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

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

Attorneys for Plaintiff

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF UTAH, CENTRAL DIVISION

PUBLIC ENGINES, INC., a Delaware Corporation,

Plaintiff,

vs.

REPORTSEE, INC., a Delaware Corporation,

Defendant.

MEMORANDUM IN SUPPORT OF PLAINTIFF'S MOTION FOR PRELIMINARY INJUNCTION

ORAL ARGUMENT REQUESTED

Case: 2:10cv00317
Assigned To : Campbell, Tena
Assign. Date : 4/9/2010
Description: Public Engines v. Reportsee

Plaintiff Public Engines, Inc. ("Public Engines") respectfully submits this memorandum in support of its motion for a preliminary injunction.

TABLE OF CONTENTS

Page

SUMMARY

Public Engines has invested millions of dollars and three years of effort to develop a website called CrimeReports.com that provides to the public—at no cost—current and complete neighborhood crime data in a user friendly format, with no advertising or editorial commentary. At the core of Public Engines' business are (1) state-of-the-art technology that processes and maps raw police reports from communities nationwide, eliminating sensitive information that should not be disclosed to the public, and (2) contractual relationships with over 800 law enforcement agencies that pay Public Engines to provide specially refined and formatted crime data to public users of CrimeReports.com.

Defendant ReportSee operates a competing website, and it sells crime report data to television stations and other media outlets. It sells advertising on its website. Although it professes to gather crime data by legitimate means, ReportSee in fact surreptitiously scrapes much of it from Public Engines' website, in violation of Public Engines' terms of use, and in violation of federal and state law. ReportSee also aggressively solicits Public Engines' proprietary information from law enforcement agencies and threatens them with suit if they do not immediately agree to turn it over in violation of their contracts with Public Engines.

Public Engines has warned ReportSee repeatedly that its conduct violates the law. Although ReportSee appeared to suspend its scraping operation for a brief period during parts of 2008 and 2009, it surreptitiously resumed the operation in late 2009 and into 2010, using a series of strategies to conceal the nature of its conduct. Public Engines has been able to detect at least some of ReportSee's scraping activity. Each time Public Engines implements a measure to block ReportSee's data scraper, however, ReportSee devises a new strategy to circumvent the measure. Public Engines now seeks a preliminary injunction because it is the only way it can terminate ReportSee's wholesale misappropriation of Public Engines' proprietary data. Without an

injunction, ReportSee will in all likelihood continue its wholesale scraping of the data from CrimeReports.com and then use it to make a profit, while misrepresenting to the public that it has acquired and presented the misappropriated data through its own legitimate efforts. ReportSee's repeated misappropriation of proprietary data is exactly the type of continuing injury that the federal courts have held to be irreparable.

Public Engines is entitled to a preliminary injunction (1) preventing ReportSee from unlawfully misappropriating and then making commercial use of Public Engines' data, (2) preventing ReportSee from interfering with Public Engines' contracts with law enforcement agencies, and (3) directing ReportSee to delete Public Engines' proprietary data from its websites, including SpotCrime.com. This motion is based on the following grounds:

Irreparable injury—ReportSee's daily misappropriation of Public Engines' proprietary data diminishes both the value of Public Engines' technology and the company's continued good will with hundreds of law enforcement agencies and the public. The courts are unanimous that such repeated and continuous acts of misappropriation result in irreparable injury. The facts set forth below show that if ReportSee is not enjoined by this Court, it will in all likelihood continue to scrape Public Engines information so as to make a profit by selling it to others or by displaying it on its website for advertising.

Balance of harms—If the defendant is not enjoined, the value of Public Engines' technology and good will will be diluted and ultimately destroyed. On the other hand, if the Court issues a preliminary injunction, ReportSee's legitimate business interests would not be affected at all. ReportSee has no right to make commercial use of Public Engines' data and no right to interfere with Public Engines' contracts, and so a preliminary injunction will not injure any protectable interest it may claim. Under the circumstances of this case, the threatened injury to Public Engines in the absence of an injunction outweighs any potential harm to ReportSee from the injunction.

Public interest—The issuance of a preliminary injunction would serve the public interests in ensuring performance of contractual obligations and compliance with applicable statutes that protect owners of websites from unauthorized commercial use of website content. An injunction would also preserve the viability of Public Engines' website as a unique, cost-free source of important information having the endorsement of hundreds of law enforcement agencies.

Likelihood of success on the merits—The factual presentation below shows that ReportSee has violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(g), the "cyber-terrorism" provisions of the Utah Unfair Competition Act, Utah Code Ann. § 13-5a-103, and the false advertising provisions of the Lanham Act , 15 U.S.C. § 1125(a). In addition, ReportSee has violated the Terms of Use of Public Engines' CrimeReports.com website; those Terms of Use prohibit, among other things, the commercial use of data on the website and the use of automated scrapers to gather such data. ReportSee is also guilty of "hot news" misappropriation, a common law doctrine that protects the plaintiff's investment in the gathering of time-sensitive data. Finally, the factual presentation below shows that ReportSee has interfered with Public Engines' contracts by threatening law enforcement agencies with suit if they refuse to turn over proprietary information generated from Public Engines' Publisher program and CrimeReports.com application.

STATEMENT OF FACTS

A. Public Engines and CrimeReports.com.

Public Engines serves law enforcement agencies across the United States by providing software and operating a website called CrimeReports.com. (G. Whisenant Decl. ¶ 3.) Public Engines' law enforcement customers vary greatly in size and resources, but nearly all of them use some variety of Computer Aided Dispatch System ("CAD") and Records Management System ("RMS") for the purpose of dispatching officers to the scene of crimes or accidents and

for tracking all of the information related to those crimes or accidents. (G. Whisenant Decl. ¶¶ 4–5.) The information contained in these CAD and RMS systems includes basic information about reported crimes and where they occurred, but also includes information about the victim, details of the crime, information about the law enforcement agency's ongoing investigation, the identity of suspects, and other types of information that law enforcement agencies generally do not share with the public. (G. Whisenant Decl. ¶ 5.) These CAD and RMS systems are sold by dozens of companies and vary widely in age, sophistication, function, and the operating systems they employ. (G. Whisenant Decl. ¶ 6.) All, however, maintain up to the minute information about reported crimes as the data is entered by the agencies that use them. (Id.)

Law enforcement agencies have a strong interest in making available to the communities they serve current and accurate information about crimes and criminal activity in those communities. Providing timely information can provide significant assistance to law enforcement in both solving and preventing criminal activity. At the same time, law enforcement agencies must ensure that certain types of information, such as the identity of suspects, the identity of victims, and details of on-going investigations, remain strictly confidential. CAD and RMS systems are designed for internal use by the law enforcement agency; they are not designed to be accessible to the public. (G. Whisenant Decl. ¶ 7.)

