Have Google and Facebook unethically breached the privacy of their users?

Word Count: [2,011]

Date: 2/28/2014

The internet giants Facebook and Google have both gone through many scandals about privacy. Some concerned their lack of protection of their users' personal information from other users. This paper, however, only concerns Facebook and Google directly breaching the privacy of their users. The question that presents itself is "Ethically, is it okay for Facebook and Google to monitor or track users data and search history?"

Google and Facebook both make money through advertisements and data mining. Google and Facebook both use users' personal data to better optimize the advertisements shown to each individual. This means that they have to track users extensively. Google tracks its users' search history. It also uses programs such as google analytics to aggregate this data. Google breaches privacy further by looking at its users' web history as a whole, even history that was not google related. Google even has gone out of its way in the past to track the users. "Recently, the Wall Street Journal reported that Google deliberately circumvented privacy protections in Apple's Safari web browser when used on the iPhone and any computer running Safari. Even when consumers followed Google and Apple's instructions to protect their privacy, the Internet search giant secretly engineered special code to track a user's web browsing." (Pociask) Because of this, Google can compile full profile of users linked to its users' IP address, which can be used internally or can be sold to marketing agencies for external use. Facebook implements similar things and has even been known to track users all over the internet. Privacy Choice founder Jim Brock said, "I was surprised to see that Facebook is tracking me across 87 percent of the Internet, despite the fact that I'm a minimal user of Facebook."(Mullin) Google and Facebook also make money through the aggregation of users' data. Between advertisements and data mining, and other sources, "Google was making $14.70 per 1,000 searches in 2010." Jim brock said that "His Google value checks in at more than $700 per year". (Mullin) As for Facebook,

"Jim Brock says his estimated annual Facebook value was a mere $1.68. His daughter, perhaps unsurprisingly, is at $12." (Mullin) These seem to be small values for Facebook and Google, which have market values of 104 and 203 billion dollars, respectively. However it should be noted that there are 900 million Facebook users as of 2012 and 1.2 trillion google searches in 2012. (*Google* and *Zeitgeist*) These numbers mean that Google and Facebook do actually make a lot of money on personal data. These privacy breaches are ongoing and ever present when you are using the sites and are often present even when you are not.

Google and Facebook have made greater privacy breaches than these in the past. Google Street View is a project that google had to add a new feature to Google Maps. Google street view lets users view actual photos of the locations that they are viewing from the map with just a click of a button. To do this, Google has a car fitted with a camera and a GPS that is driven all over the country by Google employees to take pictures of the streets and other locations and match those pictures with specific locations so that they can be viewed on Google Maps. However the actual pictures and locations were not the issue. The issue was that the Google Street View car "allegedly intercepted information from open wireless networks" (Saltarin). These networks were considered to be public by Google and thus were open to the interception of information. Also "Facebook routinely monitors user chats for suspicious or criminal activity" (Mataconis). This means that Facebook is "reading" all of its users' personal conversations. Anything that is suspicious is sent to a team of employees and actually read by real people that work at Facebook. This is very breaching of its users' privacy. However, if one is not doing anything wrong, then what is there to worry about?

These privacy breaches are not always illegal, but they may be ethically wrong, which is the issue that the public has with them. Google has made a public statement that the monitoring

of Wi-Fi that the company has done using the Street View car was actually not illegal (Saltarin). It is said to have violated the U.S. Wiretap Act. Google claims that this is not true, but San Francisco courts have decided twice that Google's actions were in violation of the U.S. Wiretap Act. Google is scheduled to appeal the court's decision. However, this is not as relevant as the civil cases that have been brought up against Google. Many individuals are suing Google for infringing on their privacy. This means that people are appalled by what Google has done, which, in turn, means that Google has pushed past the ethical boundaries of what people are willing to tolerate. Facebook monitoring the personal conversations is completely legal. It says in Facebook's privacy policy that it can do this. Specifically, the policy states, "We may disclose information pursuant to subpoenas, court orders, or other requests (including criminal and civil matters) if we have a good faith belief that the response is required by law. This may include respecting requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law under the local laws in that jurisdiction, apply to users from that jurisdiction, and are consistent with generally accepted international standards. We may also share information when we have a good faith belief it is necessary to prevent fraud or other illegal activity, to prevent imminent bodily harm, or to protect ourselves and you from people violating our Statement of Rights and Responsibilities. This may include sharing information with other companies, lawyers, courts or other government entities." (Mataconis). Many users are frightened by the fact that some Facebook employees could be reading their conversations, but in fact the process is very particular and tries to make fewer conversations be viewed by actual people. According to Mashable, "The screening process begins with scanning software that monitors chats for words or phrases that signal something might be amiss, such as an exchange of personal information or vulgar language. The software pays more attention to

