSTON, DIERCKS, HARRIS, & COOK, LLP
1201 Connecticut Avenue NW, Suite 200
Washington, D.C. 20036
Email: wdiercks@rwdhc.com

Attorneys for Defendant ReportSee, Inc.

IN THE UNITED STATES DISTRICT COURT
DISTRICT OF UTAH, CENTRAL DIVISION

PUBLIC ENGINES, INC., a Delaware corporation, Plaintiff, vs. REPORTSEE, INC., a Delaware corporation, Defendant.	**DEFENDANT'S MEMORANDUM OPPOSING PLAINTIFF'S MOTION FOR PRELIMINARY INJUNCTION.** Case No. 2:10-cv-317 Judge Tena Campbell

Table of Contents

For the reasons explained in this Memorandum of Law (the "Opposition Brief") submitted by Defendant, ReportSee, Inc. ("ReportSee"), the Court should deny the Motion for Preliminary Injunction by Plaintiff, Public Engines, Inc. ("Public Engines").

I. INTRODUCTION

The allegations in Public Engines' Complaint and evidence and arguments presented in its Memorandum in support of its Motion (the "Moving Brief") do not establish that Public Engines has a substantial likelihood of succeeding on the merits of any of its claims, that it would suffer irreparable harm in the absence of an injunction, or that any injury to Public Engines outweighs the harm to ReportSee if an injunction is issued. Also, this is a case in which the public interest clearly favors denial of the requested injunction. Public Engines essentially seeks a total victory at the preliminary injunction stage. Its Moving Brief argues that it is likely to succeed on all six claims in its Complaint and the injunctive relief it seeks would encompass every form of relief except for money damages.[1]

After this Memorandum explains why Public Engines does not satisfy the four injunction factors that are its burden to prove, it explains why Public Engines is effectively attempting to use the present Motion to obtain the Court's preliminary stamp of approval on a business model that presents significant *First Amendment* concerns. The Court should find that Public Engines, which works in tandem with its law enforcement agencies to provide an "official" agency website, is a state actor subject to the same Constitutional restrictions as the law enforcement agencies themselves. The Court should not place its preliminary approval on a relationship

[1] The Complaint has a seventh cause of action requesting an injunction, which is in essence a claim for relief.

between the agencies and a private entity that results in the privatization of basic crime data, which is then published only on one "official" law enforcement site that purports to prohibit any member of the media or other business entity from republishing or making any other use of it.

II. FACTS RELEVANT TO THIS OPPOSITION BRIEF

A. Facts regarding ReportSee.

Mark Colin Drane is the founder and sole shareholder of ReportSee. *See* Declaration of Mark Colin Drane (the "Drane Dec."), attached at Exhibit 1, at ¶ 3. In or about 2007, Mr. Drane had the idea to improve the method by which crime information is delivered to the public, and so in late 2007 he started a test site called CrimeBaltimore.com. *See id.* at ¶ 4. He founded ReportSee as a Delaware Corporation in February of 2008, for the purpose of collecting news and user reported data and geo-locating that data on a website using Google Maps type interface. *See id.* at ¶ 5. ReportSee's initial approach was to map news reported crimes for Baltimore. *See id.* at ¶ 6. Subsequently, ReportSee began collecting data from the Baltimore police department mapping system and re-representing the data on a Google map on CrimeBaltimore.com. *See id.*

About a month after forming ReportSee – in or about March of 2008 – the SpotCrime brand was created to use this approach of combining news and police data on a national level. *See id.* at ¶ 7. In about March of 2008, SpotCrime.com began providing daily crime alerts to subscribers through SMS and email. *See id.* SpotCrime now covers more than 300 cities and counties around the nation. *See id.* at ¶ 8. Approximately 98% of SpotCrime's data comes directly from police reports in the form of emails from police, police websites, police mapping vendors and direct delivery from police agencies to SpotCrime's servers. *See id.*

There are approximately 212 police departments around the nation that either supply ReportSee directly with crime data or from which ReportSee obtains crime data from public feeds. *See id.* at ¶ 9. ReportSee uses multiple criteria for requesting data from police agencies. *See id.* at ¶ 10. How an agency is selected depends on the size of the population that the agency serves, the agency's proximity to a SpotCrime media partner, and evidence of the agency's ability to provide data. *See id.* If the data is automatically published on the agency's site, and if the data is easily automated, then ReportSee creates an automation script to get the data. *See id.* Cities that provide fully public feeds in this manner include Dallas, Washington D.C., Orlando, Tampa, Milwaukee, and San Francisco. *See id.*

Agencies without direct data feeds have many different methods as to how they make data public. *See id.* at ¶ 11. Output can vary from .pdf reports, written blotters and in some cases faxed reports. Additional sources include email alerts and email press releases. *See id.* In situations where the police department is reluctant to provide public crime data, ReportSee relies on open access or public information act request laws of the various states to request access to the crime data. *See id.* at ¶ 12. In most cases, ReportSee's efforts our successful – meaning that the Police Agency either provides data directly to ReportSee or instead elects to publish crime data in a fully open format for everyone (including SpotCrime) to access. *See id.*

ReportSee has been the least successful in areas where CrimeReports has a contract with the police department. *See id.* at ¶ 13. Most major metro area police agencies in the United States provide accessible data to SpotCrime. *See id.* at ¶ 14. There are only three major cities in the nation that do not provide any type of fully public crime feed: New York, Seattle and Salt Lake City. *See id.* Both New York and Seattle have indicated intent to create open data feeds

similar to San Francisco and Washington DC, but Salt Lake City has given no indication of its future plans. *See id.* at ¶ 15. In addition to making requests to police departments for crime data, SpotCrime also receives unsolicited requests from police departments seeking to place their data on SpotCrime, at a rate of about one unsolicited request per month. *See id.* at ¶ 16.

ReportSee does not charge the departments a fee to report crime data on SpotCrime.com, nor does it charge the public or require the public to subscribe to any service (although they are able to elect to receive email alerts from SpotCrime). *See id.* at ¶ 17. Instead, ReportSee earns income from entering into contracts with media outlets and by providing a crime mapping widget for those media outlets' websites. *See id.* at ¶ 18. To date, ReportSee has contracted with more than 100 media outlets whose owners include New York Times, Cox, Tribune, Hearst, CBS, Fisher Communications, Newport Television and Belo. *See id.* Even in areas where SpotCrime is the sole mapping provider for agencies, it does not charge any fee for the service. *See id.* at ¶ 21. ReportSee does not have contracts with these agencies and requires no exclusivity with them. *See id.*

Of all the media relationships ReportSee has had over the last few years, it has terminated only one, which was with ABC4 in Salt Lake City. *See id.* at ¶ 19. ReportSee requested the termination on April 27, 2009, because it was not able to obtain data from the Salt Lake City Police Department (for reasons described above) and because the station had entered into a marketing arrangement with Public Engines. *See id.* ABC4 Salt Lake still displays the SpotCrime widget on its website, although ReportSee has had nothing to do with that decision. *See id.* at ¶ 20.

SpotCrime does not know the identities of all third parties to whom it has provided information because third parties may log onto and obtain information from SpotCrime.com for free, much like they can from CrimeReports.com. *See id.* at ¶ 22. ReportSee considers all of its crime data to be public data. *See id.* at ¶ 23. In fact, ReportSee redistribute crime data through RSS feeds and Twitter without any restrictions. *See id.*

ReportSee believes that providing the public with full, unfettered access to all crime data is in the public interest and believes it sets a dangerous precedent that is contrary to the free expression of ideas and criticism, to give police the ability to modify or even delete data that is already available to the general public. *See id.* at ¶ 24. Police are free to issue statements correcting the data, or to add their commentary or responses to commentary or criticism, should police determine that it is necessary. *See id.* As evidenced by the many police departments that have contacted ReportSee, unsolicited, to request to post data on SpotCrime.com, most law enforcement agencies believe that public dissemination of crime data in a timely manner is essential to public safety. *See id.* ReportSee also believes that it is in the public interest to not charge a fee to police agencies, many of which are struggling for funds to provide crime data and mapping services. *See id.* at ¶ 25.

A "scraper" is an industry term for a computer program that looks for information or data – and it is one of many automated means of data collection. *See id.* at ¶ 26. Scrapers and other automated programs are commonly-used methods of information and data collection. *See id.* Scraping is by no means an act that is reserved for internet outlaws or hackers. *See id.* Thus, any implication in the Complaint (whether intended or not) that only unscrupulous businesses and people employ scrapers or other automated data collection means, is inaccurate. *See id.*

For example, Google® launches scrapers, or spiders (another industry term for programs that automate the search and retrieval of data), that look inside virtually every site on the Internet and collect data that Google then indexes on its massive database. *See id.* at ¶ 27. If SpotCrime.com was inoperable on a certain date (so that a user that typed www.spotcrime.com into his or her internet browser was unable to open the site), that user may be able to obtain data from the SpotCrime database on that same date through a Google search because Google indexes, through an automated means of collecting data, more than 100,000 pages from SpotCrime. *See id.* Thus, Google scrapes and stores on its own servers hundreds of thousands of data points from SpotCrime – and it does it automatically, and posts that data to users who seek it in a Google search. *See id.*

In or about early 2008, ReportSee began collecting publicly available and accessible crime data from CrimeReports.com by automated means – a scraper. *See id.* at ¶ 28. ReportSee stopped scraping upon receiving a letter from Public Engines dated June 16, 2008, not because it agreed that Public Engines' Terms of Use were valid or that it agreed to abide by them, or that it believed that the data that had been collected was not public data, but because of the simple economics that favored avoiding a legal fight and continuing to attempt to obtain crime data from police departments across the country, whether or not those departments had a contractual or other relationship with Public Engines. *See id.* Between June of 2008 and July of 2009, ReportSee did not scrape or otherwise collect any data from CrimeReports.com. *See id.* at ¶ 30.

In or about July, 2009, ReportSee again began collecting data from CrimeReports.com by automated means, though a CrimeReports.com window access point on the San Jose Police Department. *See id.* at ¶ 31. ReportSee had made a request to that agency for crime data and

was told, as many agencies have told ReportSee, to obtain the requested data from CrimeReports.com. *See id.* The San Jose Police Department Website had a window, or portal, in which a user could access the CrimeReports.com database from the San Jose Police Department website. *See id.* The portal on the San Jose Police Department website did not contain the CrimeReports.com terms of use at are attached to Public Engines' Complaint in this lawsuit. *See id.*

The San Jose Police Department did post its own terms of use with respect to the CrimeReports portal on the site, but those terms of use did not restrict the collection, use or publication of crime data accessible and obtained through the portal. *See id.* at ¶ 33. A copy of the current San Jose Police Department terms of use are attached to my Declaration at Tab A, and these terms appear to be consistent with the terms of use that were posted on the San Jose Police Department during the times that ReportSee scraped data through the agency's portal. *See id.* (referencing attachment at Tab A).

Because the portal on the San Jose Police Department website provided complete access to the CrimeReports data around the country, ReportSee scraped data for many areas of the CrimeReports database. *See id.* at ¶ 34. CrimeReports provided these same portals or access points to many departments and news outlets without terms of service. *See id.* ReportSee simply elected to use San Jose Police Department as our primary access point. *See id.* ReportSee also has been instructed by various police agencies that are under contract with Public Engines, that ReportSee can and should access the agency's crime data on CrimeReports.com. *See id.* at ¶ 35.