To assist law enforcement agencies, Public Engines has developed an integrated system of software and services that allows the agencies to make incident-level (as opposed to statistical) crime report information available to the public in near real time without compromising the confidential information contained in the agency's CAD and RMS systems. (G. Whisenant Decl. ¶ 8.)

Public Engines' integrated system involves a package of software and services that enable the CAD and RMS systems of law enforcement agencies to be queried so data can be extracted in a designated manner, and then organized, processed, and optimized with the goal of

electronically displaying it in a user friendly format. Public Engines then posts that data on its CrimeReports.com website so it can be accessed by the public for free. The content of Public Engines' website is limited to the information approved by the law enforcement agencies themselves. Public Engines does not comment upon or provide any other information about the individual crime reports, except as required under its contracts with the law enforcement agencies it serves, and the website can therefore serve as an "official" source of agency information. (G. Whisenant Decl. ¶ 9.)

Public Engines began development of this package of software and services in 2007. From that time to the present, Public Engines has invested more than $3 million to develop, maintain, and license these software products. Public Engines currently employs a staff of 35 people who provide a range of services from sales, marketing and support to engineering and operations. (G. Whisenant Decl. ¶ 10.)

Public Engines has entered into contracts with more than 800 law enforcement agencies nationwide. The agencies pay Public Engines a fee for the CrimeReports.com products and services provided by Public Engines. (G. Whisenant Decl. ¶ 11.) As part of each such contract, the law enforcement agency obtains a license to Public Engines' proprietary CrimeReports Publisher (the "Publisher") software. That software is installed on the agency's internal computer networks and interfaces with the agency's CAD and/or RMS systems. Public Engines' staff works directly with law enforcement agency personnel to create custom queries, filters and parsing technology for the Publisher to interact successfully with the CAD and RMS. To date, Public Engines has successfully configured its Publisher program to interact with CAD or RMS systems from more than 60 different vendors. (G. Whisenant Decl. ¶ 12.)

Once configured and integrated, the Publisher processes the data contained in those systems to organize them, extract confidential information, assign unique categories defined by

Public Engines to the crimes reported, and replace the exact street addresses with more general geographical coordinates. (G. Whisenant Decl. ¶ 13.)

This processed data is referred to as De-Identified Data because it omits, among other things, names and addresses for victims and suspects as well as other information that the law enforcement agency wants to keep confidential. The De-Identified Data is sent electronically by the Publisher program to Public Engines' servers in Utah. The agencies who license the Publisher and associated services from Public Engines do not have the right or the technical ability to access the De-Identified Data that is sent by the Publisher to Public Engines. This De-Identified Data would not even exist without Public Engines' proprietary software. Under the terms of the license agreement between Public Engines and the law enforcement agency, the agency owns all of the data contained in the CAD and RMS systems, and Public Engines is required to keep that information strictly confidential. Public Engines, on the other hand, owns the Publisher, associated services, and the De-Identified Data created from the operation of the Publisher. The law enforcement agency is prohibited from reverse engineering or disclosing the intellectual property associated with the Publisher, associated services, and the De-Identified Data. A copy of the Terms of Service applicable to each law enforcement contract is attached as Exhibit 1 to the Declaration of Greg Whisenant.

After the De-Identified Data is sent to Public Engines' servers in Utah, it is further modified by the CrimeReports.com website, and sometimes by Public Engines' staff, so that it can be displayed in a user-friendly graphical form. The CrimeReports.com application scrubs the data and removes artifacts from the data entry process. The application then sends the scrubbed, "blockized" address to Google for geocoding, which produces a latitude and longitude. (A "blockized" address is one that omits the victim's specific street address but locates the crime on a particular block.) This information is then used to place the icon on the CrimeReports.com map interface. Public Engines has entered into an agreement obligating Public Engines to pay

significant sums to Google for providing this service. In some cases, the geocoding from Google fails. If it does, the application rescrubs the data according to more rigorous rules, edits the address at which the crime occurred, and resubmits the data to Google for geocoding. If it continues to fail, the record is quarantined from the other data and categorized as unmappable. If the geocoding succeeds, it is used to place an icon on the CrimeReports.com map interface so that members of the public can see the approximate location of a particular crime on a map. (G. Whisenant Decl. ¶ 15.)

Ultimately, after going through all of these processes, the resulting data produced by Public Engines consists of that information which the law enforcement agency has determined it can properly disclose, has been re-structured and re-formatted in a unique way, and has been encoded with other data to permit it to be located on a map, searched, accessed, and displayed. (G. Whisenant Decl. ¶ 16.)

The data is then made accessible to the general public on Public Engines' website, CrimeReports.com. The computer servers that operate the CrimeReports.com website are all located in Utah. (G. Whisenant Decl. ¶ 17.)

In its contracts with law enforcement agencies, Public Engines agrees to publish this information on CrimeReports.com for the benefit of the agency and the community at no cost to the public. CrimeReports.com does not advertise on its site and does not solicit business from visitors to its site. CrimeReports.com serves as an "official" crime information portal because law enforcement agencies supply the raw data based on rules and limits to which the agencies have agreed. (G. Whisenant Decl. ¶ 18.)

Users of CrimeReports.com are able to search the website by zip code, address, city, or state, and the site displays a street level map. The map is populated with coded "pins" showing the locations of reported crimes. Clicking on a particular pin brings up a modal window that provides more specific information about the reported crime, including the date of the crime and

a general description. A log appears on the left side of the screen with an inventory of the crimes reported in the area; clicking on a particular crime then highlights positions on the map where the crime occurred. Users can search for different types of crimes, over different time periods, in different areas. Users also can download an application to permit access to this information on mobile phones. Users can also access the CrimeReports website through software called a "widget," which is installed by Public Engines on approved third party websites or the law enforcement agency's website. Members of the public may also access the CrimeReports.com website via a link from an email alert sent to them from Public Engines. (G. Whisenant Decl. ¶ 19.)

Attached as Exhibit 2 to the Declaration of Greg Whisenant is a screen shot from CrimeReports.com showing how this information is displayed for an area in downtown Salt Lake City. (G. Whisenant Decl. ¶ 20.)

Without Public Engines, few law enforcement agencies would be able to make this information available in user friendly form. To do so, they would be required to develop technology like the Publisher program to which Public Engines has devoted substantial time and resources, and would be required to employ computer programmers and other employees to process and code the information, license geocoding technology from another company such as Google, and then post this information on a webpage. (G. Whisenant Decl. ¶ 21.)

