Online Privacy Practices, Issues, and Concerns

Is the loss of online privacy inevitable?

Inez Gonzalez
12/13/2010

Table of Contents

Executive Summary

Internet users are increasingly and unknowingly giving up their rights to their private information as they increase their online activities. As other countries have developed more stringent rules on privacy, the U.S. government has taken a wait-and-see approach in terms of regulating the Internet. In fact, it is not clear which government agency is responsible for overseeing the Internet. Is it the Federal Trade Commission (FTC), the Federal Communication Commission (FCC) or the National Telecommunications & Information Administration (NTIA)? Most recently, the U.S. government has indicated an interest in stepping up its oversight efforts and delegating the responsibility to the Department of Commerce.[1] Regardless of what agency ends up the custodian of the Internet, this designation of responsibility should take place soon. It is essential that online privacy rights be addressed, as Eli Pariser, from MoveOn.org, states "before the bones are set in this media framework."[2]

There are various issues and concerns regarding online privacy. It doesn't take much research to come up with egregious examples of unscrupulous third parties hijacking personal information to sell it for profit. There are the popular search engines that in return for providing a valuable free service to offer personalized searches, expect to collect the user's data and to make a profit from targeted ads. And then there are the online profiles that Internet companies are developing about consumers. It took years for Google and other companies to figure out how to make their businesses profitable. This advertisement model based on consumer information will not be easily relinquished. This is why self-regulation has not worked in maintaining online privacy and must be augmented with regulations.

Current Practices

Currently, there is no government agency designated to oversee Internet privacy issues. There is the FTC, the FCC and the NTIA but none of them have authority to fully oversee the Internet. With no government agency responsible, there are no comprehensive regulations that have been developed to protect consumers' online privacy. Current industry practices rely on self-regulation. Understandably, Corporate America is testing the limits of what is acceptable and what is not. The online privacy statements are purposefully long and difficult to

[1] Shiels, Maggie (2010, November 12). Groups applaud push to boost policing of web privacy. *BBC* from http://www.bbc.co.uk/news/technology-11748346

[2] Pariser, E. (2010, October 26). Algorithms, the News and Democracy. Presentation at the Harvard Kennedy School.

understand. Even though there are mechanisms to opt-out of tracking, they are intentionally made complicated to use. The reason there hasn't been a louder public uproar on the need for online privacy regulations may be because most consumers have no idea how their data is being used.

Intentionally or not, consumers' private information is being captured by corporations without proper authorization. Google, the altruistic search company with "Don't be Evil" as a motto, recently found itself in the middle of an international investigation in regards to privacy violations. In May 2010, a German inquiry on Google's Street View technology, which adds images of locations to maps, discovered that Google had "accidentally" grabbed personal data from unsecured hotspots. In total it is estimated to have grabbed about 600 gigabytes of data.[3] Google's collection of wifi data occurred in thirty countries over a three-year period, and several countries are still investigating.[4] In the U.S., Connecticut's Attorney General is leading a 30-state investigation.[5] Meanwhile the U.S. Government, with its laissez-faire approach to online privacy, has been weak in its reaction to this privacy violation. The FTC opened and closed its inquiry on this issue without any action against Google and the FCC is still investigating the matter.[6] Google's original statement on the matter was revised to acknowledge that personal data, including emails, were in fact collected and to promise improved privacy and security practices, "while most of the data is fragmentary, in some instances entire emails and URLs were captured, as well as passwords. We want to delete this data as soon as possible, and I would like to apologize again for the fact that we collected it in the first place. We are mortified by what happened, but confident that these changes to our processes and structure will significantly improve our internal privacy and security practices for the benefit of all our users."[7] Google offered German residents an option to opt-out of its Street View system, allowing users to block images from the service which showed their homes or

---

[3] BBC (2010, October 24). Privacy body to re-examine Google from http://www.bbc.co.uk/news/technology-11614970

[4] Electronic Privacy Information Center. (2010, December 10). Connecticut Attorney General Demands Google Street View Data. Epic.org from http://epic.org/2010/12/connecticut-attorney-general-d.html

[5] BBC (2010, June 23). Google under investigation by Met police from http://www.bbc.co.uk/news/10391096

[6] Schatz, A. & Efrati A. (2010, November 11). FCC Investigating Google Data Collection. *The Wall Street Journal* from http://online.wsj.com/article/SB10001424052748704804504575606831614327598.html

