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.

DECLARATION OF GREG WHISENANT

I, Greg Whisenant, hereby declare under penalty of perjury as follows:

1. I am an individual resident of the State of Utah, over the age of majority, and competent in every respect to make this declaration. The statements contained in this declaration are based on my own personal knowledge, except for statements explicitly made on the basis of

information and belief. As to statements made on information and belief, I am reliably informed and believe such matters to be true.

2. I am currently employed as the Chief Executive Officer of plaintiff Public Engines, Inc. ("Public Engines"). In that capacity, I am responsible for the company's strategic direction and overall performance, including its relationships with law enforcement agencies that enter into contracts with Public Engines, as described below.

A. Public Engines and CrimeReports.com.

3. Public Engines is in the business of providing software and services to law enforcement agencies across the United States. Public Engines owns and operates the Crime Reports.com website, which is one component of the services Public Engines provides to its law enforcement customers.

4. Public Engines' law enforcement customers vary greatly in terms of size and resources, from extremely large agencies like the Los Angeles County Sheriff's Office, to small municipal police departments like the Cordelle, Georgia Police Department. These agencies have varying levels of information technology support, from dedicated staffs of personnel to one or two people tasked with the maintenance of the agency's IT systems.

5. Nearly all law enforcement agencies in the United States 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. The information contained in these CAD and RMS systems includes, among other information, reported crimes and where they occurred. The information in these systems also includes specific information about the victim, details of the crime, information on the police department's ongoing investigation, the identity of suspects, and other types of information that law enforcement agencies generally do not share with the public.

6. There are more than 18,000 law enforcement agencies in the United States, and as you might expect, the CAD and RMS systems used by these agencies vary widely. Such systems

are sold by dozens of different companies. Some are sophisticated modern systems; others are quite old. They run on a variety of different operating systems and platforms. They collect and store information in different ways and are used by agencies in different ways. All, however, maintain up to the minute information about reported crimes, though sometimes agencies lag in data entry.

7. Law enforcement agencies have a strong interest in making available to the communities they serve current and accurate information about crimes and criminal activity, which is balanced by their need to maintain some level of control over the information that is provided and its distribution. A service that provides such up to the minute information to the public will assist law enforcement efforts 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.

8. 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 and while still satisfying their desire to maintain control of the data that is released to the public.

9. 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 selective manner (eliminating data that would be inappropriate for publication), 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. Public Engines does not comment upon or provide any

other information about the individual crime reports, and the website can therefore serve as an "official" source of agency information.

10. Public Engines began development of this package of software and services around 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.

11. At present, Public Engines has entered into contracts with more than 800 law enforcement agencies nationwide. The agencies pay Public Engines a fee of between $588 and $2,388 per year for the CrimeReports.com products and services provided by Public Engines.

12. As part of each such contract, the law enforcement agency obtains a license to Public Engines' proprietary Crime Reports 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 – effectively, a unique "wrapper" – for the Publisher to interact successfully with the agency's CAD and/or RMS. To date, Public Engines has successfully configured its Publisher program to interact with CAD or RMS systems from more than 60 different vendors.

13. 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.

14. 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 itself 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 true and correct copy of the Terms of Service applicable to each law enforcement contract is appended hereto as Exhibit 1.

15. 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 victim's address using scrub rules that Public Engines defines for each agency to clean out artifacts from the data entry process. The application then sends the scrubbed, "blockized" address to Google for geocoding, which produces a latitude and longitude ("XY coordinate"), which is used to place the icon on the CrimeReports.com map interface. (A "blockized" address is one that omits the victim's specific street address and instead locates the crime on a block in a street.) Public Engines has entered into an agreement obligating Public Engines to pay significant sums to Google for providing this service. In some cases, the goecoding from Google fails. If it does, the application rescrubs the data with more rigorous rules, re-blockizes the new address, and resubmits 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.