Anyone may access the information on CrimeReports.com for free, provided they comply with the website's Terms of Use. Those Terms of Use provide that individuals may access the site for their own personal, non-commercial use, and businesses may access the website for the business's internal business use. Users are not permitted to use the site for unauthorized commercial purposes or for commercial communications, and they are expressly prohibited from collecting information or data from the site by automated means. The requirements for use of

the website are set forth in the Terms of Use for CrimeReports.com, a copy of which is attached as Exhibit 3 to the Declaration of Greg Whisenant.

B. ReportSee and SpotCrime.com.

ReportSee also operates a collection of crime-related websites, including SpotCrime.com, that provide information about crimes in various communities in the United States. Like CrimeReports.com, SpotCrime.com displays that information on a map. Like CrimeReports.com, particular crimes are displayed with a "pin" coded to represent different types of crimes; and dragging a cursor over a particular pin displays additional information about the crime. Like CrimeReports.com, SpotCrime.com offers a mobile application, email alerts and access to the data via an embeddable widget for display on third party websites. Like CrimeReports.com, SpotCrime.com may only be used subject to ReportSee's terms and conditions of use. (G. Whisenant Decl. ¶ 23.)

Unlike CrimeReports.com, however, SpotCrime.com is not an official crime information site for law enforcement agencies. Instead, SpotCrime.com sometimes adds commentary about the crime reports it features and includes information about crimes obtained from sources other than law enforcement agencies. SpotCrime.com is primarily geared toward serving various media outlets and the public. To the extent ReportSee has not entered into contractual relationships with law enforcement agencies, the agencies do not have the right to control the type or content of data that appears on SpotCrime.com. A number of the law enforcement agencies with which Public Engines has entered into contracts have complained to Public Engines about the information appearing on SpotCrime.com, indicating their disapproval of De-Identified Data from their jurisdictions showing up on SpotCrime.com. (G. Whisenant Decl. ¶ 24.)

ReportSee has entered contracts with news and media organizations to provide this crime mapping data to them for a fee. For example, ReportSee has entered into such contracts with

Newport Television's subsidiary, ABC4 TV, and perhaps other similar media outlets in Utah. ABC4 TV features a link on its webpage to SpotCrime.com. (G. Whisenant Decl. ¶ 25.)

In its electronic advertising materials, ReportSee claims that it obtains the information displayed on the SpotCrime.com website by employing a staff of employees and contractors who read news accounts, police blotters, and monitor police scanner traffic. ReportSee claims that its users submit information regarding crimes as well. According to ReportSee, its employees then identify the longitude and latitude of the incident to plot its location on a map. (G. Whisenant Decl. ¶ 26.) In reality, however, SpotCrime.com obtains much of the information displayed on its webpage by systematically misappropriating it directly from CrimeReports.com using an automated "scraper," as explained in more detail below. In other words, ReportSee misappropriates information from CrimeReports.com and then sells it to media outlets, including media outlets in Utah. (G. Whisenant Decl. ¶ 27.)

C. "Scraping"

Web scraping is a computer software technique used to extract information from websites. Scraping programs are designed to mimic a human user operating a web browser to gain access to the target website. The program then collects and downloads, or "scrapes," the information displayed on the webpage or contained in the underlying databases for later use. (G. Whisenant Decl. ¶ 28.) Although the scraper imitates a human user to obtain access to the website, unlike a human user, it has the ability to access, obtain and misappropriate the entire body of data resident on the website it is scraping.

Because scraping by a competitor can have devastating effects on the operator of an original website, many commercial websites employ "terms of use" to ensure that the website is not unlawfully and unfairly exploited, and to reserve the benefits of the website to the intended user. The Terms of Use for CrimeReports.com state that users shall not "collect content or information, or otherwise access any Public Engines Sites, using automated means (such as

harvesting bots, robots, spiders, or scrapers) or by bypassing the site's user interface without our permission...." (G. Whisenant Decl. ¶ 30.)

Attached as Exhibit 4 to the Declaration of Greg Whisenant is a screen shot from SpotCrime.com showing the same area as the screen shot from CrimeReports.com in Exhibit 2. A comparison of the two exhibits shows that each of the crime reports appearing on Exhibit 4 was taken from CrimeReports.com. (G. Whisenant Decl. ¶ 29.)

D. ReportSee's Scraping of Data from CrimeReports.com in 2008.

Like most websites, CrimeReports.com maintains an automated log of users and computers that access the website. This log includes the Internet Protocol ("IP") addresses of the computers used by those users to access the website. An IP address is a unique number assigned to a computer or device connected to the Internet. That IP address is recorded when a computer accesses a webpage and Public Engines' computers log those who access its page. The log also includes information about what information in particular was accessed and when. (G. Whisenant Decl. ¶ 31.)

Beginning in the spring of 2008, Public Engines noticed an unusual pattern of user activity on CrimeReports.com. Upon investigation, Public Engines discovered that its De-Identified crime report information was being systematically scraped. (G. Whisenant Decl. ¶ 32.) In addition, Public Engines received a complaint from one of the law enforcement agencies it contracts with that the data it was providing to Public Engines was showing up on the SpotCrime.com website. The agency demanded to know why the information it understood was being accessed and improved by Public Engines for display on CrimeReports.com was being displayed on an unapproved website. (G. Whisenant Decl. ¶ 33.)

The IP address for the computer that was scraping Public Engines' site was 208.109.126.144. A Public Engines employee typed that IP address into a browser to determine the person or business with whom it was associated and discovered that the IP address resolved

to the SpotCrime.com website. Attached as Exhibit 5 to the Declaration of Greg Whisenant is a portion of the log showing the IP address for the computer that was scraping data from CrimeReports.com, and a page showing that IP address is connected to SpotCrime.com. (G. Whisenant Decl. ¶ 34.) This scraping started around March 19, 2008, if not earlier, and continued through early June 2008. (G. Whisenant Decl. ¶ 35.)

On June 16, 2008, Public Engines sent a letter to ReportSee demanding that it immediately cease and desist from any scraping of the CrimeReports.com website. Public Engines advised ReportSee that scraping was a violation of the Terms of Use of the CrimeReports.com website. A copy of that letter is appended hereto as Exhibit 6 to Greg Whisenant's declaration.

In response, ReportSee's attorney contacted Public Engines' attorney, first by voice mail and later by email, and confirmed that ReportSee would immediately cease any scraping of the CrimeReports.com website. A copy of the email dated June 30, 2008 from ReportSee's counsel to Public Engines' counsel is Exhibit 7 to Greg Whisenant's Declaration. A transcript of the voicemail dated June 24, 2008 from ReportSee's counsel to Public Engines' counsel is attached to the same declaration as Exhibit 8.