[7] Eustace, A. (October 22, 2010). Creating stronger privacy controls inside Google. *The Official Google Blog* from http://googleblog.blogspot.com/2010/10/creating-stronger-privacy-controls.html

businesses. Germany is the only country in the world where residents have the ability to opt out *before* the image goes live.[8]

This is not Google's only privacy gaffe this year. In November 2010, Google sent a mass email to Gmail users to announce a settlement in a lawsuit regarding Google Buzz, a service launched within Gmail in February, 2010. In its email Google states that shortly after the Google Buzz launch, "we heard from a number of people who were concerned about privacy. In addition, we were sued by a group of *Buzz* users and recently reached a settlement in this case. The settlement acknowledges that we quickly changed the service to address users' concerns…We will also do more to educate people about privacy controls specific to Buzz. The more people know about privacy online, the better their online experience will be." (Google Buzz, personal communication, 2 November 2010).

The most alarming example of online privacy concerns comes from RapLeaf, an online tracking company. The company has created a powerful database of more than 600 million unique addresses. RapLeaf is able to identify a person by their age, gender, education, employment status, number of children and their ages, household income, marital status, political views, interests - and the list goes on. The tracking company has been able to collect this valuable information by connecting the dots to all the information it has been able to harvest from different entities. They have in their possession real names, email addresses with their online activity and behavior. RapLeaf executives say their business offers valuable consumer benefits by allowing people to see relevant advertising and content. When a person logs in to certain sites, the sites sends identifying information to RapLeaf, which looks up that person in its database of email addresses. Then, RapLeaf installs a "cookie," a small code file, on the person's computer containing details about the individual. According to a *Wall Street Journal* report, sites where this takes place include e-card provider Pingg.com, advice portal About.com and picture service TwitPic.com. In some cases, RapLeaf also transmits data about the person to advertising partners. The company executives say that the data it collects is public and that people can permanently opt out of its services at any time. RapLeaf says it doesn't share or sell emails, but under some circumstances it will provide names and other personal details if a client already possesses that person's email address. The *Wall Street Journal* reported several instances where RapLeaf was not following its privacy policy. RapLeaf did make the necessary corrections once the *Journal* brought the violations to its attention.[9]

---

[8] Carr, A. (2010, September 20). Google Gets a Privacy Deadline. *Fast Company* from http://www.fastcompany.com/1690138/germany-sets-deadline-on-google-for-privacy-regulation

[9] Steel, E. (2010, October 25). A Web Pioneer Profiles Users by Name. *Wall Street Journal* from http://online.wsj.com/article/SB10001424052702304410504575560243259416072.html

Behavioral Tracking

Most websites allow advertising companies to place cookies, a bit of computer code, on a user's computer to track online activity and behavior. Cookies are used to track Web searches in order to inform advertisers about users' likely interests. Nevertheless, some cookies do offer convenience to users. For example, cookies allow users to log back on to frequently used Web sites without having to retype user names and passwords, and can keep track of items placed in virtual shopping carts before they are bought. Consumers are able to manage their cookies or delete them from their computer. Now advertisers have started to use more powerful software, supercookies, to better track a consumer online. Supercookies allow for a larger collection of data that can be collected and stored on the user's hard drive while online.[10] Advertisers and others could see weeks or even months of personal data. That could include a user's location, time zone, photographs, text from blogs, shopping cart contents, e-mails and a history of the Web pages visited. Supercookies are not as easily deleted as standard cookies because they store information in multiple places on a computer.

Behavioral tracking will become even more sophisticated with HTML 5, the fifth version of Hypertext Markup Language used to create Web pages. HTML 5, already in limited use, promises to bring in a new age of Internet browsing in the next few years. It will make it easier for users to view multimedia content without downloading extra software; check e-mail offline; or find a favorite restaurant or shop on a smartphone. It also presents more effective tracking opportunities with the use of supercookies. Samy Kamkar, a well-known California programmer, has created a cookie that is not easily deleted, even by experts — something he calls an Evercookie. Kamkar said he created the Evercookie to demonstrate just how thoroughly people's computers could be infiltrated by the latest Internet technology. "I think it's O.K. for them to say we want to provide better service," Kamkar said of online advertisers. "However, I should also be able to opt out because it is my computer." Kamkar said he had no plans to profit from the Evercookie and did not intend to sell it to advertisers. Instead, he has made the code open to anyone who wants to examine it and says the cookie should be used "as a litmus test for preventing tracking."[11]

