

FILED IN UNITED STATES DISTRICT
COURT, DISTRICT OF UTAH

APR 09 2010

D. MARK JONES, CLERK
BY _____
DEPUTY CLERK

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 STEVEN MEYERS

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

I, Steven Meyers, 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 those statements explicitly made on

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

2. I am currently employed as the Director of Technical Operations of Public Engines, Inc. ("Public Engines"). In that capacity, I am responsible for the company's data center operations and the management of all hardware systems and security related to the CrimeReports.com application and associated technologies.

3. I have read the Declaration of Greg Whisenant, which I understand will be filed with my declaration. The purpose of my declaration is to explain the facts relating to activities of defendant ReportSee, Inc. ("ReportSee") after it temporarily suspended the scraping of Public Engines' website in the summer of 2008, as explained in paragraph 38 of Mr. Whisenant's declaration.

A. ReportSee's Resumption of Scraping.

4. In December 2009, ReportSee again started scraping data from the CrimeReports.com website. From a review of our website's user log information, I was able to determine 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 our API (application programming interface) to retrieve the crime data.

5. 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 orderly, 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.

6. Initially, the IP address for these requests was 174.129.243.60, which I confirmed is an IP address for SpotCrime.com. I determined this first through DNS, which maps domain names to IP addresses, and second by typing the address into a browser.

7. My staff and I further verified this by temporarily inserting two dummy crimes into our database on January 7, 2010 and five dummy crimes on January 8, 2010. These dummy crimes were ones we 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, we also changed the latitude and longitude of the crime to be incorrect in relation to its mapped location. This enabled us to confirm that ReportSee relies on Public Engines' mapping to locate the crime sites on its maps. Attached hereto as Exhibit 9 are screen captures from SpotCrime.com showing these dummy reports entered by Public Engines. The crimes inserted on January 8 were time stamped and match the scraping requests tracked in the logs on Public Engines' servers.

8. As a result of an effort to keep a more detailed log of the scraping habits of SpotCrime.com, on February 25, 2010, Public Engines unintentionally modified the CrimeReports.com website in a way that prevented that particular IP address from scraping CrimeReports.com. ReportSee's scraper was therefore unable to access the API.

9. In response, however, on March 2, 2010, ReportSee began using a new IP address for its scraper. The new IP address of the server hosting the scraper was 208.109.126.144. The scraper operated in the same manner as it had before – systematically scraping, area-by-area, the crime report information contained in CrimeReports.com. Their previous IP address was registered to Amazon.com, Inc., indicating that they were previously using a server hosted by Amazon's hosting services. Public Engines checked for information about this IP address and determined it was registered to GoDaddy.com, Inc., indicating that they were using a server hosted by GoDaddy's hosting services. By using this IP address, ReportSee was able to conceal its identity. Also, because numerous parties including legitimate users of CrimeReports.com

may have an IP address associated with GoDaddy.com, we could not, as a practical matter, exclude all IP addresses associated with GoDaddy.com. We observed that, using this new IP address, ReportSee continued scraping CrimeReports.com from March 2 to March 18, 2010.

10. In addition, starting on March 2, 2010, ReportSee's scraper was disguised to be the Firefox version 3.5.5 web browser, as indicated by the "user-agent" data contained in the electronic requests and collected in the log. Since many legitimate users of CrimeReports.com use the Firefox web browser, we could not, as a practical matter, exclude requests using the Firefox web browser.

11. To verify that the new IP address of the scraper was controlled by ReportSee, we typed that IP address into a browser, which resulted in our viewing the SpotCrime.com web site.

12. To further verify that the new IP address for the scraper was associated with SpotCrime.com, on March 5, 2010 we again temporarily entered a series of dummy crime reports into CrimeReports.com. Then, after the scraping by ReportSee had occurred, we examined SpotCrime.com and found many of these dummy reports posted on the webpage the next day. Attached hereto as Exhibit 10 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.