After that exchange, ReportSee appeared at least temporarily to suspend its scraping of CrimeReports.com. (G. Whisenant Decl. ¶ 38.)

E. ReportSee's Contacts with Public Engines' Law Enforcement Customers.

ReportSee, however, then resorted to other methods to obtain Public Engines' proprietary information. ReportSee began contacting Public Engines' law enforcement agency customers, demanding that they provide the data feed from Public Engines' proprietary Publisher software – that is, the De-Identified Data – directly to ReportSee. (G. Whisenant Decl. ¶ 39.)

Starting in the spring of 2009 and continuing to the present, ReportSee has contacted at least 30 different law enforcement agencies who are customers of Public Engines for this

purpose. ReportSee has contacted the Salt Lake City Police Department, the Salt Lake County Sheriff's Office, and the Utah Attorney General's office, all of which are customers of Public Engines. ReportSee has demanded that these agencies provide ReportSee with the De-Identified Data processed through Public Engines' Publisher program. (G. Whisenant Decl. ¶ 40.)

ReportSee has insisted without any basis that it is entitled to this information under various public records access laws. In fact, however, such public records access laws do not require the automated disclosure of either the crime data or the De-Identified Data that is the property of Public Engines. ReportSee has demanded that the agencies provide this information even though doing so would require reverse engineering Public Engines' software and would constitute a breach of the agency's license agreement with Public Engines. ReportSee also has threatened to sue some of the agencies if they do not provide the requested information. (G. Whisenant Decl. ¶ 41.)

ReportSee stepped up these demands in the fall of 2009. Public Engines received complaints from its law enforcement customers about these contacts, and Public Engines has been required to devote substantial time and resources in addressing these complaints. Some agencies have advised Public Engines that ReportSee has threatened to sue them to get access to this information; some have reported that they have had to obtain legal counsel in order to respond to ReportSee's demands. At least one Public Engines customer terminated its agreement as a result of ReportSee's demands. (G. Whisenant Decl. ¶ 42.)

In October 2009, Public Engines' Chief Executive Officer, Greg Whisenant, called ReportSee's Chief Executive Officer, Colin Drane, to discuss ReportSee's inappropriate contacts with Public Engines' customers and interference with Public Engines' business. Mr. Whisenant advised Mr. Drane that these contacts were seriously damaging Public Engines' business relationships and that Public Engines had lost at least one customer as a result of them. Mr. Whisenant explained that the data ReportSee was demanding was unique to Public Engines, was

not publicly available, was uniquely refined, improved, and assembled by Public Engines, and was not something the agencies were required or allowed to provide under public records laws. (G. Whisenant Decl. ¶ 43.) In response, Mr. Drane acknowledged that ReportSee had made these contacts and that ReportSee was trying to get the information that Public Engines was publishing on CrimeReports.com. But Mr. Drane said that ReportSee would continue to pursue all means to get it. (G. Whisenant Decl. ¶ 44.)

On October 27, 2009, through counsel, Public Engines sent a letter to Mr. Drane demanding that ReportSee stop interfering with Public Engines' business relationships. The letter was not acknowledged by ReportSee. Public Engines continues to receive complaints from its law enforcement customers about harassment from ReportSee and the demands it is making to obtain the data provided to Public Engines as part of its contracts with its customers. (G. Whisenant Decl. ¶ 45.)

F. Resumption of ReportSee's Scraping of CrimeReports.com.

In December 2009, ReportSee again started scraping data from the CrimeReports.com website. From a review of Public Engines' website's user log information, its personnel determined that starting on or before December 7, 2009, an automated scraper began systematically extracting crime report data from CrimeReports.com. The scraper was designed to mimic a user on a computer using a web browser, which would access Public Engines' API (application programming interface) to retrieve the crime data. (S. Meyers Decl. ¶ 4.) Since then, nearly every day at around 1:00 a.m. Mountain Time, ReportSee has scraped CrimeReports.com. The scraper operates by making a series of systemic, electronic API requests for information contained within a rectangular-shaped geographic area defined by longitude and latitude, followed by another request for an adjacent rectangular area, and so on until all of the desired information on CrimeReports.com has been downloaded and saved by ReportSee. (S. Meyers Decl. ¶ 5.)

Initially, the IP address for these requests was 174.129.243.60, confirmed as an address for SpotCrime.com. (S. Meyers Decl. ¶ 6.) Public Engines further verified this by temporarily inserting two dummy crimes into the CrimeReports.com database on January 7, 2010 and five dummy crimes on January 8, 2010. These dummy crimes were fabricated and were not based on police reports. Each of these dummy crimes showed up the next day on SpotCrime's website. For one of the dummy crimes, Public Engines also changed the latitude and longitude of the crime to be incorrect in relation to its mapped location. Attached as Exhibit 9 to the Declaration of Steve Meyers are screen captures from SpotCrime.com showing these dummy reports entered by Public Engines. The dummy crimes inserted on January 8 were time stamped and match the scraping requests tracked in the logs on Public Engines' servers. (S. Meyers Decl. ¶ 7.) In an effort to thwart ReportSee's unlawful activity, Public Engines modified the CrimeReports.com website on February 25, 2010 to prevent the IP address for ReportSee's scraper from scraping CrimeReports.com. ReportSee's scraper was therefore temporarily prevented from obtaining access to Public Engines' website. (S. Meyers Decl. ¶ 8.)

ReportSee, however, circumvented Public Engines' countermeasure on March 2, 2010, by using a new IP address for its scraper, after which the scraper operated in the same manner – systematically and comprehensively scraping the crime report information contained in CrimeReports.com. Public Engines determined that the new address was registered to GoDaddy.com, Inc., indicating that ReportSee was using a server through GoDaddy.com's hosting service. By using this IP address and by using a hidden proxy service, ReportSee was able temporarily to conceal its identity. Also, because numerous parties including legitimate users of CrimeReports.com may have an IP address associated with GoDaddy.com, Public Engines could not, as a practical matter, exclude all IP addresses associated with GoDaddy.com's hosting service. Using this new IP address, ReportSee continued scraping CrimeReports.com from March 2 to March 18, 2010. (S. Meyers Decl. ¶ 9.) In addition, starting

on March 2, 2010, ReportSee's scraper was disguised to be the Firefox version 3.5.5 web browser. Since many legitimate users of CrimeReports.com use the Firefox web browser, Public Engines could not, as a practical matter, exclude requests using the Firefox web browser. (S. Meyers Decl. ¶ 10.)