A growing number of consumers are taking legal action against companies that track computer users' activity on the Internet. The legal cases are based on Flash cookies placed on hard drives by the Flash program from Adobe when users watch videos on popular Web sites like YouTube and Hulu. Class-action lawsuits

---

[10] Richmond, R. (2010, November 10). Resisting the Online Tracking Programs. *The New York Times* from https://www.nytimes.com/2010/11/11/technology/personaltech/11basics.html?src=me&ref=technology

[11] Vega, T. (2010, October 10). New Web Code Draws Concern Over Privacy Risks. *The New York Times* from https://www.nytimes.com/2010/10/11/business/media/11privacy.html?pagewanted=1&_r=1&th&emc=th

have accused large media companies like the Fox Entertainment Group and NBC Universal, and technology companies like Clearspring Technologies and Quantcast, of violating users' privacy by tracking their online activities even after the users took steps to prevent that. The suits claim that the companies collected information on the Web sites that users visited and from the videos they watched, even though the users had set their Web browser privacy settings to reject cookies that could track them. Some privacy advocates are concerned with the fact that Flash cookies can be used to restore HTML cookies that have been deleted from a user's computer, ignoring a user's privacy settings. "The core function of the cookie is to link what you do on Web site A to what you do on Web site B," said Peter Eckersley, a technologist at the Electronic Frontier Foundation. "The Flash cookie makes it harder for people to stop that from happening." According to Adobe, more than 75 percent of online videos are delivered using Flash technology, with media companies also using it to serve games and animation to users. The company says that Flash cookies are intended to be used for basic Web functions like saving a user's volume and language preferences or remembering where a user left off on a video game. In a public letter to the FTC in January, 2010 Adobe condemned the practice of restoring cookies after they had been deleted by a user. The company provides an online tool on its Web site to erase Flash cookies and manage Flash player settings. At least one suit, however, claims that the controls are not easy to reach and are not obvious to most Web users.[12]

Most people control their online privacy by adjusting settings in today's most popular Web browsers, which include Internet Explorer by Microsoft, Firefox by Mozilla, Safari by Apple and Opera, which is used mostly in Europe and Asia and on mobile devices. Each browser has different privacy settings, but not all of them have obvious settings for removing data created by HTML 5. Even the most proficient software engineers and developers acknowledge that deleting that data is tricky and may require multiple steps. Privacy experts say that makers of Web browsers should agree on one control for eliminating all tracking capabilities at once (Vega, 2010). Standard defaults are mainly set to allow for tracking. As users become more informed on how their data is being used and shared, it is likely that they will prefer a different, more private, default setting.

Deteriorating Online Privacy Policies

Facebook (FB) with half a billion users and growing has now surpassed Google as the most popular website on the Internet.[13] FB has been increasingly criticized for its lack of commitment and transparency to online privacy. In the past five years as it has gained power, with the sheer number of its subscribers, it has become embolden to weaken its privacy policies. Jaron Lanier says, "In Facebook

[12] Vega, T. (2010, September 20). Code that Tracks Users' Browsing Prompts Lawsuits. *The New York Times* from https://www.nytimes.com/2010/09/21/technology/21cookie.html?pagewanted=1
[13] Sydell, L. (2010, December 1). New Network Target Discomfort With Facebook. *NPR* from http://www.npr.org/2010/12/01/131700947/new-networks-target-discomfort-with-facebook?sc=fb&cc=fp

we are no longer the client, we are the product."[14] When the service first launched in 2005, its privacy policy created a fortress around personal data: "No personal information that you submit to Thefacebook," its terms of service read, "will be available to any user of the Web Site who does not belong to at least one of the groups specified by you in your privacy settings." In other words, in the original FB, anyone who was interested in getting to know you had to be your FB friend. Late last year, the company announced that a long list of personal details — everything from your profile photo, your friends and fan pages, your gender, your geographic region, and the networks you belong to — were "considered publicly available to everyone,"[15] — no exceptions or opt-outs allowed. Mark Zuckerberg, FB's founder and CEO, defended the change saying that people's notions of privacy were changing. [16] FB was heavily criticized for both reducing its users' privacy and pushing users to remove privacy protections.[17] Groups criticizing the changes include the Electronic Frontier Foundation and American Civil Liberties Union.[18] FB has since re-included an option to hide friends' lists from being viewable. Defending the changes, Zuckerberg said "we decided that these would be the social norms now and we just went for it".[19]