16. Ultimately, after going through all of these processes, the data (a) is limited to that information which the law enforcement agency has determined it can properly disclose, (b) has been re-structured and re-formatted in a unique way, and (c) has been encoded with other data to permit it to be located on a map, searched, accessed, and displayed.

17. 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.

18. 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 for the law enforcement agency because law enforcement agencies supply the raw data based on rules and limits to which the agencies themselves have agreed. Public Engines also agrees to keep the data up to date and accurate, satisfying the agencies' desire to maintain control over the data.

19. Users of CrimeReports.com are able to search the website by 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 crimes 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 this information through software called a "widget," which is installed by Public Engines on authorized third party websites, and often on the law

enforcement agency's website. Members of the public may also access this information via the website through a link in an email alert sent to them from Public Engines.

20. Attached hereto as Exhibit 2 is a screen shot from CrimeReports.com showing how this information is displayed for an area in downtown Salt Lake City.

21. 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 in 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.

22. 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 appended hereto as Exhibit 3.

B. ReportSee and SpotCrime.com.

23. ReportSee also operates a collection of websites, including SpotCrime.com, that provides 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. I am informed and believe that unlike CrimeReports.com SpotCrime.com is not an official crime information site for law enforcement agencies.

24. Instead, SpotCrime.com sometimes adds commentary about the crime reports it features and sells advertising. As explained in detail below, much of the information appearing on the SpotCrime.com website has been taken wholesale from Public Engines' CrimeReports.com website, without alteration. I am unaware that SpotCrime.com has provided software or services to any law enforcement agencies. SpotCrime.com is primarily geared toward serving various media outlets and the public. To the extent enforcement agencies do not have contracts with ReportSee, law enforcement agencies have no ability 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 us and indicating their disapproval of the appearance of De-Identified Data from their jurisdictions on SpotCrime.com, over which they cannot exert or maintain any control.

25. I am informed and believe that ReportSee has entered contracts with news and media organizations to provide this crime mapping data to them for a fee. I am informed and believe, for example, that 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 and an embedded widget from SpotCrime.com displaying crime information.

26. 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.

27. I am informed and believe that in reality, however, SpotCrime.com obtains much of the information displayed on its webpage by 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.

C. "Scraping"

28. Web scraping is a computer software technique used to extract information from websites. Among other methods, 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.

29. Attached as Exhibit 4 is a screen shot from SpotCrime.com showing the same area as the screen shot from CrimeReports.com attached as Exhibit 2. Every one of the crime reports appearing on Exhibit 4 was taken from CrimeReports.com.

30. The Terms of Use for CrimeReports.com specifically 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…."

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

31. Like most websites, CrimeReports.com maintains an automated log of users who access the website. This log includes the Internet Protocol ("IP") addresses of those users. 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 the page. The log also includes information about what information in particular was accessed and when.

32. 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 crime report information was being systematically scraped.

33. 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 sourced exclusively by Public Engines and approved for display on the CrimeReports.com website was being displayed on an unapproved website.

34. 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 IP address resolved to the SpotCrime.com website. Attached as Exhibit 5 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.

35. This scraping started around March 19, 2008, if not earlier, and continued through early June 2008.

36. On June 16, 2008, Public Engines, through its attorney, sent a letter to ReportSee demanding that it immediately cease and desist from any scraping of the CrimeReports.com website. Among other things, Public Engines specifically 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.

37. 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 appended hereto as Exhibit 7. A transcript of

the voicemail dated June 24, 2008 from ReportSee's counsel to Public Engines' counsel is appended hereto as Exhibit 8.

38. After that exchange, to my knowledge, ReportSee's scraping of CrimeReports.com was temporarily suspended.

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

39. ReportSee, however, then resorted to other methods to obtain Public Engines' proprietary information. I am informed and believe that 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.