To further verify that the new IP address for the scraper was associated with SpotCrime.com, on March 5, 2010 Public Engines again entered a series of dummy crime reports into CrimeReports.com. After the scraping by ReportSee had occurred, many of these dummy reports were posted on the SpotCrime.com webpage the next day. Attached as Exhibit 10 to the Declaration of Steve Meyers are screen shots from SpotCrime.com showing these dummy reports entered by Public Engines. The dummy crimes were time stamped and match the scraping requests tracked in the logs on Public Engines' servers. (S. Meyers Decl. ¶ 12.)

Public Engines' inserted dummy crime reports also contained incorrect geocoding information (mapping of street address to a specific latitude/longitude). The dummy reports displayed on SpotCrime.com used the same incorrect geocoding information, further confirming the scraping, and further confirming that ReportSee had not generated its own geocoding as it claimed, but had instead misappropriated it from Public Engines. (S. Meyers Decl. ¶ 13.)

G. ReportSee's Efforts to Circumvent Public Engines' Protective Measures.

Public Engines has continued to deploy various technical measures to prevent ReportSee from scraping the data. The measures Public Engines can reasonably use to stop ReportSee's conduct are, however, limited. Public Engines intends the data to be accessible for non-commercial use by the public. Because ReportSee's scraper poses as a human being on a computer using a browser, CrimeReports.com cannot easily distinguish it from a legitimate user. As Public Engines has taken increasingly aggressive technical steps to prevent ReportSee from accessing Public Engines' website, it encounters the increased risk that it will impair the general

public's ability to access the site, in violation of its obligations to law enforcement customers. (S. Meyers Decl. ¶ 14.)

Since March 18, 2010, Public Engines has deployed an escalating series of technical measures to stop ReportSee's scraper. (Steve Meyers Decl. ¶¶ 15-17). While some of these have worked temporarily, ReportSee on each occasion modified its scraper to get around each of these measures. (Id.) Through the placement of dummy reports and other technical measures, Public Engines has confirmed that the scraper is being operated by ReportSee to populate the SpotCrime.com website. (S. Meyers Decl. ¶ 18.) Every time Public Engines institutes a measure to prevent ReportSee from scraping Public Engines' website, ReportSee responds with a more elaborate strategy to conceal the identity of its scraper and circumvent all of Public Engines' efforts. (G. Whisenant Decl. ¶ 46.) As a result of ReportSee's conduct, Public Engines has incurred losses over the last year well in excess of $5,000. (Id. ¶ 46.)

H. Irreparable Injury

An injunction from this Court is the only means by which ReportSee will be prevented from continuing to misappropriate and make commercial use of the data Public Engines creates. If the Court does not issue a preliminary injunction against ReportSee's scraping activities, Public Engines will suffer the following types of irreparable injury:

(a) To prevent ReportSee's unauthorized use of Public Engines' data, Public Engines will be required to undertake increasingly elaborate measures to block ReportSee's scraper. Since scrapers are disguised as members of the public using web browsers, Public Engines runs the risk of blocking members of the public for legitimate purposes from accessing CrimeReports.com, thereby diminishing the value of Public Engines' website to both law enforcement agencies and the public. (G. Whisenant Decl. ¶ 47(a).)

(b) ReportSee's commercial publication and sale of data that Public Engines has spent millions of dollars to create devalues Public Engines' investment, diminishes the value of the technology that created the data, and could ultimately destroy the company, whose most valuable product is the data it offers to the public, in the form in which it is offered. (G. Whisenant Decl. ¶ 47(b).) Public Engines' injury would be difficult to quantify and could not be completely addressed by an award of damages.

(c) ReportSee's commercial publication and sale of Public Engines' data diminishes and could ultimately destroy the good will the company has developed with law enforcement agencies and its legitimate user base. The agencies depend on Public Engines' products to report crime data to the public in near real time, and to do so accurately, without advertising, and without editorial commentary. Each time ReportSee misappropriates and then sells Public Engines' data without any of these limitations or safeguards, the Company's good will is diluted. (G. Whisenant Decl. ¶ 47(c).)

If ReportSee is not enjoined from contacting Public Engines' law enforcement customers to solicit and threaten them regarding the disclosure of De-Identified Data created by the Publisher program, Public Engines will be irreparably injured in the following additional respects:

(a) One or more law enforcement agencies is likely to be persuaded by ReportSee's harassment to terminate their agreements with Public Engines to avoid legal confrontations, just as one such agency has already done. (G. Whisenant Decl. ¶ 48(b).)

(b) ReportSee's solicitation and threats will likely require Public Engines to incur the cost, expense, and risk to good will involved in litigation against its own customers to enforce the Terms of Use that prohibit the customer's disclosure of De-Identified Data. (G. Whisenant Decl. ¶ 48(c).)

ARGUMENT

A preliminary injunction preserves the Court's power to render a meaningful decision on the merits by maintaining the status quo pending the outcome of the case. Tri-State Generation & Transmission Ass'n, Inc. v. Shoshone River Power, Inc., 805 F.2d 351, 355 (10th Cir. 1986). Public Engines moves for entry of an order, effective during the pendency of the case, restraining ReportSee and its officers, directors, employees and agents, from (a) accessing or making any commercial use of the De-Identified Data generated from Public Engines' Publisher software; (b) making any commercial use whatsoever of any information from CrimeReports.com including, without limitation, crime report data that appears on the website; and (c) contacting or communicating with any of Public Engines' customers for the purpose of misrepresenting their obligations under open record laws or interfering with Public Engines' contractual relationships with those customers. Public Engines also asks the Court for an order directing ReportSee to 1) delete all information from its website(s) that was previously misappropriated from Public Engines; and 2) contact all third parties to whom it has distributed information that was misappropriated from Public Engines and directing them to delete the information.

Public Engines is entitled to a preliminary injunction on contractual, statutory, and common law grounds. The Terms of Use of CrimeReports.com—to which ReportSee has assented, as explained in Part D.2 of this Argument—provide that in the event a person makes commercial use of the information in the website, "Public Engines shall be entitled to equitable remedies, including without limitation preliminary and permanent injunctive relief . . . ." (Ex 3 to Whisenant Decl., Terms of Use ¶ 11.) Moreover, the Computer Fraud and Abuse Act ("CFAA") provides that "[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. 18 U.S.C. § 1030(g) (emphasis added). And, as the

following discussion demonstrates, Public Engines has met each of Rule 65's elements for a preliminary injunction.[1]

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

The Terms of Use for CrimReports.com provide: "[The user] hereby acknowledge[s] and recognize[s] the uniqueness of the services provided by the Public Engines Sites and Public Engines' substantial investments in such Sites as described herein, such that a violation of Section 1 of this Agreement by [the user] will result in irreparable harm to Public Engines for which money damages or other legal remedies may not adequately compensate." Ex 3 to Whisenant Decl., (Terms of Use, ¶ 11.) Courts in the Tenth Circuit have held that provisions like this one support preliminary injunctive relief and may be decisive where, as here, a sophisticated defendant has ignored its contractual obligations. See, e.g. Meitler Consulting, Inc. v. Dooley, 2007 WL 1834008, *11 (D. Kan. June 26, 2007) (enforcing employment contract provision that breach would result in irreparable injury); Pre-Paid Legal Servs. v. Harrell, 2008 WL 111319, *2 (E.D. Okla. Jan 8, 2008) (finding that commercial agreement provided for party's recognition that breach would result in irreparable harm). Cf. Dominion Video Satellite, Inc. v. Echostar Satellite Corp., 356 F.3d 1256, 1266 (10th Cir. 2004) (recognizing that a contract provision establishing irreparable harm is one factor to be considered in the court's analysis of irreparable harm).