ReportSee stopped collecting data from CrimeReports in late March 2010, after it discovered that CrimeReports.com had placed its Terms of Use on the access window on the San

Jose Police Department site and at least a week prior to being notified of Public Engines lawsuit. *See id.* at ¶ 36. The scraping was stopped to avoid any legal dispute over the issue – albeit unsuccessfully. *See id.*

At no time did the crime data collected from Public Engines' CrimeReports.com database exceed approximately 2% of all of the total crime data on the ReportSee's database. *See id.* at ¶ 37. In addition, as of the date of this Declaration, no crime data that was collected from Public Engines' CrimeReports database is available to the public or for public view on SpotCrime. *See id.* at ¶ 38.

Regarding Public Engines' claims (both expressly and by implication) that its Publisher program is uniquely-developed, very expensive software that gives it a unique capability to "de-identify" crime data, those claims are untrue as Mr. Drane understands them. *See id.* at ¶ 42. Because of ReportSee's success rate in obtaining data directly from police agencies, it also has developed the technical means to de-identify the data. *See id.* Also, because most crime data is recorded in a database and eliminating victim and other personal information from crime data is a relatively simple process, ReportSee has requested each department to provide similar output that is being provided to CrimeReports. *See id.*

It is Mr. Drane's understanding that most RMS and CAD systems used by police departments are built on basic database structures. *See id.* at ¶ 44. Removing the victim data and specific address information has been accomplished through simple database instructions for years by many departments that already supply media outlets. *See id.* Many agencies already publish de-identified data on their websites through this same process and some provide that data directly to ReportSee. *See id.* The figure that Public Engines' Complaint sites for investment in

software that queries police CAD and RMS systems ($3,000,000) is excessively high. *See id.* at ¶ 45. It is not a particularly advanced or difficult process to create software that queries databases and pull out specific information ("de-identified data" for example). *See id.* ReportSee creates software to scrub identifying information from police database reports that are sent to, and it takes about 4-hours to create that software for each brand of CAD or RMS system. *See id.*

Finally, ReportSee has not intended to defraud or mislead anyone by any activity, and disagrees with the proposition that it does not have a lawful right to compete for business with Public Engines – even if that means requesting basic crime data from Public Engines' customers, which are government agencies.

B. Facts regarding Public Engines alleged in the Complaint or adduced during discovery in this Action.

Pursuant to the Court's April 27, 2010 approval of the parties' Stipulated Motion for Entry of Discovery Plan and Scheduling Order (and subsequent approved amendments thereto), ReportSee engaged in document discovery and deposed two witnesses whose Declarations are attached to the Moving Brief, Public Engines' Chief Executive Officer, Gregory Whisenant, and Public Engines' Director of Technical Operations, Steven Meyers. Excerpts from Mr. Whisenant's deposition transcript are attached at Exhibit 2 (hereinafter, the "Whisenant Dep."); excerpts from Mr. Meyers' deposition transcript are attached at Exhibit 3 (the "Meyers Dep.").[2] ReportSee also took a corporate deposition of Public Engines pursuant to Fed. R. Civ. P. 30(b)(6), for which Mr. Whisenant was designated to testify on all matters except for technical

[2] Public Engines designated both deposition transcripts as "Confidential" pursuant to the Protective Order entered by the Court, but has agreed to remove the Confidential designation from the pages of the transcripts that are attached at Exhibits 2 and 3.

information, which was the subject of Mr. Meyers' testimony. The deposition testimony and documents that Public Engines produced reveal important facts that, for the reasons in this Opposition Brief, establish that Public Engines is not entitled to a preliminary injunction.

1. Agencies maintain complete editorial control over crime data published on CrimeReports.com through an "Admin. Tool."

Public Engines' Complaint alleges that law enforcement agencies "desire to maintain control over the information that is released to the public" and that the CrimeReports.com website provides police with a means to provide "information approved and controlled by the agencies themselves." *See* Complaint ¶¶ 11, 13. The Complaint does not explain how CrimeReports.com gives law enforcement agencies "control" over crime data or the level of control that the agencies enjoy. Discovery revealed, however, that through a so-called "Admin. Tool," agencies have the unfettered right to manipulate crime data or delete it altogether, even after the data is published on CrimeReports.com:

> Q. Turning to paragraph 13 of the complaint. In that paragraph there's an allegation about the Public Engines' website being user friendly whose content is limited to information approved or controlled by the agencies themselves. The control portion of that allegation, how is it that the agencies accomplish control?
>
> A. They have complete and unfettered access to the Publisher which is behind their firewall and Public Engines does not have any access to the Publisher under any circumstances. And they also have the ability to log in directly to CrimeReports.com to make changes or temporarily halt the display of information on the website.

Whisenant Dep., Exh. 2, at 78:2-17. When questioned further about the Admin. Tool, Mr. Whisenant explained that it gives agencies, "the ability to log in directly [to] the site to remove, edit or add information as needed." *Id.* at 38:13-15. The Admin. Tool is a selling feature for

CrimeReports.com. For example, in one email a Public Engines salesperson explains to a police lieutenant in Florida that, "[y]ou do have complete control of the data so you will have access to an admin tool where you can delete or change crimes or stop certain crimes from being uploaded." *See* email correspondence attached at Exhibit 4, at p. PE 000361.

According to Public Engines, there are several reasons why police want to maintain tight control over data and the right to manipulate or delete it, such as budgeting or political concerns:

> I think the very nature of crime data is that it is open to interpretation in many respects. As most people might know, there's a lot of argument and debate about crime rates across the country. It's a subject of budgets. It's a subject of hiring chiefs, allocating resources, and even to elect people.

Whisenant Dep., Exh. 2, at 74:12-24. Agencies also want to avoid a "perception issue" that could have "political consequences":

> A. [Discussing agencies' desire to maintain control]: It's not just about the data itself, but it's the perception of crime among the public, so it might not be a public issue per se, but also a perception issue as well.
>
> Q. What is the perception issue, in your understanding?
>
> A. Well, it would be associated with the public safety issue itself, but an individual might visit the website and get a false sense was security or conversely a false sense of danger for anywhere neighborhood they live in or may be visiting if the data is not kept up-to-date. And that potentially there would be legal consequences as well as political consequences for the agency in that regard.

Id. at 76:20-77:10. The police chiefs usually control the Admin Tool and decide who else will have access to it. *See id.* at 79:10-13.

Finally, Public Engines contends that agencies want to maintain control over crime data on CrimeReports.com for "public safety" purposes. The reason, according to Mr. Whisenant, has to do with the two separate agency systems from which Public Engines' "Publisher" program collects data – the "CAD" and the "RMS" systems. Emergency calls to 9-1-1 are typically logged on the CAD and once the police determine that an actual crime may have occurred, the CAD information is logged in the RMS. If an emergency call logged in the CAD does not concern a crime, it is not logged in the RMS. *See* Whisenant Dep., at 31:21-32:13. Agencies want the ability to delete evidence of reports of from the CAD system if they later determine that no crime occurred. *See id.* at 60:12-61:23**.**

2. Public Engines and its agency customers collaborate in responding to and denying ReportSee's requests for crime data.

When data from CrimeReports.com began to appear on SpotCrime.com, Public Engines received complaints from its agency customers. The agencies allegedly complained that "their data" should not be displayed on any website that they could not control:

> [T]he nature of those complaints was that they [agencies] had seen their data, which Public Engines was contractually authorized to produce and display showing up on a third party website that did not have permission to show that data from the agency, and they felt that that was a violation and a shortcoming on the part of Public Engines.

Id. at 59:19-60:1. A representative of the San Jose Police Department, for example, lodged the following complaint:

> [He said that] his understanding was that we had a contractual agreement whereby we would be provided access to this data for display on the Public Engines CrimeReports.com website and that was the only place where it was approved, and it was showing up on a third party website, and he wasn't happy about it.

Id. at 102:8-14. The agencies allegedly told Public Engines they were upset about the data being posted elsewhere because, "they wanted to be able to control" the data. *Id.* at 60:5-6 (also testifying that, "I don't think they [the agencies] would be adverse to having the data show up somewhere will else so long as they had the abilities to go and edit that data and remove it and change it as they saw fit"). Public Engines stated that, "[w]hen you join and go live, we make a commitment to present data to the public in a way that the agency can manage and control. Obviously, if someone scrapes the data from us, it would limit our ability to fulfill our end of the bargain." *See* email from Whisenant to police representative, Exhibit 5, at PE 000096.

Public Engines and its law enforcement agency clients also collaborate in responding to (and denying) ReportSee's requests for crime data from the agencies. For example, in emails to some of its agency clients, Mr. Whisenant summarizes the "key points" that some agencies had been making to deny ReportSee's requests for crime data, including that:

> - CrimeReports.com provides free, unfettered access to the agency's crime data. The agency views this as fulfilling requirements under open records laws.
> - As a vendor to the public, CrimeReports.com is under specific contractual obligations, including (among others) 1) to keep the agency's records up to date; 2) to provide free access to all data; and 3) to not allow advertising.

See, e.g., March 26, 2009, email from Public Engines Sergeant in Jackson, Tennessee, attached at Exhibit 6, at PE 000092 (responding to Sergeant's email that, "the Chief wanted me to contact ya'll and see what over departments cited as far as the FOIA and how they kept from providing [ReportSee] with Data").[3]

[3] The notation at the top of the email stating, "Email Sent to All Customers on Thursday, November 12, 2009, is Mr. Whisenant's notation for purposes of this litigation. Whisenant Dep., Exh. 2., at 134:6-12.

On November 12, 2009, Mr. Whisenant sent an email to all Public Engines agency customers that contained "discussion points you may want to consider in your response if you are contacted" by ReportSee. *See* November 12, 2009, email from Mr. Whisenant, Exhibit 7, at PE 000022.[4] Mr. Whisenant's "discussion points" include three sample scripted responses for agencies to use with ReportSee, two of which are:

> - [Sample 2]. Dear _____: Thank you for your request. We already contract with CrimeReports for that service, and it is publicly available for free, so we don't have any need for additional outlets at this time.
>
> - [Sample 3] [I]n response to an open records request. Dear _____: We have reviewed your request and are declining your request to provide access to a data feed, which is beyond the scope of public records laws. If you would like to view crime data for your neighborhood, you may access it for free at CrimeReports.com.

Id.

The emails produced by Public Engines establish that the agencies took Mr. Whisenant's advice and, in many instances, used his scripts *verbatim* to respond to ReportSee's requests. *See, e.g.*, collection of email responses from agencies to Mr. Whisenant's November 12, 2009, email, attached at Exhibits 8A-8L. For example, one agency responded "I sent [ReportSee] a response very similar to #2 below and have not heard back from them since." *Id.* at Exh. 8C. Another response indicated that, "We were contacted by SpotCrime and used your exact points to deny them access. Thanks for your information!" *Id.* at Exh. 8H.

Mr. Whisenant also used the points from his November 12, 2009, email to create a document on CrimeReports.com letterhead to provide to new agency customers who receive

[4] *See* Whisenant Dep., Exh., 2, at 134:5-17.

ReportSee requests for crime data. *See* Document entitled, "Our Data Sharing Policies and Open Records Requests" at Exhibit 9; *see also* Whisenant Dep., Exh. 2, at 137:11-17 (explaining that the document was created so that Public Engines could, "have something we could send subsequently to new customers as they came onboard").