Zuckerberg has become more vocal about his believe that online privacy is immaterial. In January, 2010 Zuckerberg told a live audience that if he were to create FB again today, user information would by default be public, not private as it was for years until the company changed dramatically in December, 2009 (Kirkpatrick, 2010). Nevertheless, public criticism and political pressure have forced FB to backtrack on some of its brazen changes regarding online privacy. In the summer of 2010, FB simplified its privacy settings following criticism from US senators, the European Union and civil liberty groups (Shiels, 2010). It reduced its

---

[14] Lanier, J. (2010, October 4). Seeing Through the Fog of Digital Fads at the Joan Shorenstein Center, Harvard Kennedy School.

[15] Johnson, S. (2010, May 20). Web Privacy: In Praise of Oversharing, *Time*.

[16] Van Buskirk, E. (2010, April 28). Report: Facebook CEO Mark Zuckerberg Doesn't Believe in Privacy.

[17] BBC News (2009, December 10). Facebook faces criticism on privacy change from http://news.bbc.co.uk/2/hi/technology/8405334.stm

[18] American Civil Liberties Union. Facebook's Privacy Transition: Push Facebook in the Right Direction. https://secure.aclu.org/site/SPageServer?pagename=Nat_Petition_Facebook_Policy&JServSessionIdr004=tun9qkc7f3.app20a

[19] Kirkpatrick, M. (2010, January 9). Facebook's Zuckerberg Says The Age of Privacy is Over. *ReadWriteWeb* from http://www.readwriteweb.com/archives/facebooks_zuckerberg_says_the_age_of_privacy_is_ov.php

privacy settings from 50 to 15.[20] Yet it still kept the default setting as sharing all information with everyone.

The Selling of Consumers' Private Information

In October, 2010, the Wall Street Journal reported that some of FB's most popular applications, including FarmVille and FrontierVille, had been sending users' personal information to dozens of advertising and Internet monitoring companies. To correct this problem FB agreed to use encryption on user IDs that are being transmitted to third-party Web sites. The Wall Street Journal, noted that the issue impacted tens of millions of users, even those who had set their privacy settings to the strictest levels. "It would be great if Facebook took steps to keep user information from being transmitted off Facebook's site, but encryption is better than no solution at all," said Ezra Gottheil, an analyst with Technology Business Research.[21] Gothheil continued to say that FB is built on selling user information. They will continue to fix specific problems, as they appear but they won't stop user information from leaving FB.

Now in its latest promotion, FB is pushing a "Like" button which lets sites put little FB buttons on anything from blog entries to T-shirts in web stores. Clicking that button sends that information to FB, which publishes it as part of what it calls the Open Graph, linking your identity to things you choose online. That information, in turn, is shared with whatever sites FB chooses to share it with — and to the sites you've allowed to access your profile (Buskirk, 2010).

Online Profiling

Eli Pariser talks about the "Filter Bubble" and how Google, FB and others are using algorithms to personalize the information we see on the Internet (Pariser, 2010). Based on a user's Internet behavior and activities, the algorithms select search results that are best suited for a user. Pariser states that due to online profiling, two unrelated users searching for the same topic will see different news results on Yahoo! News. It's unclear how FB does its profiling of users, but it is likely that it looks at the pages users "Like" and the applications and games that they download. Pariser claims that the News Feeds that users see on FB are not a random selection from an entire list of friends but rather friends that FB selects as top friends based on the FB's profiling of the users. It is likely that friends that have a different ideology or interests will not show up as often on a user's FB feed.

---

[20] Morozov, E. (2010, June 1). Surfing the Surfer. *The New York Times* from https://www.nytimes.com/2010/06/02/opinion/02iht-edmorozov.html?emc=eta1

[21] Gaudin, S. (2010, October 22). Facebook tackles latest privacy slip with encryption. *Computerworld* from http://www.computerworld.com/s/article/9192638/Facebook_tackles_latest_privacy_slip_with_encryption

Some may not be bothered by the personalized results, but the problem is that most people don't even know this is taking place. Pariser states that the fact that the "filter bubble" is invisible to users and that the user doesn't get to opt-out should be causes for concern. Online profiling may be well-meaning, to help filter by preference, but they have unintended consequences. Limiting consumers to homogenous information that does not take into consideration human nature's ability to change its mind, preference and opinion will do more harm than good to society.