chats between users who don't already have a well-established connection on the site and whose profile data indicate something may be wrong, such as a wide age gap. The scanning program is also "smart" — it's taught to keep an eye out for certain phrases found in the previously obtained chat records from criminals including sexual predators. If the scanning software flags a suspicious chat exchange, it notifies Facebook security employees, who can then determine if police should be notified. Keeping most of the scanned chats out of the eyes of Facebook employees may help Facebook deflect criticism from privacy advocates, but whether the scanned chats are deleted or stored permanently is yet unknown." (Mataconis). This means that the scanning is actually meant to be used for the good of its users and protection of children, which means that, inherently at least, it is an ethically good move that Facebook has made. However, many users are still scared by this. This may be offset not just by the good that this decision could possibly do, but by the good that it has already done. According to Reuters, "A man in his early thirties was chatting about sex with a 13-year-old South Florida girl and planned to meet her after middle-school classes the next day. Facebook's extensive but little-discussed technology for scanning postings and chats for criminal activity automatically flagged the conversation for employees, who read it and quickly called police. Officers took control of the teenager's computer and arrested the man the next day, said Special Agent Supervisor Jeffrey Duncan of the Florida Department of Law Enforcement." (Mataconis). Law enforcement officers agree with Facebook's policy as a good thing. That same article stated, ""The manner and speed with which they contacted us gave us the ability to respond as soon as possible," said Duncan, one of a half-dozen law enforcement officials interviewed who praised Facebook for triggering inquiries." (Mataconis). Law enforcement officers are supposed to uphold justice and ethical

behavior within society, so their approval of the policy is very promising for the ethical goodness of it.

The services provided by Google and Facebook are free to use. Since users are not paying them for their services, they have to make their money somehow. They do this through the aggregation of data and tracking its users. If one is opposed to this, then that individual does not have to use either of these services. However, a minimal amount of users will actually stop using the services for any privacy breach. This means that, ethically, the privacy breaches are not bad enough to drive users away. A writer at *Searchengineland* said "Sensing a weakness where it might win against Google, Microsoft declared it would anonymize data after 18 months. Yahoo said it would cut retention to only 90 days. Ask launched Ask Eraser, promising instant privacy, for those who wanted it. All this happened in an environment where there was much media focus on search privacy. How'd it work out? None of the Google competitors trying to win with a "private" feature made any impact on Google's share. Yahoo rolled back and starting keeping data up to 18 months. Even Startpage, based out of Europe and with a long-time focus on promising private searching, found its efforts in 2009 didn't pay off. It took until now for Startpage to get to 3 million searches per day." (Sullivan). These other, "safer", options emerged in the market, but users of Google stuck with Google. This shows that people would rather use the more convenient search engine that has a larger variety of options that breaches privacy than the less sophisticated engines that are supposedly "safer". This means that Google, the "more convenient" choice, does not push ethical boundaries far enough to warrant users to stop using their services.

Ethically, anything inside of their services using their servers is fine ethically regardless of whether it is helpful to its users or only to itself, because the company itself pays for the

servers and provides a service. However, anything that breaches privacy outside of the service itself is not, because the companies do not have control over these external domains. This means that tracking cookies that follow users' web histories and program that follow users' sites visited are completely unethical. Companies should not have the right to delve into peoples' personal lives like this, especially just for personal gain of the company. Google and Facebook should not be allowed to track users' like this. Also, interception of information in the real, tangible world is also unethical. Google's Street View car intercepting information is outrageous and completely encroaching on the privacy of people. Some of the people who had their information intercepted were not even Google users, which meant that they had no choice but to have their information intercepted. This means that Google had even less right to intercept people's information. The simple solution to this problem would be to have a protected Wi-Fi and stop Google from intercepting data. However, no one outside of Google knew that this was going on and had no way of protecting themselves. The solutions to the other problems that take place in the realm of the internet would be to block cookies and to install, or possibly create (if one does not yet exist), a program to stop Google and Facebook from tracking a user's data or to not use Google or Facebook at all. Another, more long term, solution could be to develop browsers so that users' could decide easily if they want to be tracked or not. Another solution in the long term would be to pass acts that made these things illegal outside of the sites themselves.

All in all, anything inside of the programs is ethical, while anything outside of the programs is not.

Works Cited

"Google vs. Facebook: How The Two Companies Compare By The Numbers." *The Huffington Post*. TheHuffingtonPost.com, Inc, 17 May 2012. Web. 26 Feb 2014. <http://www.huffingtonpost.com/2012/05/17/google-vs-facebook_n_1525606.html?>.

Mataconis, Doug. "Your Facebook Chats Are Being Monitored, By Facebook." *Outside the Beltway*. Outside The Beltway, 13 Jul 2012. Web. 26 Feb 2014. <http://www.outsidethebeltway.com/your-facebook-chats-are-being-monitored-by-facebook/>

Mullin, Joe. "How much do Google, Facebook profit from your data?." *CNN*. Turner Broadcasting System, Inc, 09 Oct 2012. Web. 26 Feb 2014. <http://www.cnn.com/2012/10/09/tech/web/facebook-google-profit-data>.

Pociask, Steve. "Stealing your privacy -- it's Google once again." *FOX News*. FOX News Network, LLC, 01 Mar 2012. Web. 26 Feb 2014. <http://www.foxnews.com/opinion/2012/03/01/stealing-your-privacy-its-google-once-again/>.

Saltarin, Alex. "Google finds no respite from Street View WireTap case." *Tech Times*. techtimes.com, 30 Dec 2013. Web. 26 Feb 2014. <http://www.techtimes.com/articles/2340/20131230/google-finds-respite-street-view-wiretap-case.htm>.

Sullivan, Danny. "Duck Duck Go's Post-PRISM Growth Actually Proves No One Cares About "Private" Search." *Search Engine Land.* Third Door Media, inc, 22 Jun 2013. Web. 26 Feb 2014. <http://searchengineland.com/duck-duck-go-prism-private-search-164333>.

"Zeitgeist 2012." *Google*. Google inc. Web. 26 Feb 2014.

<http://www.google.com/zeitgeist/2012/#the-world>