Finally, after it filed the present lawsuit, Public Engines emailed all of its agency customers to inform them of the lawsuit and to provide new scripted responses for the agencies to use to deny ReportSee's data requests. *See* April 14, 2010, email from Mr. Whisenant, Exhibit 10.[5] The two "[e]xample statements to SpotCrime" that Mr. Whisenant's email gave the agencies to use are:

> ONE
> Thank you for your request. As you know, we are currently providing this information to the public for free through CrimeReports.com. We also understand that Public Engines, which owns CrimeReports.com, has taken legal action against ReportSee, and we are waiting for an outcome on the case before considering alternative publishers.
>
> TWO
> We appreciate your interest. As you know, we are working with CrimeReports.com, who simplifies the process of making this data available to the general public in a way that we can still manage and control. <u>You are welcome to use the site, as it is open and free to the public</u>.

Id. (emphasis added). Public Engines received confirmation from agencies that they planned to use the scripts. *See, e.g.*, April 15, 2010, email from Chief of Police in Cleveland to Public Engines, Exhibit 11 (confirming that, "I will use one of the responses that you have provided").

[5] Public Engines also issued the same statement in a press release to the media via the news wire. *See* Whisenant Dep., Exh. 2, at 140:14-18.

3. The CrimeReports.com Terms of Use do not prohibit business entities, such as ReportSee, from accessing crime data; they purport to prohibit only certain uses of any data obtained.

Paragraph 24 of the Complaint alleges that, "[a]nyone is free to access the information on CrimeReports.com, provided they comply with the website's Terms of Use" – and the remainder of the paragraph explains all the manners in which the Terms of Use (or "TOU") prohibits individuals and businesses from using the data that they obtain from the site. *See* Complaint ¶ 24 (explaining specific prohibited uses and stating that, "[t]he requirements for use of the website are set forth in the Terms of Use for CrimeReports.com, a copy of which is appended hereto as Exhibit 2 and incorporated by this reference") (emphasis added). The TOU also state that "All information provided by a law enforcement agency is offered and owned by that agency. TOU, Exh. 3 to Complaint, at ¶ 6.

Public Engines confirmed during its deposition that its TOU do not restrict access, but instead prohibit business entities from making use of the data that they obtain. *See* Whisenant Dep., Exh. 2, at 90:3-25. Paragraph 1 of the TOU provides in relevant part that:

> 1. PERMITTED USE. Subject to these TOU, Public Engines hereby grants you the right to access and use the Public Engines Sites solely for the following purposes: (i) if you are accessing the Public Engines Sites as an individual, then any and all use of the Public Engines Sites is for your personal, non-commercial use only; or **(ii) if you are accessing the Public Engines Sites on behalf of a business entity, then any and all use of the Public Engines Sites must be for such business entity's internal business purposes in connection with the establishment or continuation of a business relationship with Public Engines.**

TOU, Exh. 3 to Complaint, at p. 1 (emphasis added). Mr. Whisenant testified about the meaning of the above-quoted language:

> Q. Can you explain to me what internal business purposes means?
>
> A. Where it says internal business purposes in connection with the establishment or continuation of a business relationship with Public Engines?
>
> Q. Yes, that's it.
>
> A. That means a contractual agreement, authorization effectively to use the data.
>
> Q. Contractual agreement with Public Engines?
>
> A. Yes.
>
> Q. So unless a business entity has a contractual relationship with Public Engines, these terms of use would prohibit use of the site, of the Public Engines sites?
>
> A. Yes.
>
> Q. What about access? Let's just say a business entity that didn't have a contractual relationship with Public Engines accessed the website. Would these terms of use prohibit that access?
>
> A. No.

See Whisenant Dep., Exh. 2, at 90:3-25.[6]

4. The only agency that terminated its contract with Public Engines did so for reasons that are not exclusive to ReportSee.

Of the more than 800 agencies that Public Engines lists as its exclusive customers, the Complaint alleges that only one terminated its contract as a result of ReportSee's demands for equal access to crime data. *See* Complaint, ¶ 42. ReportSee's demand for data was not, however, the sole reason for the termination by the agency, which Public Engines identified as the Annapolis, Maryland Police Department:

[6] After delivering the unambiguous "no" answer, Mr. Whisenant then requested time to review the TOU to ensure that his answer was accurate. After he was given that time (the deposition was even recessed while he reviewed the TOU), he went back on the record to confirm that his answer was correct – that is, the TOU do not prohibit access in the first place; only use of the data obtained as a result of that access. *See id.* at 91:1-92:3.

> Q. So getting back to Annapolis. Around October of 2009 is when Annapolis cancelled its contract?
>
> A. That's correct.
>
> . . .
>
> Q. Did [the Annapolis police] say that the only reason they were cancelling the contract was because of a threat or actually lawsuit by Reportsee?
>
> A. No.
>
> Q. What else, what other reason might have been given?
>
> A. She indicated that they had been considering building their own tool and that this was the event that pushed them to actually do it, so it was the deciding factor.

Whisenant Dep., Exh. 2 at 55:6-56:2. Mr. Whisenant's testimony is inconsistent with his email from October of 2009, in which he recounts his recent conversation with a representative from the Annapolis Police Department, saying, "they have already built their site and wanted the flexibility, but that the SpotCrime thing basically pushed them over the edge." *See* October 16, 2009, email from Whisenant to other Public Engines employees, Exhibit 12 (emphasis added). Mr. Whisenant also tells his staff that, "we'll shortly have a network-wide legal strategy to roll out." *See id.*

5. ReportSee scraped data from an agency website that posted a portal to CrimeReports data, and the portal did not contain the TOU.

As Mr. Drane's Declaration explains, there is a window or portal to the CrimeReports.com data that exists on the San Jose Police Department (as is common with many Public Engine agency customer sites), through which in or about July of 2009, ReportSee collected crime data. *See* Drane Dec., Exh. 1, at ¶¶ 31-34. At that time – and until the end of

March, 2010, when ReportSee stopped any collection of data through the San Jose portal – the CrimeReports TOU were not posted anywhere in connection with the portal:

> Q. Now, on the San Jose website, there exists . . . a window that would permit a search on Crime Reports directly from the San Jose website; is that correct?
>
> A. That's correct.
>
> Q. Does that window contain Public Engines' terms of use?
>
> A. It does.
>
> Q. Has it always?
>
> A. No.
>
> Q. When were the terms of use then added to the San Jose website?
>
> A. Roughly on March, at the end of March 2010.
>
> Q. How did it come to be that the terms of use got added to that website?
>
> A. I think it was Ken [Myers, the President of Public Engines] who pointed out that we didn't have the terms of use on the widget.

Whisenant Dep., 102:25-103:22. Any data that ReportSee collected from CrimeReports.com through the use of the San Jose Police Department website portal was limited to the data that was already available to the general public:

> Q. Do you know whether when a scraper is used on the database, that scraper can access the data that's no longer accessible on the Crime Reports website?
>
> A. It cannot.
>
> Q. So is it fair to say generally that a scraper can get no more data than . . . an average citizen like you or I can get by logging into the Crime Reports website?
>
> A. Right, that's pretty much the definition of a scraper[.]

Meyers Dep., Exh. 3, at 41:2-3 (only relevant transcript portions attached).

6. Public Engines is alleging that the De-Identified Data has been organized by its proprietary software in a unique way.

In its Complaint, Public Engines alleges that Public Engines provides proprietary software. Complaint ¶ 16. Public Engines further alleges that this proprietary software processes law enforcement agency crime data ". . . to organize them, separate them from confidential information, assign unique categories to the crimes reported as defined by Public Engines, and replace the exact street address with more general coordinate." *Id.* at ¶ 17. Public Engines describes this processed data as "De-Identified Data" and claims to own the "De-Identified Data." *Id.* at ¶ 18.

III. LEGAL STANDARD

To obtain a preliminary injunction, Public Engines must show, "(1) a substantial likelihood of success on the merits; (2) irreparable harm to the movant if the injunction is denied; (3) the threatened injury outweighs the harms that the preliminary injunction may cause the opposing party; and (4) the injunction, if issued, will not adversely affect the public interest." *Wilderness Workshop v. United States BLM*, 531 F.3d 1220, 1224 (10th Cir. 2008) (citation omitted). "[B]ecause a preliminary injunction is an extraordinary remedy, the [movant's] right to relief must be clear and unequivocal." *Id.; see also Systemic Formulas, Inc. v. Daeyoon Kim*, 2009 U.S. Dist. LEXIS 116038 (D. Utah Dec. 14, 2009); *APG Enters. v. Money & More, Inc.*, 2009 U.S. Dist. LEXIS 95852 (D. Utah Oct. 14, 2009). When a moving party has not prevailed on the first two factors it is not crucial to address the second two. *Seroctin Research & Techs., Inc. v. Unigen Pharms.*, Inc., 541 F. Supp. 2d 1238, 1246-47 (D. Utah 2008) (citation omitted).

Preliminary injunctions are "never awarded as of right." *Munaf v. Geren*, 553 U.S. 674 (2008) (citation omitted).

Several types of injunctions are disfavored by the Tenth Circuit and thus, require a stronger showing. Disfavored injunctions include those what would disturb the status quo, those that are mandatory rather than prohibitory, and those that would afford the movant substantially all the relief it would recover if it prevailed at the end of a full trial on the merits. *O Centro Espirita Beneficente Uniao Do Vegetal v. Ashcroft*, 389 F.3d 973, 975 (10th Cir. 2004); *see also Systemic Formulas, Inc. v. Daeyoon Kim*, 2009 U.S. Dist. LEXIS 116038 (D. Utah Dec. 14, 2009). Obtaining a disfavored type of injunction requires a strong showing on likelihood of success on the merits and the balance of harms factors. *O Centro Espirita*, 389 F.3d at 976.

IV. ARGUMENT

A. Public Engines seeks a disfavored type of injunction, which is overbroad.

Public Engines seeks a preliminary injunction that grants it all the relief it seeks in its complaint except, of course, for damages. Although there are six claims in the Complaint, the relief sought by the Complaint, aside from damages, is effectively to: (i) stop any current and prohibit any future collection or use by ReportSee of any data from CrimeReports.com; (ii) require ReportSee to delete all CrimeReports.com data that it has collected; and to (iii) stop ReportSee from contacting or communicating with any law enforcement agencies that are Public Engines customers. The cover Motion seeks injunctive relief that accomplishes all of the above.

The Motion also asks for relief that is facially overbroad. For example, it seeks a mandatory injunction, "directing ReportSee to contact all third parties to whom it has provided information misappropriated from Public Engines and directing them to delete misappropriate[d]

information permanently from their databases[.]"[7] The Court should require Public Engines to make a "strong showing" of likelihood of success on the merits and the balance of harms factors. *See O Centro Espirita*, 389 F.3d at 976.

B. Public Engines Has Not Made a Strong Showing That it is Substantially Likely to Succeed on the Merits of the Claims in its Complaint.