Policy Considerations

Recent privacy breaches, such as Google's Street View and FB's applications transmitting IDs to third-parties, have made the U.S. government reconsider its piecemeal approach to overseeing the Internet. In October, 2010 the White House council on technology announced a new Subcommittee on Privacy and Internet Policy. The subcommittee is comprised of representatives from various parts of the federal government and is charged with developing principles that will attempt to balance the economic opportunity of the Internet with protecting individual privacy. The subcommittee will develop principles and strategic directions with the goal of promoting consensus in legislative, regulatory, and international Internet policy realms. Core principles the committee will base its work on include: facilitating transparency, promoting cooperation, empowering people to make informed and intelligent choices, strengthening multi-stakeholder governance models, and building trust in online environments.[22]

Furthermore, Rep. Joe L. Barton (Tex.), ranking GOP member of the House Energy and Commerce Committee, has already indicated an interest in making Internet privacy a legislative priority for the new Congress. "I want the Internet economy to prosper, but it can't unless the people's right to privacy means more than a right to hear excuses after the damage is done," Barton said.[23]

Do not track

The FTC, the government agency in charge of consumer protections, recently proposed standards for the use of behavioral user data that includes a universal "do not track" mechanism similar to the national "do not call" registry. The agency states that self-regulation has not worked and "that online companies have failed to

---

[22] The White House, Office of Science and Technology Policy. Web October 24, 2010 http://www.whitehouse.gov/blog/2010/10/24/white-house-council-launches-interagency-subcommittee-privacy-internet-policy

[23] Kang, C. (2010, November 4). Internet privacy could be priority in next Congress. *Washington Post* from https://www.washingtonpost.com/wp-dyn/content/article/2010/11/03/AR2010110309508.html?sid=ST2010110400365

protect the privacy of Internet users." The FTC is especially concerned with online third parties that follow a user without the user's knowledge to track them online, and sell the user's information to others without the user's approval. The FTC is asking for industry and public comment on its proposal for the next two months, December and January, 2011. Because the FTC lacks the necessary jurisdiction to impose its entire proposal, it will need the support of Congress to implement parts of its recommendations. For now, the FTC is promoting "privacy by design," where companies are required to build consumer protections in their daily business practices. The FTC is asking the industry to be more transparent in their self-regulation and is recommending that the user be able to look at the data being collected.[24]

The Internet companies, who have been collecting personal data from users and creating a composite of consumers' preferences, are bound to lose billions of dollars in advertising dollars if a "do not track" mechanism is imposed. The online advertisement companies do not support the "do not track" mechanism and prefer to continue self- regulating, promising more new measures of privacy controls. The House Subcommittee on Commerce, Trade and Consumer Protection is holding a hearing early in December, 2010 to discuss the "do not track" mechanism.

Already the conversation about a "do not track" mechanism has resulted in some changes by Internet companies on privacy issues. Google states it supports the idea that consumers should understand their privacy rights, and has simplified its privacy agreement to include a YouTube video. Microsoft declares that its new browser, Internet Explorer 8, includes a feature called InPrivate Filtering that stops data from traveling between a user and third parties who ask for it frequently. The problem with this feature is its lack of practicality; a user has to set the privacy controls at the start of every new browsing session. Although the "do not track" mechanism is a good option, it does not resolve all online privacy issues. Search companies will still be able to compile users' search activities and target certain advertisement to them as a result of their search.