---

1 In Tri-State Generation & Transmission Ass'n, Inc. v. Shoshone River Power, Inc., 805 F.2d 351, 355 (10th Cir. 1986), the Court held that the moving party must satisfy the following requirements: "(1) the moving party will suffer irreparable injury unless the injunction issues; (2) the threatened injury to the moving party outweighs whatever damage the proposed injunction may cause the opposing party; (3) the injunction, if issued, would not be adverse to the public interest; and (4) there is a substantial likelihood that the party will eventually prevail on the merits." Tri-State, 805 F.2d at 355.

At the core of Public Engines' business are two key elements in which the company has invested millions of dollars and three years of effort. First, Public Engines has developed a state-of-the-art technology that processes and maps raw police reports from communities nationwide, eliminating sensitive information that should not be disclosed to the public, and then reporting the data to the public in a user friendly format. Second, Public Engines has entered into contractual relationships with over 800 law enforcement agencies that pay Public Engines to provide crime data to the members of the public in a complete, accurate and consistent manner. The conduct alleged of ReportSee in the complaint threatens both the value of Public Engines' technology and the good will it has earned with hundreds of law enforcement agencies.

ReportSee's misappropriation of Public Engines' data will dilute, and threatens ultimately to destroy, the company's investment in technology. Left unchecked, ReportSee will in all likelihood continue to scrape Public Engines' proprietary data on a daily basis and then sell it for profit. Each day on which ReportSee sells the data that Public Engines has created results in violation of Public Engines' rights, a diminution in the value of the technology, and a loss to its business. (G. Whisenant Dec. ¶47(b). To prevent ReportSee's unauthorized activity, Public Engines will be required to undertake increasingly aggressive measures, to the detriment of both law enforcement and the public. (G. Whisenant Decl. ¶ 47(a).)

Under both Utah and federal law, "irreparable harm justifying a preliminary injunction includes wrongs of a repeated and continuing character." Hunsaker v. Kersh, 1999 UT 106, ¶ 9, 991 P.2d 67 (citations omitted). By its very nature, injunctive relief is "an anticipatory remedy purposed to prevent the perpetration of a threatened wrong or to compel the cessation of a continuing one." Sys. Concepts, Inc. v. Dixon, 669 P.2d 421, 428 (Utah 1983) (citations omitted). Such repeated and continuing wrongs are especially likely to cause irreparable harm where the defendant infringes intellectual property rights. See, e.g. Lorillard Tobacco Co. v. Engida, 213 Fed. Appx. 654, 656–57 (10th Cir. 2007) (finding that irreparable injury is

frequently presumed where a trademark is wrongfully appropriated); New Pro Publ'ns v. Links Media Group, L.L.C., 2007 WL 4115995, *4 (D. Colo. Nov. 16, 2007) ("Misappropriation of trademarks and copyrights . . . create[s] a high risk of irreparable injury because misuse of such rights is likely to have a bad effect on the owner's business, reputation, and good will."); Harris Research, Inc. v. Lydon, 505 F.Supp.2d 1161, 1168 (D. Utah 2007) (holding that likelihood of confusion, dilution of a trademark, and risk to a business's good will and investments in intellectual property establish irreparable harm).

More than 800 law enforcement agencies have contracted with Public Engines to process and report crime data in a user friendly format, without advertising, and without editorial commentary. If ReportSee is allowed to continue to make daily commercial use of Public Engines' data on a website that observes none of these limitations, Public Engines' good will will be diluted and will ultimately be destroyed. (G. Whisenant Decl. ¶¶ 47(c) & 48.) As shown above, one agency has terminated its contract with Public Engines for this very reason, and more will follow unless ReportSee is enjoined. (Id. ¶ 48.) In similar cases, the courts have not been reluctant to issue preliminary injunctions to preserve the good will of a business that is the subject of continuous assault by the defendant's misconduct. See, e.g., Tri-State, 805 F.2d at 356; see also John B. Hull, Inc. v. Waterbury Petroleum Products, Inc., 588 F.2d 24, 28-29 (2d Cir. 1978) (holding that the possibility of going out of business is irreparable harm).

Compensatory relief after final judgment will not be adequate to redress the ongoing harm suffered by Public Engines in the meantime. The wrongs perpetrated by ReportSee against Public Engines have been repeated and are continuous, threatening the intellectual property and the good will in which Public Engines has invested millions of dollars.

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

In determining whether to issue an injunction, the federal court weighs the relative harm to each party that would occur if it issues an injunction versus if it does not issue an injunction.

Tri-State, 805 F.2d at 357. In this case, the harm Public Engines faces if an injunction is not issued far outweighs any harm that ReportSee could suffer if an injunction issues. In fact, ReportSee's legitimate interests would not be affected at all because ReportSee has no right to make commercial use of the information on the CrimeReports.com website. ReportSee has no right to access Public Engines' servers, to scrape and use Public Engines' data, or to interfere with Public Engines' contracts with law enforcement customers in an effort to obtain the De-Identified Data. Under the circumstances of this case, the injunction that is the subject of this motion would not impair any of the defendant's rights.

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

The issuance of a preliminary injunction would serve the public interest by ensuring performance of the parties' contractual obligations and compliance with applicable statutes. See Mountain Am. Credit Union v. Godfrey, 2006 WL 2129465, at *4 (D. Utah) ("There is a strong public interest in requiring adherence to contracts and statutes.") In Tri-State, the Tenth Circuit observed that "the 'public interest' in a public utility case is actually the interest of purchasers of electric power." 805 F.2d at 357. The court held that the public would not be harmed by, and would potentially benefit from, the injunction because it would enable the plaintiff public utility to continue providing service to its customers. Id. at 357–358. Likewise, the public interest in the outcome of an internet scraping case coincides with the interests of members of the public who patronize an important website. Website users' interest will not be harmed by the proposed injunction. Rather, the injunction will enable Public Engines to continue operating CrimeReports.com without any disruption to ReportSee's legitimate business efforts. CrimeReports is the official source of crime report data for communities nationwide. Without advertisement or editorial commentary, the website benefits the public by informing users of an

area's current crime patterns and history and promoting the public safety. The proposed injunction would not be adverse to the public interest.