1. CFAA claim (The First Claim for Relief).

There are five independent reasons why Public Engines does not have a substantial likelihood of success on the merits of Count I of its Complaint, which alleges a violation of the CFAA, 18 U.S.C. § 1030. First, Public Engines fails to state a claim for violations of the two sections of the CFAA that are citied in its Moving Brief. Second, Public Engines should be estopped from asserting a violation of the CFAA because it encouraged agencies to direct ReportSee to collect data from CrimeReports. Third, ReportSee's alleged violations of the TOU are not actionable under the CFAA because the statute does not prohibit unauthorized "use" of data obtained from a computer that a defendant had authority to access. Fourth, imposing liability under a federal criminal statute for breach of contract would render the CFAA unconstitutionally vague. Fifth, the CFFA claim being asserted by Public Engines is preempted by the federal Copyright Act, 17 U.S.C. § 101, *et. seq.* (the "Copyright Act").

[7] For example, ReportSee does not have any authority to require third parties to delete any data from their databases, yet Public Engines seeks an injunction requiring ReportSee to "direct" third parties to delete data.

(i) The two CFAA subsections cited in the Moving Brief are not supported by any allegation in the Complaint or evidence submitted to date by Public Engines.

The Moving Brief contends that ReportSee's conduct violates two subsections of the CFAA -- 1030(a)(4) and (a)(5)(A). *See* Moving Brief, pp. 24-25. Section 1030(a)(5)(A) prohibits a person from "knowingly caus[ing] the transmission of a program, information, code or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer." There is no allegation in the Complaint that ReportSee's alleged activities – including scraping activities – caused any damage to Public Engines' computers or servers. *See generally*, Complaint. The Moving Brief and its exhibits do not present any evidence that ReportSee's scraper caused damage to Public Engines' computers. Instead, the Complaint and Moving Brief describe the technical measures that Public Engines employed to attempt to stop ReportSee's scraper from collecting data. Thus, without any allegation or evidence of damage to Public Engines' computers or server as a proximate result of ReportSee's activities, Public Engines cannot succeed on the merits of its claim under Section 1030(a)(5)(A) of the CFAA.

Section 1030(a)(4) prohibits a person from "knowingly with and with intent to defraud, access[ing] a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value [unless the value is less than $5,000 in any one year period]." There are no allegations in the Complaint that ReportSee's activities are fraudulent, nor any allegations of fact that would satisfy the heightened pleading requirements for fraud required by Fed. R. Civ. P. 9(b). The Moving Brief does not explain how or why the alleged violation of the TOU, which is the sole basis of its

CFAA claim, amounts to a fraud. Accordingly, Public Engines has not made a strong showing that it is substantially likely to succeed on the merits of its claims under the two subsections of the CFAA that are cited as the basis for its Motion for Preliminary Injunction.[8]

(ii) Public Engines should be estopped from asserting a CFAA violation.

As explained above, Mr. Whisenant instructs law enforcement agency clients respond to ReportSee's requests for crime data by directing it to CrimeReports. He provides scripts for the agencies to read that tell ReportSee, "you may access [the data you request] for free on CrimeReports.com" [9] and "You are welcome to use the site, as it is open and free to the public."[10] Public Engines sent the second quoted script after it had filed the present action, when it knew that ReportSee sought to collect data to publish on SpotCrime.com. The emails attached to this Opposition Brief establish that the agencies took Public Engines' advice. *See also* Drane Dec., Exh.1 at ¶ 35 (affirming that some agencies under contract with Public Engines referred ReportSee to CrimeReports.com to obtain the requested data).

Thus, at the same time Public Engines is instructing agencies to direct ReportSee to obtain data from CrimeReports.com – knowing full well that ReportSee's purpose for obtaining

[8] Public Engines does not argue that ReportSee violated Section 1030(a)(2) of the CFAA, which prohibits "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtains -- (C) information from any protected computer." Thus, even if it attempted to proceed under that subsection at some later date it cannot do so now because it has not presented argument to meet its burden of proving a substantial likelihood of success on the merits of that claim.

[9] *See* November 12, 2009, email from Mr. Whisenant, Exhibit 7 (emphasis added).

[10] *See* April 14, 2010, email from Mr. Whisenant, Exhibit 10 (emphasis added).

the data is to publish it on SpotCrime.com – it is proceeding with this lawsuit alleging that ReportSee's publication of data from CrimeReports.com violates federal law.[11]

(iii) The CFAA does not impose liability for unauthorized use of information obtained from a computer that a defendant had authority to access.

Recent court decisions that interpret the CFAA deny liability when a defendant's *access* to a computer was authorized but its *use* of data obtained from the computer was not. Although this is an issue of first impression in the Tenth Circuit, this Court should apply the same interpretation to the CFAA because it is consistent with standard articulated by the Supreme Court for interpreting a statute that has both civil and criminal penalties.

The CFAA "is primarily a criminal statute[.]" *LVRC Holdings, LCC v. Brekka,* 581 F.3d 1127, 1134 (9th Cir. 2009). For example, a single violation of the CFAA subsections cited in Public Engines' Moving Brief -- (a)(4) or (a)(5)(A) -- is punishable by fines and imprisonment for up to ten years. *See id.* at § 1030(c)(3)(A) (imposing "a fine under this title or imprisonment for not more than five years, or both" for violating subsection (a)(4)); *see also id*. at § 1030(c)(4)(B) (imposing "a fine under this title, imprisonment for not more than 10 years, or both" if the violation of subsection (a)(5)(A) causes, among other things, loss to the plaintiff in any one year aggregating at least $5,000 in value).

Under the rule of lenity, any ambiguity in a criminal statute must be interpreted narrowly and if a narrow interpretation permits it, in favor of the defendant. *See Leocal v. Ashcroft*, 543 U.S. 1, n.8 (2004) (citing *United States v. Thompson/Center Arms Co.*, 504 U.S. 505, 517-518,

[11] This estoppel argument applies equally to all of the other claims that are based upon ReportSee's use of data obtained from CrimeReports.com, which is every Count in the Complaint except for the Lanham Act claim (the Fourth Claim for Relief in the Complaint).

119 L. Ed. 2d 308, 112 S. Ct. 2102 (1992) (applying the rule of lenity to a tax statute, in a civil setting, because the statute had criminal applications and thus had to be interpreted consistently with its criminal applications)). A criminal statute cannot be interpreted differently in the civil context than it would in the criminal context. *See id.* The rule of lenity therefore applies to interpretations of the CFAA. *Brekka*, 581 F.3d at 1134.

The CFAA is ambiguous because it does not define "authorization" or "authorized access" for purposes of determining the propriety of a defendant's access to a computer. The CFAA does define "[e]xceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled to so obtain or alter." *Id.* at § 1030(e)(6). Because there is no express prohibition in the CFAA against unauthorized use, and because the statute must be interpreted narrowly, the Ninth Circuit held that a person that has permission to access a computer cannot be liable under the statute for misuse or unauthorized use of information obtained from that computer, regardless of the individual's intent *Brekka*, 581 F.3d at 1133-35. In other words, wrongful intent does not automatically revoke access rights for purposes of the CFAA. *See id.*

In *Brekka*, a residential treatment center for adults brought a civil CFAA action against its former employee, a marketing contractor, who used his login information to access the center's computers after his employment was terminated and emailed company documents to himself. *Brekka*, 581 F.3d at 1130. The company alleged violations of subsections (a)(2) and (a)(4) of the CFAA. *See id.* The district court granted summary judgment in favor of the defendant and the Ninth Circuit affirmed, holding that "a person uses a computer "without authorization" under *§§ 1030(a)(2)* and *(4)* when the person has not received permission to use

the computer for any purpose (such as when a hacker accesses someone's computer without any permission), or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway." *Id.* at 1135.

The Court rejected the idea that a defendant can lose authorization to use a computer when it does so with the intent of acting contrary to the computer owner's interest. *See id.* Doing so, it observed, would be to interpret the CFAA broadly even though it is "first and foremost a criminal statute that must have limited reach and clear parameters under the rule of lenity and to comply with the void for vagueness doctrine. *Id.* at 1134 (citation omitted).

Relying on *Brekka*, the United States District Court for the Eastern District of California recently granted dismissal of a CFAA claim pursuant to Fed. R. Civ. P. 12(b)(6) because the complaint, "merely stated] there were limits on how [the defendant] could use [information obtained from plaintiff's computer] by making copies of it or disclosing it to third parties" – but did not contain specific, plausible factual allegations that would establish the defendant's lack of any right to access the plaintiff's computers for any reason. *Aptac, Inc. v. Aptitude Sol'ns*, 2010 U.S. Dist. LEXIS 42109, at *13-14 (E.D. Cal. Apr. 29, 2010).

Also relying on *Brekka*, the United States District Court for the Northern District of California reconsidered its earlier ruling on a CFAA indictment and reversed itself, holding that no CFAA violation occurred when co-conspirators employed by an executive search placement firm accessed and downloaded firm trade secrets, because the defendants had permission to access the database that contained the trade secrets. *United States v. Nosal*, 2010 U.S. Dist. LEXIS 24359 (N.D. Cal. Jan. 6, 2010). The *Nosal* opinion thoroughly reviews the holding and effect of *Brekka* to answer the question, "does an employee act 'without authorization' or 'in

excess of authorized access' if he accesses confidential and proprietary business information from his employer's computer that he has permission to access, but then uses that information in a manner inconsistent with the employer's interests or in violation of other contractual obligations, and . . . intended to use the information in that manner at the time of access?" *Id.* at *8-9 (internal quotations omitted). The answer, the Court held, is "no." *Id.* at *12-13 (quoting *Brekka*, 581 F.3d at 1135). The *Nosal* Court then applied *Brekka* to determine when the CFAA imposes liability for "exceeding authorized access." It held that, "an individual's intent in accessing a computer, be it to defraud or otherwise, is irrelevant to determining whether an individual has permission or is authorized to access the computer" – and therefore an individual cannot "exceed authorized access" by having a particular state of mind. *Id.* at *16.

The Court should apply the Ninth Circuit and California line of cases to the present action because they properly interpret the CFFA in accordance with the rule of lenity, and also because Public Engines' TOU provide that, "[t]his Agreement shall be governed in all respects by the laws of the State of California, USA, without giving effect to its conflict of laws provisions, or any other provisions that would result in the application of a different body of law." *See* TOU, Exh. 3 to the Complaint, § 13. [12]

There cannot be any dispute that the TOU permit access by any business entity, including ReportSee. The Complaint alleges that, "[a]nyone is free to access the information on

[12] The Ninth Circuit and California's district courts are not alone in their narrow interpretation of the CFAA. *See, e.g., Shamrock Foods v. Gast*, 535 F. supp. 2d 1322 (N.D. Ga. 2007); *Brett Senior & Assoc., P.C. v. Fitzgerald*, 2007 U.S. LEXIS 50833 (E.D. Pa. July 13, 2007); *Lockheed Martin Corp. v. Speed*, 2006 U.S. Lexis 53108 (M.D. Fla. Aug. 1, 2006); and *Int'l Ass'n of Machinists and Aerospace Workers v. Werner-Masuda*, 390 F. Supp. 2d 479 (D. Md. 2005) (rejecting CFAA claim because "the gravamen of the [plaintiff's] complaint is not so much that Werner-Masuda improperly access the information contained in [the plaintiff's computer], but rather what she did with the information").

CrimeReports.com"[13] and Public Engines' deposition testimony (quoted above) confirms that the TOU do not prohibit a business entity, even ReportSee, from accessing CrimeReports.com.[14] Public Engines affirmatively instructs its customers to direct ReportSee to access data on CrimeReports.com. Moreover, the Moving Brief does not discuss irreparable harm in terms of access; it contends that harm will result without an order enjoining, "ReportSee's unauthorized use of Public Engines' data " and "Reportsee's publication and commercial sale of data[.]" Whisenant Dec., pp. 13-14 (emphasis added). Accordingly, ReportSee's collection of crime data with an intent to commercialize, publish or sell it falls outside the scope of the CFAA.