40. I am informed and believe that starting in the spring of 2009 and continuing to the present, ReportSee has contacted at least 30 different law enforcement agencies on many occasions who are customers of Public Engines for this purpose. I am informed and believe that 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. I am informed and believe ReportSee has demanded that these agencies provide ReportSee with the De-Identified Data processed through Public Engines' Publisher program.

41. I am informed and believe that in making these demands, ReportSee has insisted that it is entitled to this information under various public records access laws when, in fact, those laws do not require the agencies to provide this information as demanded by ReportSee; in particular, such public records access laws do not require the disclosure of De-Identified Data that is the property of Public Engines. They have 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. I am informed and believe that ReportSee also has threatened to sue some of the agencies if they do not provide the requested information.

42. I am informed and believe that ReportSee stepped up these demands in the fall of 2009. Public Engines received a number of complaints from its law enforcement customers about these contacts, and Public Engines has been required to devote substantial time and resources to managing 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.

43. In October 2009, I called ReportSee's Chief Executive Officer, Colin Drane, to discuss ReportSee's inappropriate contacts with Public Engines' customers and interference with Public Engines business. I 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. I explained that the data ReportSee was demanding was unique to Public Engines, was not publicly available, was uniquely improved by Public Engines, and was not something the agencies were required or allowed to provide under public records laws.

44. Mr. Drane acknowledged that ReportSee had made these contacts, that ReportSee was trying to get the information that was being sourced by Public Engines, and that ReportSee would continue to pursue all means to get it. After explaining that ReportSee's behavior was putting the company in legal jeopardy and that Public Engines would enforce its rights, Mr. Drane ultimately told me to "do what you need to do" and hung up the phone. On October 27, 2009, Public Engines' lawyer sent a letter to Mr. Drane demanding that ReportSee stop interfering with Public Engines' business relationships, but Mr. Drane did not respond.

45. 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 sourced and uniquely improved by Public Engines as part of its contracts with its customers.

F. Irreparable Injury

46. The Declaration of Steve Meyers, which is filed and served with my declaration, explains in detail ReportSee's resumption of scraping Public Engines' data beginning in late 2009, our efforts to block ReportSee's scraper, and ReportSee's efforts to circumvent these measures. The bottom line is that 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 our company's efforts. In undertaking the measures described in Mr. Meyers's Declaration, Public Engines has incurred losses over the last year well in excess of $5,000.

47. I believe that an injunction from this Court is the only means by which ReportSee will be prevented from permanently 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 to appear as members of the public using web browsers, Public Engines runs the risk of blocking legitimate, authorized members of the public having no ulterior motives from accessing CrimeReports.com, which it is required to do by contract, thereby diminishing the value of our website to both law enforcement agencies and the public.

(b) ReportSee's publication and commercial sale of data that Public Engines has spent millions of dollars to create devalues our company's investment, diminishes the value of the technology that created the data, and could ultimately destroy our company, whose most valuable product is the data it offers to the public, in the form in which it is offered.

(c) ReportSee's publication and commercial sale of Public Engines' data diminishes and could ultimately destroy the good will our company has developed with law enforcement agencies. Those agencies depend on our products to report crime data to the public in near real time, and to do so accurately, without advertising, and without editorial commentary. The agencies also expect to be able to exert some level of control over what information is provided to the public through the De-Identified Data. Each time ReportSee misappropriates and then sells our data without any of these limitations or safeguards, our good will is diluted.

48. 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, I believe Public Engines will be irreparably injured in the following respects.

(a) One or more law enforcement agencies will probably be persuaded to disclose De-Identified Data rather than fight ReportSee in court, thereby diminishing the value of the data to Public Engines.

(b) One or more law enforcement customers will probably 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.

(c) ReportSee's solicitation and threats will probably require Public Engines to incur the cost, expense and risk of 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.

I hereby affirm that the foregoing information is truthful under penalty of perjury of the laws of the United States.

DATED this 9 day of April, 2010.

Greg Whisenant

Greg Whisenant

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