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

In the Tenth Circuit, if the movant has established the other three requirements for a preliminary injunction, it satisfies the "likelihood of success" requirement by showing that "questions going to the merits are so serious, substantial, difficult, and doubtful as to make the issue ripe for litigation and deserving of more deliberate investigation." Fed. Lands Legal Consortium v. United States, 195 F.3d 1190, 1194–95 (10th Cir. 1999). In this case, Public Engines has raised "questions going to the merits" that, at a minimum, constitute fair grounds for deliberate investigation and litigation. As the following argument shows, Public Engines has not only raised significant issues for adjudication, but is likely to prevail.

1. Computer Fraud and Abuse Act

First, ReportSee's conduct violates the federal Computer Fraud and Abuse Act (the "CFAA"), which specifically provides for injunctive relief. 18 U.S.C. § 1030(g). The CFAA imposes civil liability on a person who "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value. . . ." 18 U.S.C. § 1030(a)(4). Also, the CFAA imposes liability where the defendant "knowingly causes 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." 18 U.S.C. § 1030(a)(5)(A). Whether the infraction by the defendant is analyzed under § 1030(a)(4) or § 1030(a)(5)(A), a civil remedy is available where the loss to one or more persons during any one-year period has an aggregate

value of at least $5,000. 18 U.S.C. § 1030(c)(4)(i)(I); see Southwest Airlines Co. v. Boardfirst, L.L.C., 2007 WL 4823761, *12 (N.D. Tex. Sept. 12, 2007).

As the factual presentation above shows, ReportSee has acted intentionally and without authorization to access computer servers owned by Public Engines that are connected to the internet and used in interstate commerce. Public Engines has also shown that ReportSee has acted surreptitiously with the intent to defraud Public Engines of its intellectual property by obtaining information from Public Engines' servers. Further, ReportSee has transmitted a program, code or command to Public Engines' computer servers, causing loss to Public Engines exceeding $5,000.00 in aggregate value in a one year period, including the costs of responding to and monitoring ReportSee's unauthorized access, conducting damage assessments, and undertaking various measures to attempt to prevent ReportSee's unauthorized access. (G. Whisenant Decl. ¶ 46.) As a result, Public Engines is entitled to a civil remedy under the CFAA, including injunctive relief.

2. Breach of Contract

Second, ReportSee has violated the "Terms of Use" agreement between the parties. Under the laws of both California and Utah, the elements of a breach of contract claim are "(1) a contract, (2) performance by the party seeking recovery, (3) breach of the contract by the other party, and (4) damages." Bridgeport Retail, LLC v. Commerce CRG Utah, LLC, 2008 WL 3295850, *2 (D. Utah Aug. 7, 2008) (citing MBNA Am. Bank, N.A. v. Goodman, 2007 UT App 276, ¶ 6, 140 P.3d 589, 591 (Utah App. 2006)). By accessing CrimeReports.com, ReportSee entered into what is known as a "browsewrap contract" with Public Engines, that is, a contract formed where an internet user browses a website, the use of which is conditioned on posted

"Terms of Use" or other provisions. See McMillan v. Wells Fargo Bank, N.A., 2009 WL 1686431 (N.D. Cal. June 12, 2009) (treating a website's "terms of use" as an agreement with a website user); Ticketmaster L.L.C. v. RMG Techs., Inc., 507 F.Supp.2d 1096, 1107 (C.D. Cal. 2007) (same); Pollstar v. Gigmania Ltd., 170 F.Supp.2d 974, 982 (E.D. Cal. 2000) ("[T]he browser wrap license agreement may be arguably valid and enforceable."). Courts routinely enforce a website's terms of use where, as here, a competitor uses automated means to exploit information posted to the website. See, e.g., Southwest Airlines Co. v. Boardfirst, LLC, 2007 WL 4823761, *12 (N.D. Tex. Sept. 12, 2007) at 12 (holding that defendant violated the terms of use by using Southwest's website for commercial purposes); Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 403-04 (2d Cir. 2004) (affirming a preliminary injunction against defendant's scraping of a website in violation of the website's terms of use).

ReportSee has caused damage to Public Engines by breaching express provisions of the Terms of Use, including prohibitions against (1) making commercial use of the data contained on CrimeReports.com, (2) copying and modifying the data contained on CrimeReports.com for its own business purposes, and (3) employing an automated scraper to obtain information from CrimeReports.com. As a result, ReportSee is liable for breach of contract.

3. Utah Unfair Competition Act

Third, ReportSee has violated the Utah Unfair Competition Act (the "UUCA"), which establishes a private cause of action for parties injured by unfair competition in violation of the Act. Utah Code Ann. § 13-5a-103. The UUCA specifically prohibits "cyber-terrorism," which is defined as a defendant's "willfully communicating, delivering, or causing the transmission of a program, code, or command without authorization or exceeding authorized access" in a way that

unfairly or fraudulently "leads to a material diminution in value of intellectual property." Utah Code Ann. § 13-5a-102(2)(c) & 102(4); see also Margae, Inc. v. Clear Link Techs., LLC, 620 F. Supp.2d 1284, 1286 (D. Utah 2009) (interpreting "cyber-terrorism" under the UUCA as including both the unauthorized use of intellectual property and the use of a program, code or command as a tool to attack intellectual property).

As shown in the factual presentation above, ReportSee has willfully deployed an automated scraper to "attack" Public Engines' intellectual property. Its surreptitious use of a scraper, especially after warnings from Public Engines' lawyers and Chief Executive Officer, clearly constituted unauthorized access to CrimeReports.com, which has led to a diminution in the value of Public Engines' website and the information reported on the website. As a result, Public Engines is entitled to relief from ReportSee under the UUCA.