(iv) Using the CFAA to criminalize a breach of contract would render the statute unconstitutional.

Another recent California federal district court case illustrates the fourth reason why Public Engines does not have a substantial likelihood of succeeding on the merits of its CFAA claim. In *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009), the California court held that the CFAA would violate the void-for-vagueness doctrine if it were used to criminalize a breach of a website's terms of service or use.

Drew concerned a federal prosecutor's CFAA charge against a defendant for violating the terms of use of the site, www.myspace.com. The Defendant, Lori Drew, created a fake MySpace page that criticized 13-year-old Megan Meier, a classmate of Drew's daughter. *See id.* at 452. The federal prosecutor alleged that Drew's interactions with Meier on the fake MySpace page led Meier to commit suicide. *See id.* A federal jury convicted Drew on only one count – violation of the CFAA – because her actions violated the MySpace website terms of service (to

[13] *See* Complaint ¶ 24.
[14] *See* Whisenant Dep., Exh. 2 at 90:3-25 (quoted in full, *supra*, in Section II (p. 17)).

which Drew had to click "I agree" before creating the fake MySpace page). *See id.* at 453. The California court held that converting the breach of a website's terms into a CFAA violation renders the statute unconstitutionally vague, and it vacated the jury's verdict. *Id.* at 457.

The court recognized that other federal decisions 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." *Id.* at 460 (citations omitted). It determined, however, that such an application would run afoul of the "void for vagueness" doctrine, which requires a criminal statute to "contain 'relatively clear guidelines as to prohibited conduct' and provide 'objective criteria' to evaluate whether a crime has been committed.'" *Id.* at 463-64 (citing *Gonzales v. Carhart*, 500 U.S. 123, 149, 127 S. Ct. 1610, 167 L. Ed. 2d 480 (2007) (additional citations omitted)).

The court held that imposing criminal liability for violating a website's terms of service would not provide sufficient notice of possible violations of the statute, which violates the void-for-vagueness doctrine. *Id.* at 464. For example, the Court held that there is no language in the CFAA that suggests or provides notice that the statute has "criminalized breaches of contract" that "[n]ormally, … are not the subject of criminal prosecution." *Id.* at 464 (citation omitted). Second, the CFAA "would be unacceptably vague" because it would be "unclear whether any or all violations of terms of service will render the access unauthorized, or whether only certain ones will." *Id.* Third, allowing "the website owner – in essence – [to be] the party who ultimately defines the criminal conduct … will lead to further vagueness problems." *Id.* at 465.

The court also found that permitting a website owner to define violations of the CFAA through terms of use would fail to give minimal guidelines to govern law enforcement, which also runs afoul of the void-for-vagueness doctrine. *See id.* at 466. The Court recognized that the

situation "would result in transforming [the CFAA] into an overwhelmingly overbroad enactment that would convert a multitude of otherwise innocent Internet users into misdemeanant criminals." *Id.* (providing examples in the context of the MySpace terms of service). Finally, the court rejected the government's argument that Drew had consciously violated the MySpace terms of service – holding that "if any conscious breach of a website's terms of service is held to be sufficient by itself to constitute intentionally accessing a computer without authorization or in excess of authorization, the result will be that [the CFAA] becomes a law that 'affords too much discretion to the police and too little notice to citizens who wish to use the [Internet].'" *Id.* at 467 (quoting *City of Chicago v. Morales*, 527 U.S. 41, 64 60, 119 S. Ct. 1849, 144 L. Ed. 2d 67 (1999)).

The application of Public Engines' TOU to impose liability under a criminal statute would, for the reasons explained in *Drew*, render the CFAA unconstitutional under the void-for-vagueness doctrine. Public Engines cannot make a strong showing that it substantially likely to succeed on the merits of a claim that hinges on an unconstitutional application of a criminal statute.

(v) The CFAA Claim is preempted by the Copyright Act.

The Complaint alleges that Public Engines owns the "De-identified Data" and that this "De-identified Data" is organized in a unique way using Public Engines proprietary software. Complaint, ¶¶ 16-18. If these factual allegations are assumed to be true for the sake of the instant motion, the "De-identified Data" would copyrightable. In *Feist Publications, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340, 345 (1991), the Supreme Court held that facts are not copyrightable, but an original compilation of facts is:

> The *sine qua non* of copyright is originality. To qualify for copyright protection, a work must be original to the author. Original, as the term is used in copyright, means only that the work was independently created by the author (as opposed to copied from other works), and that it possesses at least some minimal degree of creativity. To be sure, the requisite level of creativity is extremely low; even a slight amount will suffice.

As shown above, the gravamen of Public Engines' CFAA claim is the use by ReportSee of the "De-Identified Data." Congress has specifically preempted all state law claims that are equivalent to those protected under federal copyright law. " '[A] state-law claim is preempted if '(1) the work is within the scope of the 'subject matter of copyright' as specified in 17 U.S.C. §§ 102 and 103; and (2) the rights granted under state law are equivalent to any exclusive rights within the scope of federal copyright as set out in 17 U.S.C. § 106.'" *R.W. Beck, Inc. v. E3 Consulting, LLC*, 577 F.3d 1133, 1147 (10th Cir. 2009). In other words, taking the factual allegations as true, which appear to allege that the Publisher organizes the data in a unique way, rights granted under state law that are equivalent to rights under the Copyright Act are preempted, even with respect to any uncopyrightable elements of the "De-Identified Data," regardless of whether Public Engines registered the copyright for the "De-Identified Data." *Id.*

The Supreme Court also applies this principle to claims under the federal Lanham Act. *See Dastar Corp. v. Twentieth Century Fox Film Corp*, 539 U.S. 23 (2003) (rejecting claim of "reverse passing off" in violation of Section 43(a) of the Lanham Act). In *Dastar*, the Supreme Court held that the Lanham Act only protects the producer of tangible goods that are offered for sale and not the author of an idea, concept of communication embodied in those goods, because ". . . to hold otherwise would be akin to finding that § 43(a) created a species of perpetual copyright, which Congress may not do." *Id.* at 37. Since Public Engines' CFFA claim (as

alleged in the Complaint) is the equivalent of a copyright claim, it cannot rely upon the CFAA to create a new species of perpetual copyright. *See id.*

2. Public Engines does not have a substantial likelihood of success on the merits of its breach of contract claim (the Second Claim for Relief).

To state a claim for breach of contract there must, of course, be a contract. Public Engines is unlikely to succeed on the merits of its breach claim because the TOU did not apply to the scraping activities that are the subject of the present injunction, the Terms of Use cannot form a contract because they are illusory, the TOU state that Public Engines does not own the crime data on CrimeReports.com and the Copyright Act preempts this Action.

ReportSee's automated collection activities were accomplished on the San Jose Police Department website, which contained a portal that permitted the access of CrimeReports data directly from the agency's site. *See* Drane Dec., Exh. 1, at ¶ 35. In fact, the agency directed ReportSee to the portal on the San Jose Police Department website when ReportSee made a request for crime data. *See id.* at ¶ 31. The agency's website contained terms of use that placed no prohibitions on use of the data that could be collected. *See id.* at ¶ 33 (attaching the San Jose terms of service). The window on the agency's site did not contain the Public Engines' TOU until the end of March, 2010 – which is the same time that ReportSee discontinued scraping. *See id.* at ¶ 36 (affirming that scraping stopped at the end of March, 2010); *see* Whisenant Dep., Exh. 2, at 102:25 - 103:22 (stating that the TOU were first posted with respect to the San Jose window "at the end of March"). Thus, the TOU did not apply to the scraping activities that are the foundation for Public Engines' present Motion for Preliminary Injunction.

Even if the TOU had been posted, they could not form a contract because they are illusory. Under Utah law, a contract is illusory when by its terms one party "could unilaterally modify the terms at any time." *Dumais v. American Golf Co.*, 299 F. 3d 1216 (10th Cir. 2002) (holding that an agreement allowing one party an unfettered right to alter the agreement's existence or its scope is illusory and therefore unenforceable) (citations omitted). In *Dumais*, an employee signed an arbitration agreement that bound the employee to the terms of the defendant's handbook, but in the handbook the employer, "reserve[d] the right to at any time change, delete, modify, or add to any of the provisions contained in this handbook at its sole discretion." That language, the court held, rendered the contract illusory and therefore, unenforceable as a matter of law. *See id.*

The CrimeReports TOU contains the following illusory language:

> With respect to your access and use of the public Engines Sites, Public Engines provides its services to you, subject to the following Terms of Use ("TOU"), which may be updated by Public Engines from time to time without notice to you, and which updates become effective when posted. You are responsible for regularly reviewing these terms and conditions.

TOU, Exh. 3 to Complaint, at ¶ 3 of Recitals on p. 1. The Court should find the CrimeReport's TOU illusory and invalid. *See Gull Labs., Inc. v. Diagnostic Tech., Inc.*, 695 F. Supp. 1151, 1154 (D. Utah 1988) (dismissing breach of contract claim that was based upon an illusory contract because, "[i]t is axiomatic that where consideration is lacking, there can be no contract . . . [m]oreover, a void contract is no contract at all; it binds no one and is a mere nullity") (citations omitted); *see also Brekka*, 581 F.3d at 465 (recognizing that it would be

unconstitutional to apply the CFAA when "terms of service may allow the website owner to unilaterally amend and/or add to the terms with minimal notice to users").

Public Engines also is not likely to succeed on a breach claim based upon a contract that proclaims that it does not own the crime data that is the subject of this Action. Paragraph 6 of the TOU cast doubt on Public Engines' contentions throughout the Complaint that it owns the so-called "De-Identified Data," or at the very least, establish that Public Engines' TOU are misleading with respect to information ownership:

> 6. **OWNERSHIP OF LAW ENFORCEMENT AGENCY SUBMITTED CONTENT**. All information provided by a law enforcement agency is offered and owned by that law enforcement agency. Unless otherwise indicated by the law enforcement agency, all data will be retained by Public Engines, Inc. and remain accessible by the general public in accordance with the provisions of this Agreement.

TOU, Exh. 3 to Complaint.

Finally, Public Engines' breach of contract claim is nothing more than a repackaged copyright infringement claim that ReportSee has used the "De-Identified Data." It is a state law claim that is equivalent to those protected under federal copyright law. Therefore, accepting as true the facts alleged in the Complaint for purposes of this motion, Public Engines' breach claim is preempted. *R.W. Beck*, 577 F.3d at 1147. For the sake of avoiding repletion, this same preemption applies to the Third and Fifth Claims for Relief of the Complaint, which are discussed below.

3. Public Engines is not likely to succeed on its Utah Unfair Competition Action claim (the Third Claim for Relief).

To succeed on its claim under the Utah Unfair Competition Statute, Utah Code Ann. § 13-51-103 (the "UUCA"), Public Engines must prove that ReportSee engaged in "unfair competition" – which the act defines as, "an intentional business act or practice that . . . (A) is unlawful, unfair, or fraudulent; and (B) leads to a material diminution in value of intellectual property; and (ii) is one of the following: (A) cyber-terrorism . . . ." *Id.* at § 13-5a-102(4)(A). Public Engines is not likely to succeed on its claim because it does not define, explain or even suggest what "intellectual property" rights it holds in crime data.