13. These new 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.

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

14. We have continued to deploy various technical measures to prevent ReportSee from scraping the data. And while there are a variety of technical measures that can be deployed

to prevent the scraping of a website, those measures are necessarily limited because the data are presented to the public for free. Because ReportSee's scraper poses as a human being on a computer using a browser, the computer cannot easily distinguish it from a legitimate user. As we take increasingly aggressive technical steps to prevent ReportSee from accessing Public Engines' website, we encounter the increased risk that we will also impair the general public's ability to access the site, in violation of our obligations to law enforcement agencies.

15. On March 18, 2010, we again attempted to stop ReportSee's scraping by changing our API to support only "POST" requests. Previously, it supported either "GET" or "POST" requests, even though legitimate API requests always use POST. The difference between a GET or POST is relatively straightforward and easy to recognize. Both are used to send data to the server, but a GET request includes the data in the URL, while a POST sends the data separately. This attempt was initially successful; we observed from the log that on March 19, ReportSee was unable to scrape CrimeReports.com. However, ReportSee then modified its scraper to use a POST request. This effectively defeated our technical change, and ReportSee resumed its daily scraping of the site on March 20.

16. We again confirmed that ReportSee was responsible for the scraper because the IP address was 174.129.243.60, the IP address of www.spotcrime.com.

17. In addition, at this point ReportSee began indicating that <http://www.crimereports.com/map> had referred them to the API. In other words, ReportSee's scraper claimed to have visited the CrimeReports.com home page containing the map page, and that it was the map page that had given the scraper access to our API. Previously, the scraper had not indicated any referring page.

18. On March 23, we again tried to stop ReportSee's scraping by blocking all of its known server IPs from accessing our website. This was done at the firewall level, so ReportSee's servers would no longer be able to access our servers at all. This attempt was also

initially successful. On March 24, ReportSee was unable to scrape CrimeReports.com during the usual timeframe. I am informed and believe, however, that ReportSee then modified its scraper to run from a different IP address, 173.188.2.190. This effectively defeated Public Engines' technical change, and ReportSee resumed its daily scraping of the site later that same day. This IP address is dynamically generated, and is owned by Windstream Communications Inc., and appears to be associated with a DSL connection at a residence or business office. The scraping from 172.188.2.190 only happened once, and so we were not able to confirm it. Our beliefs concerning this IP address are based on the methodology used for the scraping which were consistent with the scope and pattern of ReportSee's previous scraping efforts.

19. On March 25th, ReportSee switched once again to a new IP address, 184.73.50.166, which is a virtual server hosted by the Amazon Elastic Computing Cloud (EC2). SpotCrime.com's server is also an Amazon EC2 virtual server.

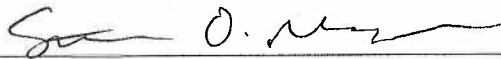
20. To verify that the new IP address for the scraper was associated with SpotCrime.com, on March 25, 2010, we again temporarily entered a dummy crime report into our system in San Jose, California. Then, after the scraping had occurred, we examined SpotCrime.com and found that dummy report posted on the webpage the next day. Attached hereto as Exhibit 11 are screen shots from SpotCrime.com showing the dummy report entered by Public Engines. The dummy crime report was time stamped and matches the scraping requests tracked in the logs we maintain for Public Engines' servers. The inserted dummy report also contained incorrect geocoding information created by us (mapping of street address to a specific latitude/longitude). The dummy report displayed on SpotCrime.com used the same incorrect geocoding information, further confirming the scraping, and that the geocoding had been misappropriated by ReportSee.

21. As shown above, Public Engines has deployed a series of different technical measures to stop ReportSee's scraper. While some of these have worked temporarily, ReportSee

on each occasion has modified its scraper to get around each of these measures. Through the placement of dummy reports and other technical measures, we have been able to confirm that the scraper is being operated by ReportSee to populate the SpotCrime.com website.

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

DATED this 9th day of April, 2010.



Steven Meyers

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

A handwritten signature in black ink, appearing to be "A. L. S.", is written above a horizontal line.