4. False Advertising Under the Lanham Act

Fourth, ReportSee is likely to be held liable for false advertising in violation of the Lanham Act. 15 U.S.C. § 1125(a). A claim for false advertising under § 1125(a) requires proof of the following elements: "(1) that defendant made material false or misleading representations of fact in connection with the commercial advertising or promotion of its product; (2) in commerce; (3) that are either likely to cause confusion or mistake as to (a) the origin, association or approval of the product with or by another, or (b) the characteristics of the goods or services; and (4) injure the plaintiff." Folkers v. Am. Massage Therapy Ass'n, Inc., 2004 WL 306913, *9 (D. Kan. Feb. 10, 2004) (citing Cottrell, Ltd. v. Biotrol Int'l., Inc., 191 F.3d 1248, 1252 (10th Cir. 1999)). As shown in the factual presentation above, ReportSee has falsely represented in its electronic advertising materials that its crime reports data derives from the efforts of its staff,

who are said to gather the data from news accounts, police blotters, and police scanners. In fact, however, SpotCrime.com obtains much of its information by misappropriating it directly from CrimeReports.com. (G. Whisenant Decl. ¶¶ 26-27.) Such misrepresentations are likely to cause confusion or mistake as to the origin, association, or approval of ReportSee's products or services, or the characteristics of those goods or services. As a result, Public Engines is entitled to relief from ReportSee under the Lanham Act for false advertising.

5. Hot News Misappropriation

Fifth, ReportSee is guilty of "hot news" misappropriation, a common law claim requiring proof of the following elements: "(i) the plaintiff generates or collects information at some cost or expense; (ii) the value of the information is highly time-sensitive; (iii) the defendant's use of information constitutes free-riding on the plaintiff's costly efforts to generate or collect it; (iv) the defendant's use of the information is in direct competition with a product or service offered by plaintiff; (v) the ability of the other party to free-ride on the efforts of the plaintiff would so reduce the incentive to produce the product or service that its existence or quality would be substantially threatened." Nat'l Basketball Ass'n v. Motorola, Inc., 105 F.3d 841, 845, 852 (2d Cir. 1997).

As shown in the factual presentation above, Public Engines has invested millions of dollars to establish a nationwide network to gather crime data from hundreds of law enforcement agencies, to electronically eliminate data that are inappropriate for public consumption, and then package the resulting data stream in a uniform and user friendly format. The information Public Engines gathers is time sensitive. In fact, one of the main purposes of the CrimeReports.com website is to make information about crimes available to the public in near real time. By

scraping this data from CrimeReports.com, and then selling it for a profit, ReportSee free-rides on Public Engines' investment, competing with CrimeReports.com, and thus threatening Public Engines' incentive to produce this product and service. As a result, Public Engines is entitled to relief for hot news misappropriation.

6. Interference with Contract

Finally, ReportSee has intentionally interfered with Public Engines' contracts with law enforcement agencies. To establish a claim for tortious interference with business relations, the plaintiff must prove "(1) that the defendant intentionally interfered with the plaintiff's existing or potential economic relations; (2) for an improper purpose or by improper means, (3) causing injury to the plaintiff." Leigh Furniture & Carpet Co. v. Isom, 657 P.2d 293, 304 (Utah 1982).

ReportSee is unquestionably aware of the existing contractual relationships between Public Engines and law enforcement agencies. In fact, it has repeatedly targeted those very agencies because it knows that Public Engines has installed the Publisher program for each of them, and its objective is to profit from the data stream from the Publisher program. As the factual presentation above shows, ReportSee has intentionally interfered with these contracts by soliciting Public Engines' customer agencies in an effort to persuade them to violate their agreements with Public Engines, and knowingly misrepresenting to the agencies their obligations under public access laws, with the goal of obtaining proprietary information belonging to Public Engines and then using that information for its own personal gain and to compete with Public Engines. ReportSee's conduct has damaged Public Engines' relationships with its customers and harmed its business reputation. As a result, Public Engines is entitled to relief for interference with contract.

E. There Is No Need for Security Here Because Issuance of the Injunction Will Not Result In Any Financial Harm to ReportSee.

Rule 65(c) requires that the movant provide security "in an amount that the court considers proper to pay the costs and damages sustained by any party found to have been wrongfully enjoined or restrained." In this case, the Court need not require security from the plaintiff in any amount because, in accepting the Terms of Service for CrimeReports.com, ReportSee has already agreed that security will not be required. Paragraph 11 of the Terms of Use provides in part: "[The user] explicitly agree[s] that Public Engines will not be required . . . to post or secure a bond in order to obtain [injunctive] relief."

Beyond that, if the injunction issues, ReportSee is not likely to incur or suffer any costs associated with the injunction. Kenny v. Rich, 2008 UT App 209, ¶ 39, 196 P.3d 989 186 P.3d 989, 1002 (Utah Ct. App. 2008) ("[I]f there is an absence of proof showing a likelihood of harm, certainly no bond is necessary" (internal citations omitted)). The proposed injunction would not limit ReportSee's ability to operate its business based on information from legitimate sources. No cognizable harm will result from requiring ReportSee (1) to comply with the provisions of the Terms of Use and (2) to refrain from free-riding on the efforts of Public Engines. See, e.g., MedAvante, Inc. v. ProxyMed, Inc., Slip Op., 2006 WL 2927623, *4 (D. N.J. Oct 12, 2006) ("The injury a defendant might suffer if an injunction is granted should be discounted if there are any facts indicating that the defendant brought the injury upon himself or herself.") Public Engines should not be required to provide security as a condition to issuance of the requested preliminary injunction.

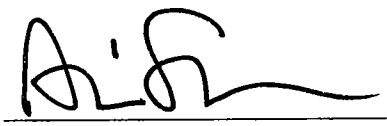
CONCLUSION

Public Engines has met each of the required elements for issuance of a preliminary injunction effective during the pendency of this action. Furthermore, Public Engines is entitled to a preliminary injunction under the Terms of Use and under 18 U.S.C. § 1030(g). For all the foregoing reasons, Public Engines respectfully requests that the Court grant this motion for

preliminary injunction enjoining defendant, its officers, directors, employees, agents, and affiliates from (a) accessing or making any commercial use of the De-Identified Data generated from Public Engines' Publisher software; (b) making any commercial use whatsoever of any information from CrimeReports.com including, without limitation, crime report data that appears on the website; and (c) contacting or communicating with any of Public Engines' customers for the purpose or with the result of misrepresenting their obligations under open record laws or interfering with Public Engines' contractual relationships with those customers. Public Engines also requests that the Court direct ReportSee to 1) permanently delete from its collection of websites, including the SpotCrime.com website, all information that was previously misappropriated from Public Engines; and 2) contact all third parties to whom it has distributed information that was misappropriated from Public Engines and direct them to delete the information.

DATED this 9th day of April, 2010.

Snell & Wilmer L.L.P.



Alan L. Sullivan
Todd M. Shaughnessy
Attorneys for Plaintiff Public Engines, Inc

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing will be hand delivered to the following on the 12th day of April, 2010:

ReportSee, Inc.
300 East Lombard St., Suite 840
Baltimore, MD 21202