The Complaint contains only two conclusory statements regarding "intellectual property." *See* Complaint ¶ 75 (alleging that, "ReportSee has [launched a scraper onto CrimeReports.com computers] for the purposes of obtaining CrimeReports.com intellectual property in the form of data scraped); *see also id.* at ¶ 76 (alleging that "ReportSee's conduct has led to a material diminution in the value of Public Engines' intellectual property"). The Moving Brief does not provide any further explanation. *See* Moving Brief, pp. 26-27.

A conclusory allegation that Public Engines owns "intellectual property" is insufficient as a matter of law for purposes of Fed. R. Civ. P. 8(a). The allegations that Public Engines owns "intellectual property" and that ReportSee's actions "have led to a material diminution in the value of Public Engines' intellectual property" are mere recitations of the elements that it must prove. Those "mere labels and conclusions," however, are not sufficient to survive a Rule 12(b)(6) motion to dismiss. *See, e.g, Bell Atl. Corp. v. Twombly,* 550 U.S. 544, 555 127 S. Ct. 1955, 1974, 167 L. Ed. 2d 929 (2007) ("Factual allegations must be enough to raise a right to

relief above the speculative level" to survive a motion to dismiss). If the only allegations are insufficient to survive a motion to dismiss, they cannot be sufficient to establish a substantial likelihood of success on the merits of a claim for purposes of an injunction.

In any event, the TOU states that "all" of the information provided by the law enforcement agencies is owned by the agencies, so there are no intellectual property rights that Public Engines could own with respect to the crime data. TOU, Exh. 3 to Complaint, ¶ 6.

4. Public Engines is not likely to succeed on its Lanham Act claim (the Fourth Claim for Relief).[15]

The Complaint alleges that ReportSee makes the following statements on its SpotCrime.com website and that the statements are false:

- That ReportSee "obtains the information displayed on the SpotCrime website from police departments, news reports, and other third party sources."
- That "ReportSee has publicly stated that it draws 90% of its data from local police records and in cities where that information is not released, ReportSee gathers the crime reports from local news sources.
- That "ReportSee also claims that its own employees plot the locations of crime reports on Google maps to permit them to be displayed."

See Complaint, ¶¶ 53 & 54. The Complaint then alleges that the statements are false because, "ReportSee does not draw all of its crime report information from local police or news sources." *Id.* at ¶ 55. The Complaint does not allege that ReportSee makes the statement that "all of its crime report information [is] from local police or news sources" – and so the allegation of falsity

[15] This Opposition Brief addresses Public Engines' Lanham Act claim to be responsive to the Moving Brief. The cover Motion to the Moving Brief does not, however, request an injunction to prohibit ReportSee from making any statements that Public contends to be false.

attacks a statement that ReportSee is not alleged to have made. The Moving Brief does not provide any additional evidence to support Public Engines' false advertising claims; it merely repeats the conclusory assertions made in the Complaint.

The Complaint also alleges that ReportSee's statements are false because it "appropriates much of this information from CrimeReports.com, its competitor, through the daily scraping of the CrimeReports.com website." *Id.* (emphasis added). Mr. Whisenant, however, cannot hazard a guess about what the word "much" means:

> Q. Now, in that sentence in paragraph 6 of the complaint, you use the word much to describe much of the information has been misappropriated directly from Crime Reports. How do you, for purposes of this allegation, define the word much?
>
> A (Mr. Whisenant). I think we weren't ready to say all. And we had seen enough from the cities that we looked at and just our own internal studies to suggest to us that it was much. So we don't have a number associated with that.
>
> Q. So less than a hundred percent?
>
> A. Correct.
>
> Q. More than 50?
>
> A. I'd be speculating.

Whisenant Dep., Exh. 2, at 65:1-15. Public Engines cannot establish a substantial likelihood on the merits of a claim that is based upon pure speculation.

Mr. Whisenant also admitted during his Deposition that most of ReportSee's statements that the Complaint recites are not false:

> Q. Why is it false for Reportsee to claim that it obtains information displayed on SpotCrime from news reports and other third-party sources?

> A. (Mr. Whisenant). I would put that as a -- I would say that it's not false, each of those – collectively that's as [sic] false statement. Individually they are not.
>
> Q. So it's not false for Reportsee to claim that they obtained information from news reports?
>
> A. Correct.
>
> Q. It's not false for Reportsee to claim that they obtained information from third-party sources?
>
> A. Correct.
>
> . . .
>
> Q. Is it also Public Engines' claim that it is false for Reportsee to claim that it has employees that plot locations of crime reports?
>
> A. Yes.
>
> Q. What is the basis for the allegation that that claim is false?
>
> A. Well, I think it may be true that SpotCrime's employees plot the locations of Crime Reports on Google maps, but I don't think that's exclusive to what they do, and we've collected evidence to support that position.

Id. at 110:24-112:22.

Finally, the facts in the Drane Declaration establish that, even if ReportSee made the statements alleged by the Complaint, they are true. ReportSee obtains crime data directly from approximately 212 agencies – either through direct fees, emails or other manners. *See* Drane Dec., Exh. 1, at ¶ 9. In fact, at no time did the crime data collected from Public Engines' CrimeReports.com database exceed approximately 2% of all of the total crime data on the ReportSee's database. *See id.* at ¶ 37. Accordingly, Public Engines has not made a strong showing that it is substantially likely to succeed on the merits of its false advertising claim.

5. Public Engines is not likely to succeed on its Hot News Misappropriation Claim (the Fifth Claim for Relief).

Public Engines' "hot news misappropriation" claim also consists of mere recitals to the elements of the claim adopted by the Second Circuit[16] and conclusory assertions that Public Engines is likely to establish each element. *See* Moving Brief, pp. 28-29. These bald and conclusory allegations are insufficient to meet Public Engines' burden.

Public Engines has not explained, for example, why a third party's collection and republication of basic crime data, "threatens Public Engines' incentive to produce this product or service" to law enforcement agencies, which is one of the elements of the tort. *See* Moving Brief, p. 28-29. In fact, its business model sets it apart from the ordinary "hot news" plaintiff – where the timeliness of the reporting may be a key to success. The allegations in the Complaint establish that the key to Public Engines' success is not based on its ability to deliver "hot news" – but rather, because it offers police agencies an automated, hassle-free means to gather and to de-identify crime data, and gives them unfettered control over the data even after it is published.

Also, unlike the traditional "hot news" plaintiff that generates revenue only after the news or data gathering work has been finished (from advertisers, subscribers, etc.), Public Engines gets paid *up front* by the police agencies to create and post the data, for free, to the general public. A hot news misappropriation claim does not fit within the nature of Public Engines' business model and, in any event, Public Engines' recitation of the elements and conclusory statements that it will succeed on its claim do not establish a substantial likelihood of success.

[16] It does not appear that the Tenth Circuit and this Court have adopted or analyzed this tort.

6. Public Engines is not likely to succeed on its Interference with Contract claim (the Sixth Claim for Relief).

Public Engines is not likely to succeed on its tortious interference claim because it has not disclosed all of the terms of the contract with which it contends ReportSee interfered. Public Engines attaches, at Exhibit 1 to the Complaint and Exhibit 1 to the Whisenant Dec., only a portion of its law enforcement agency contract. This portion, called "Terms of Service," repeatedly references an "Order Form" that is not attached to the Complaint or the Moving Brief. For example, the Terms of Service state that the parties are subject to "other business terms" in the Order Form. *See* Exh. 1 to Whisenant Dec., at ¶ 1. The Order Form is referenced in a multitude of other paragraphs in the Terms of Service, including: 2.5, 2.11, 3.1, 5, 6, 7, 12.14, 12.15 (stating that "This Agreement and the Order Form(s) together are a binding contract"). Public Engines cannot meet its burden of proving a substantial likelihood of success in its tortious interference with contract claim when it has not provided the Court or parties with the entire contract.

Nevertheless, the arguments that Public Engines presents in support of its claim also are insufficient. It contends, for example, that ReportSee's requests for agencies to provide equal access to crime data is a tortious interference because ReportSee attempts to "persuade [the agencies] to violate their agreements with Public Engines" by providing the De-Identified Data. Moving Brief, p. 29. For the reasons explained above, however, the agencies have no method of intercepting the De-Identified Data so no amount of persuasion by ReportSee would make a difference.

The tortious interference claim also is premised on the conclusory assertion that Public Engines "knowingly misrepresent[s] to the agencies their obligations under public access laws." A sweeping generality about the applicability and scope of public access laws in every state in the nation cannot pass for evidence, nor can it establish a likelihood of success on the merits.

C. The facts establish that Public Engines is a "state actor" attempting to impose an unconstitutional prior restraint on speech and publication.

Aside from the legal and factual issues that plague each of Public Engines' claims individually, the United States Constitution renders its claims fatally infirm. The facts alleged in the Complaint and obtained during discovery establish that Public Engines' relationship with law enforcement agencies is so intertwined that it has become a state actor. As such, it cannot place any greater restrictions on republication of crime data than the agencies, themselves, could impose.

The *First Amendment* provides that, "Congress shall make no law . . . abridging the freedom of speech, or of the press[.]" "It is no longer open to doubt that the liberty of the press, and of speech, is within the liberty safeguarded by the *due process clause of the Fourteenth Amendment* from invasion by state action." *Near v. Minnesota ex rel. Olson*, 283 U.S. 697, 707, 51 S. Ct. 625, 75 L. Ed. 1357 (1931). The Supreme Court "has interpreted these guarantees to afford special protection against orders that prohibit the publication or broadcast of particular information or commentary – orders that impose a 'previous' or 'prior' restraint on speech." *Nebraska Press, et al. v. Stuart, et al.*, 427 U.S. 539, 556, 49 L. Ed. 2d 683, 96 S. Ct. 2791 (1976). In fact, "'[a]ny prior restraint on express comes to [the Supreme] Court with a 'heavy presumption' against its constitutional validity" and "prior restraints on speech and publication

are the most serious and the least tolerable infringement on *First Amendment* rights." *Id.* at 558-59 (citations omitted). The damage from a prior restraint "can be particularly great when the prior restraint falls upon the communication of news and commentary on current events." *Id.* at 559.

ReportSee, which operates SpotCrime.com, is undoubtedly a member of the press. *See, e.g., Entm't Software Ass'n v. Blagojevich,* 404 F. Supp. 2d 1051, 1056 (N.D. Ill. 2005) (recognizing that even video are "considered protected expression under the First Amendment) (citing *Am. Amusement Machine Ass'n v. Kendrick*, 244 F.3d 572, 579 (7th Cir.. 2001)). For the reasons below, Public Engines' prohibitions against use and publication of crime data is an unconstitutional act by a state actor.

1. Public Engines is a state actor.

Because the *Fourteenth Amendment* prohibits a "State" from making or enforcing a law that abridges the freedoms of the *First Amendment*, only a "state action" that violates the *First Amendment* is unconstitutional. *Near*, 283 U.S. at 707. A private party can be deemed a "state actor" if it, (i) exercises a right or privilege that is "created by the State or by a rule of conduct imposed by the State or a period for whom the State is responsible"; and (ii) "has acted together with or has obtained significant aid from state officials, or because his conduct is otherwise chargeable to the state." *Lugar v. Edmonson Oil co, et al.*, 457 U.S. 922, 937, 73 L. Ed. 482, 102 S. Ct. 2744 (1982). The "state actor test" is satisfied in this case.

(i) Public Engines is exercising a right or privilege and rules of conduct created by persons for whom the State is responsible.

Public Engines' posting of police-supplied crime data on crimereports.com is an exercise of a right or privilege created by more than 800 law enforcement agencies, which certainly qualify as "person[s] for whom the State is responsible." *Id*. Public Engines also exercises a privilege bestowed upon it by law enforcement agencies that are under no affirmative Constitutional obligation to provide data. *See, e.g., Lanphere & Urbaniak, et al. v. Colorado, et al.*, 21 F.3d 1508 (10th Cir. 1994) (holding that there is no "overriding constitutional right of access to government records").[17] In fact, at least according to the TOU, the law enforcement agencies continue to own the data that that they give CrimeReports.com the privilege of displaying. *See* TOU, Exh. 3 to Complaint, § 6.

(ii) Public Engines acts together with or obtains significant aid from state officials, or its conduct is otherwise chargeable to the state.

The Second *Lugar* "state actor" test factor can be analyzed under any one of four tests that the Supreme Court has articulated. They are the: (i) "public function test;" (ii) "state compulsion test," which also is called the "symbiotic relationship test,"; (iii) "nexus test;" and (iv) "joint action test." *Lugar*, 457 U.S. at 939 (listing decisions in which the Court has adopted each test) (citations omitted); *see also, Johnson v. Rodriguez*, 293 F.3d 1196 (10th Cir. 2002) (listing and applying all four tests); *Gallagher v. Neil Young Freedom Concert*, 49 F.3d 1442 (10th Cir. 1995) (also analyzing and applying the tests). The Tenth Circuit in *Gallagher* recognized that "[t]he [Supreme] Court has taken a flexible approach to the state action doctrine,

[17] The agencies, of course, may be obligated to produce data under various state public access laws.

applying a variety of tests to the facts of each case". *Id.* at 1447 (internal quotation marks omitted). The actions and conduct of Public Engines and law enforcement agencies are sufficient to satisfy all four tests.

Public function Test

The Public Function Test requires the Court to "determine whether the state has delegated to a private party 'a function traditionally exclusively reserved to the States." *Johnson*, 293 F.3d at 1203. (citing *Gallagher*, 49 F.3d at 1447). The Tenth Circuit has called this, "an arduous standard to satisfy" because "'[w]hile many functions have been traditional performed by governments, very few have been 'exclusively reserved to the State.'" *Id.* (quoting *Flagg Brothers, Inc. v. Brooks*, 436 U.S. 149, 158, 56 L. Ed. 2d 185, 98 S. Ct. 1729 (1978)). The Tenth Circuit lists examples such as to, "hold elections, perform necessary municipal functions, or run a nursing facility" that are "traditionally the exclusive prerogative of the state." *Id.*; *see also Gallagher*, 49 F.3d at 1457 (listing additional examples, including "operation of a company-owned town" and "management of a city park") (citations omitted).

In *Gallagher*, the Tenth Circuit held that a private entity providing security at a government-owned facility was not performing a function traditionally performed exclusively for the states by analogizing the security firm's duties as those similar to a private investigator who investigates a crime or a citizen who makes a citizen's arrest. *Id.* at 1457. In *Johnson*, the Tenth Circuit likewise held that the plaintiff in the case before it had not presented evidence that the defendant, an adoption center, was the exclusive province of the state (Utah) or the "exclusive means to adopt children in Utah." *Johnson*, 293 F.3d at 1203. Rather, the court observed, "four and a half pages of adoption agencies are listed in the Salt Lake City yellow Pages." *Id.*

Unlike the function of providing the means to adopt children, investigating a crime or performing a citizen's arrest, the collection and imputing of crime report data received from 911 and other police reports is the exclusive prerogative of law enforcement agencies. There is no other original source of crime report data other than the agencies – which according to the TOU, own the crime data. The decision to release data that the agencies own is also, therefore, the exclusive prerogative of those agencies. Public Engines even alleges that it is the "official crime information portal for the law enforcement agencies." Complaint ¶ 21; *see also* ¶ 26 (distinguishing SpotCrime.com as "not an official crime information site"). Law enforcement agencies even have windows or portals to CrimeReport.com on their own websites. Because the agencies delegated to Public Engines functions traditional reserved to the state, Public Engines is a "state actor" under the public function test.

Nexus Test

To establish that a private party is a state actor under the Nexus Test, "a plaintiff must demonstrate that 'there is a sufficiently close nexus' between the government and the challenged conduct such that the conduct 'may be fairly treated as that of the State itself.'" *Gallagher*, 49 F.3d at 1448 (quoting *Jackson v. Metro. Edison Co.*, 419 U.S. 345, 351, 42 L. Ed. 2d 477, 95 S. Ct. 449 (1974)). This usually requires evidence that the state or arm of the state "'has exercised coercive power or has provided such significant encouragement, either overt or covert, that the choice must in law be deemed to be that of the State.'" *Id.* (quoting *Jackson*, 419 U.S. at 351). In *Gallagher*, the nexus test was not established because there was no evidence that any state official participated in the decision by the private security firm to conduct pat-down searches. *Gallagher*, 49 F.3d at 1444. The nexus test was not satisfied in *Johnson* because there was no

evidence that Utah had exercised coercive power or significant encouragement over the adoption center defendant, which made a completely "private decision." *Johnson, 293 F.3d* at 1203-04.

The Nexus Test is established in this case by the existence of the Admin Tool to CrimeReports.com, which gives police the ability to modify or delete published crime report data at any time, and for any reason (or as Mr. Whisenant testified, "as they see fit"). In this case, the agencies not only "participate" or exercise "coercive power" over CrimeReports.com, they actually have the unilateral ability to control the site's data, even after it is published.

Symbiotic Relationship Test

The symbiotic relationship test requires that the "state must have 'so far insinuated itself into a position of interdependence' with a private party that 'it must be recognized as a joint participant in the challenged activity." *Gallagher*, 49 F.3d at 1451 (*quoting Burton v. Wilmington Parking Auth.*, 365 U.S. 715, 725, 6 L. Ed. 2d 45, 81 S. Ct. 856 (1961). After reviewing decisions by the Supreme Court and various appellate courts that have analyzed and applied the symbiotic relationship test, the Tenth Circuit observed that,

> [t]he applicable decisions clearly establish no bright line rule for determining whether a symbiotic relationship exists between a government agency and a private entity. Questions as to how far the state has insinuated itself into the operations of a particular private entity and when, if ever, the operations of a private entity become indispensible to the state are matters of degree.

Id. at 1452 (holding that there was no interdependence between the state and the private security firm); *see also Johnson,* 293 F.3d at 1204 (holding that there were no facts alleged in plaintiff's complaint that would establish the state of Utah had "insinuated itself into a position of long-term interdependence with either the adoption center or adoptive parents") (citations omitted).

Again, the Admin Tool is sufficient, alone, to establish that "the state has insinuated itself into the operations of a particular private entity" for purposes of satisfying the symbiotic relationship test. Public Engines and the agencies also are joint participants in the effort to block ReportSee from obtaining any crime data. The emails produced by Public Engines establish that the agencies not only reported the requests, but request and use the scripted responses that Public Engines provides. This is the quintessential symbiotic relationship.

The Joint Action Test

Under this test, if "state officials and private parties have acted in concert in effecting a particular deprivation of constitutional rights" then the private party is a state actor. *Gallagher*, 49 F.3d at 1453 (citing *Collins v. Womancare*, 878 f.2d 1145, 1154 (9th Cir. 1989) (additional citation omitted)). The Tenth Circuit, in *Johnson*, also recognized that, "[m]ost decisions discussing this concept hold that if there is a substantial degree of cooperative action between state and private officials, or if there is 'overt and significant state participation' in carrying out the deprivation of the plaintiff's constitutional rights, state action is present." 293 F.3d at 1205 (citations omitted). It is not sufficient for purposes of the joint action test for a state official to have merely acquiesced in the actions of a private party. *See Gallagher*, 49 F.3d at 1454 (citing *Malak v. Associated Physicians, Inc.*, 784 F.2d 277, 281-84 (7th Cir. 1986) (additional citation omitted)). In *Gallagher*, the Court declined to hold that the private security firm was a state actor merely because the state remained silent about the type of security that was being provided at the government-owned facility. *See id.* at 1455.

Little needs to be repeated with respect to the evidence that establishes that Public Engines meets the "joint action" test. The agencies complain when "their data" appears on

SpotCrime and demand that Public Engines stop the publication, which it is attempting to do in this Action and through technical measures described in the Complaint, and Public Engines provide scripts for the agencies to read when denying SpotCrime's requests for equal access to crime data.

2. Public Engines seeks to impose unconstitutional prior restraints upon publication.

As a state actor, Public Engines can no more prohibit SpotCrime from using or publishing publicly-released crime data than law enforcement agencies could if the data was displayed on their own web pages. *See Lugar*, 457 U.S. at 937. The *First Amendment* applies to corporations. *See Citizens United v. Federal Election Comm'n,* 558 U.S. ___, 130 S. Ct. 876, 175 L. Ed. 2d 753 (2010) (string citation to line of supporting cases omitted).

The TOU is a means by which Public Engines seeks to impose upon certain speakers prior restraints on speech. "Speech is an essential mechanism of democracy, for it is the means to hold officials accountable to the people." *Id.* at 103 S. Ct. 898 (citation omitted). It is not constitutional to place "restrictions distinguishing among different speakers, allowing speech by some but not others" because "[s]peech restrictions based on the identity of the speaker are all too often simply a means to control content." *Id.* at 899.

Public Engines' Complaint makes it clear, as do the documents produced in discovery and Mr. Whisenant's deposition testimony, that agencies demand complete control over the data to prevent, among other things, "political consequences" that may result from the publication of crime data. The CrimeReports Admin Tool that agencies can use to modify or delete crime information is usually controlled by the police chief, who usually are hired (and fired) by

politicians. Public Engines states that police chiefs began to complain when they saw data posted on SpotCrime because that would mean that that the "content [would no longer be] limited to information approved and controlled by the agencies themselves." Complaint ¶ 13.

Public Engines also contends that agencies seek to control data for "public safety" reasons, such as to correct misreported crimes or entries from the CAD system (which logs 9-1-1 calls). The fact is, however, that the general public is permitted to use the crime data without restriction, and there is no means of notifying them about corrections to entries. In fact, CrimeReports sends out email alerts about crime to members of the public who sign up for the alerts on the CrimeReports.com site, but it does not send out "corrective alerts" when the agencies make corrections. *See* Whisenant Dep., 62:2-63:15. Thus, even if "public safety" were a legitimate purpose for restraining republication of crime data, that purpose cannot be served by CrimeReports.

Regardless of the reason for wanting to correct a crime, however, Public Engines' conduct and its present attempt to enforce its TOU violates the *First Amendment* because it seeks to punish the press for publishing crime data, and to place a prior restriction on publication. *See Florida Star v. B.J.F.*, 491 U.S. 524, 109 S. Ct. 2603, 105 L. Ed. 2d 443 (1989).

In *Florida Star*, the Supreme Court held that that the imposition of civil fines upon a newspaper that published the name of a rape victim was unconstitutional. *See id.* at 534-36. The newspaper had obtained the name from a sheriff's press room, which had mistakenly published it. *See id.* The Court held that "punishing the press for its dissemination of information which is already publicly available is relatively unlikely to advance the interests in the service of which the State seeks to act [protecting a rape victim's identity]." *Id.* at 535. It reasoned that, "where

the government has made certain information publicly available, it is highly anomalous to sanction persons other than the source of its release" and that "'[b]y placing the information in the public domain . . . the State must be presumed to have concluded that the public interest was thereby being served.'" *Id.* (citation omitted). Holding that the newspaper had "lawfully obtained truthful information about a matter of public significance," the Court reversed the imposition of civil fines against the paper for violating a Florida law prohibiting the publication of a rape victim's name. *Id.* at 536-37.

Here, the agencies' decision to authorize the Public Engines "Publisher" software to extract daily data from the agencies' CAD and RMS systems and to publish it on CrimeReports.com establishes that they "must have presumed that the public interest was thereby being served." The Supreme Court in *Florida Star* observed that instead of punishing publication, the government should "extend a damages remedy against the government or its officials where the government's mishandling of sensitive information leads to its dissemination." *Id.* at 535. Applying that principle to this case, the agencies should insist on a means to hold Public Engines accountable if the Publisher software published misinformation or personally-identifying information to CrimeReports.com, rather that attempt to impose a prior restraint on speech or publication. *See id.* Or, if the agencies believed the CAD system information to be unreliable to the point of creating potential "public safety" issues, the agenceis could stop supplying CAD data to Public Engines.

In addition, Public Engines' attempt to prevent SpotCrime from publishing crime data supplied from law enforcement agencies should be viewed with heightened scrutiny because its purpose is to eliminate speech that is at the core of the *First Amendment* – commentary and

criticism. "[P]rior restraints on speech and publication are the most serious and the least tolerable infringement on *First Amendment* rights" and the damage from a prior restraint "can be particularly great when the prior restraint falls upon the communication of news and commentary on current events") *Nebraska Press*, 427 U.S. at 559. Demanding the right to maintain control of crime data to delete data that could have "political consequences" to elected and appointed officials, including police chiefs, is particularly repugnant to the *First Amendment*. In this case, the police chiefs, themselves, control the access to the crime data 'delete' key on the Admin Tool.

Finally, the fact that Public Engines has concerns that ReportSee is "free riding" on its database does not justify is imposition of a prior restraint on publication. A decision by the Court of Appeals for the Second Circuit concerning a government-controlled database of legislative information is on point. *See Legi-Tech, Inc. v. Keiper*, 766 F.2d 728 (2d Cir. 1985). In *Legi-Tech*, a legislative commission of the State of New York offered a public "Legislative Retrieval Service" known as the "LRS" – which was a computerized database that contained the full text of legislation pending before the New York Legislature and summaries of other information. *See id.* at 731. The LRS was available to all members of the general public who subscribed to the service (for a small fee). *See id.* The Plaintiff, Legi-Tech, was a private corporation that operated its own computerized information retrieval service that contained information about New York and California legislation. *See id.*

The state refused to permit Legi-Tech to subscribe to the LRS and then passed a law that prohibited subscriptions by any entity "which offers for sale the services of an electronic information retrieval systems which contains data relating to the proceedings of the legislature."

Id. LegiTech sued, arguing that restricting its access or use of the LRS information that was available to members of the general public was unconstitutionally discriminatory and in violation of its right of publication under the press clause of the *First Amendment*. *See id.* The state argued that it was only trying to restrict competitors from "free riding" and from retransmitting the data at lower prices, which it argued would put the LRS out of business. *See id.* The state also argued that, because it had no obligation to publish the legislative data in the first place it could set restrictions on who could subscribe to, use and republish the LRS information. *See id.*

The Second Circuit held that the state's actions were unconstitutionally discriminatory. The court observed that, "[t]he evils inherent in allowing government to create a monopoly over the dissemination of public information in any form seem too obvious to require extended discussion. Government may add its own voice to the debate over public issues . . . but it may not attempt to control or reduce competition from other speakers." *Id.* at 733 (citations omitted). It also explained that, "[w]hen the state creates an organ of the press, as here, it may not grant the state special access to governmental proceedings and information and then deny to the private press the right to republish such information. Such actions are an exercise of censorship that allows the government to control the form and content of the information reaching the public." *Id.*

CrimeReports.com, which claims to be the "official" crime reporting site for more than 800 law enforcement agencies, is effectively an organ of the press created by the agencies. The collaborative effort between police agencies and Public Engines to deny any other member of the press, including SpotCrime.com, the right to republish crime data that is available to the rest of

the general public is unconstitutional for the same reasons explained in *Legi-Tech*.[18] Agencies can decline to publish crime data in the first place but once they disclose data to the public they cannot assert authoritarian control over the data, outlaw and punish "republication" of the data, or contract a private entity to do those things for them.

D. Public Engines is not likely to suffer irreparable harm in the absence of an injunction.

Public Engines contends that it will suffer irreparable harm without an order placing a prior restraint against SpotCrime from contacting law enforcement agencies that are under contract with Public Engines. The Court should not entertain this overbroad request.

The Moving Brief also contends that without the requested injunction, "[o]ne or more law enforcement agencies is likely to be persuaded by ReportSee's harassment to terminate their agreements with Public Engines[.]" Moving Brief, p. 18. So far, however, Public Engines has only cited to one agency that terminated as a result of its interactions with Public Engines – Annapolis, Maryland. But Annapolis informed Public Engines that it had "already built" its own crime publishing site by the time it terminated its contract. One termination out of more than 800 customers that happened six months ago, for at least one reason that was completely unrelated to SpotCrime – does not establish the likelihood of irreparable harm.

Also, Public Engines can be compensated by damages for any wrongful termination caused by ReportSee. The law enforcement contract terms (at least the incomplete portion attached at Exhibit 1 to the Complaint), are terminable for convenience for any reason by the agencies and, upon such termination, there is a set fee that the agencies must pay – and the

[18] The Second Circuit also rejected the argument that, "because [the government] can constitutionally refuse to provide LRS at all, it may discriminate in offering LRS[.]" *Id.*

agencies have no obligation to renew at the end of each one-year term, or pay any damages for non-renewal. *See* Terms of Service, Exh. 1 to Complaint, at §§ 7.1 and 7.2(a).

Public Engines also contends that it may be forced to sue its own agency customers to enforce its TOU prohibitions against the customers' disclosure of De-Identified Data. *See* Moving Brief, p. 18. That fear lacks merit because, again, "[t]he agencies that license the Publisher and associated services from Public Engines do not have the right or technical ability to access the De-Identified Data that is sent by the Publisher to Public Engines servers in Utah." Complaint, ¶ 18.

Public Engines also argues that SpotCrime's scraping and its demands for equal access "threatens both the value of Public Engines' technology and the good will it has earned with hundreds of law enforcement agencies." *Id.* at p. 21. Importantly, the data at issue in this case is what Public Engines publishes for free to the general public – <u>after it is paid</u> by the law enforcement agencies. It strains common sense to argue that millions of people are entitled to use the crime data on CrimeReports.com free of charge, but that ReportSee's same use of the data devalues the Public Engines' technology to the point that it "threatens ultimately to destroy" the company. *Id.* Moreover, during the most recent period in which ReportSee was collecting data from CrimeReports.com, Public Engines' business was booming:

> Q. But you had 500 agencies in the fall of '09?
>
> A. Uh-huh (affirmative).
>
> Q. And you now have -- well, I think in Exhibit 15 is close to 850?
>
> A. Yeah.
>
> Q. So say in the course of six to seven, eight months, is it fair to say you signed up more than 300?

A. Ballpark, yeah.

. . .

Q. So from the date of [Public Engines'] inception through the fall of '09 . . . [Public Engines singed up] about 500 [customers]?

A. Ballpark I'd say that's about right.

Q. And now in the last six or seven months, you've gained another 300 something?

A. Correct.

Whisenant Dep., Exh. 2, at 138:10-139:7. Public Engines' customer boom during the same period that ReportSee was obtaining data from CrimeReports.com calls into doubt the allegation that scraping and unauthorized use of crime data threatens to destroy the company.

E. The Balance of Harms factor weighs against issuing an injunction.

Again, because Public Engines requests a disfavored type of injunction, it must make a strong showing on likelihood of success on the merits and the balance of harms factors. *O Centro Espirita*, 389 F.3d at 976. The harm to ReportSee's reputation if an injunction is issued (which essentially grants all of the requested relief that Public Engines seeks) would be enormous. *See* Drane Dec., Exh. 1, ¶ 39.

If the requested injunction is issued in which ReportSee is found substantially likely to be liable for violating the law in connection with its business activities, police departments and other government officials may not continue trusting SpotCrime with their data. *See id.* It also is possible that a law enforcement agency, knowing of a federal injunction against SpotCrime.com (regardless of the breadth or scope of the injunction), would consider ReportSee's requests for information, much less trust ReportSee with crime data. *See id.*

Also ReportSee's media partners with whom it has contractual relationships may discontinue doing business with ReportSee if an injunction suggested that CrimeReports is or was engaging in the unlawful collection of crime data to which the media partners link on their websites. *See id.* at ¶ 40. If anything, ReportSee's media partners might be concerned about legal liability to Public Engines. *See id.* In addition, it is possible that negative publicity fanned by a press release from Public Engines regarding an injunction may cause SpotCrime's advertisers to pull their endorsement and advertisements, much as advertisers often pull advertising when connected with a controversial topic or celebrity. *See id.*

An injunction also could have serious implications to SpotCrime's ability to secure financing to operate its business – particularly in today's economic climate. *See id.* at ¶ 41. Thus, if there is a party whose entire livelihood is threatened in this case it is ReportSee's, by the negative publicity and potential devastating damage that an injunction could cause to its relationships with police departments, its media partners and advertisers, and to its financial health. *See id.*

F. It is in the public interest to deny the injunction.

It is not in the public interest to permit law enforcement agencies or any of its actors – including Public Engines – to exert a monopoly over the publication, comment, criticism and other use of crime data, particularly in the name of avoiding "political consequences." It also is not in the public interest for law enforcement agencies (or its "official" website operator), who have a "keen interest" in making crime data available to the public, to place prior restraints on republication of crime data otherwise available to the general public for free. The restraint on republication, especially as Public Engines is enforcing it in this action, has broad implications.

For example, 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. The only source for that data would be CrimeReports.com. Applying the same theories that support the claims in the Complaint, NBC would be prohibited from using or republishing any of the data that it could obtain from CrimeReports.com. Doing so would, according to the Complaint, violate a federal fraud statute that also carries criminal penalties, breach the TOU and constitute "hot news misappropriation" and other wrongs.

It is difficult to conceive of a situation that is more contrary to the public interest than a federal order that endorses the practices in which Public Engines engages. Given the serious constitutional implications of Public Engines' actions, the Court should decline to decide on such short notice that SpotCrime is likely to have violated a federal criminal statute or any other law.

V. CONCLUSION

The Court should deny Public Engines' Motion for Preliminary Injunction.

Respectfully submitted,

_____

Joshua A. Glikin
Walter E. Diercks
Jeffrey J. Hunt
David C. Reymann
Attorneys for Defendant ReportSee, Inc.