Congress

On the same day that the FTC released its "do not track" proposal, Senate Commerce Communications Subcommittee Chairman John Kerry, D-Mass., said that he is working on privacy legislation that would give consumers more information about what is being collected about them and a way to opt out of it. The bill will be introduced early in the next Congress. The bill mandates that

[24] Wyatt, E. & Vega, T. (2010, December 1). F.T.C. Backs Plan to Honor Privacy of Online Users. *The New York Times* from https://www.nytimes.com/2010/12/02/business/media/02privacy.html?pagewanted=1&_r=2&nl=todaysheadlines&emc=a2

consumers have "three nonnegotiable rights" -- ensuring that all companies adequately secure personally identifiable information; that consumers are told in "clear and concise terms" what firms intend to collect, and why and how the data will be used; and that they be given a "simple mechanism" to opt out of the process. Senator Kerry is weighing including a global opt-out, do-not-track mechanism in the privacy bill.[25]

Additionally, two House bills drafts have been circulated that would make it difficult for advertisers and media firms to create profiles on users for behavioral advertising. The most sensitive information about users – their location, ethnic background, financial and medical data – could only be collected on a voluntary basis. Privacy experts believe that the Republicans may seek a weaker version of those bills in the next Congress (Kang, 2010).

Cybersecurity

In December, 2010 the Australian government plans to implement a cybersecurity consumer program that allows Internet service providers to notify its customers if their computers are taken over by hackers through a botnet. A botnet is a network of infected computers that can number in the thousands, the network is usually controlled by hackers through a small number of scattered PCs. Computer owners are often unaware that their machine is linked to a botnet and is being used to shut down targeted websites, distribute malicious code or spread spam. The U.S. government is taking a look at the Australian plan as a possible solution to the problem of computers across the U.S. increasingly being taken over by hackers and other computer criminals. But U.S. officials do not support the Australian option that allows Internet providers to wall off or limit online usage by customers who fail to clean their infected computers, saying this would be technically difficult and likely run into opposition.[26]

"Cybersecurity expert James Lewis, a senior fellow at the Center for Strategic and International Studies, said that Internet providers are nervous about any increase in regulations, and they worry about consumer reaction to monitoring or other security controls. Online customers, he said, may not want their service provider to cut off their Internet access if their computer is infected. And they may complain at being forced to keep their computers free of botnets or infections. But they may be amenable to having their Internet provider warn them of cyberattacks and help them clear the malicious software off their computers by providing instructions, patches or anti-virus programs." (Baldor, 2010).

---

[25] Gruenwald, J. (2010, December 1). Kerry to Offer Online Privacy Bill. *National Journal.*
[26] Baldor, L.C., (2010, October 16). US studying Australian Internet security program. *Associated Press* from http://news.yahoo.com/s/ap/20101016/ap_on_bi_ge/us_staying_safe_online

In the U.S., Comcast Corp. is already expanding a pilot program that alerts customers whose computers are controlled through a botnet. The carrier provides free antivirus software and other assistance to clean the malware off the machine. The program does not require customers to fix their computers or limit the online usage of people who refuse to do the repairs. (Baldor, 2010) "Voluntary programs will not be enough, said Dale Meyerrose, vice president and general manager of Cyber Integrated Solutions at Harris Corporation. "[W]e need to have things that have more teeth in them, like standards," said Meyerrose. For example, he said, coffee shops or airports might limit their wireless services to laptops equipped with certain protective technology. Internet providers might qualify for specific tax benefits if they put programs in place, he said. Unfortunately, he said, it may take a serious attack before the government or industry impose such standards and programs." (Baldor, 2010).

Conclusion

This paper focused on specific online privacy practices, issues and concerns. The benefits and drawbacks of cookies, used for online behavioral tracking, was discussed as well as the dangers of the hard to find supercookies and hard to delete evercookie. New technology, such as HTML 5, was presented that will bring greater convenience to the consumer but also come with an increase of clandestine consumer tracking. The failures of self-regulation and upcoming proposed legislation were addressed along with the U.S. government's slow response to this important issue. Finally, an example of deteriorating online privacy policies was provided.

The scope of this paper, however, was limited. National security online privacy issues were not examined. For instance, the Obama administration plans to submit a bill to Congress that would require all services that enable communications – including encrypted email transmitters like BlackBerry, social networking Web sites like Facebook and software that allows direct "peer to peer" messaging like Skype — to be technically capable of complying with a wiretap order.[27] Another important topic not analyzed is locational privacy, also known as location privacy. Companies have incentives to keep extensive records of their users' data, so that they can sell more effective advertisements. Should there be a limit on the time a cell phone company keeps users' location history? Consumers seem to enjoy the capability of sharing with others their whereabouts, perhaps because they are unaware of how their locational history could eventually be used against them. For example, would an insurance company be able to obtain location

[27] Savage, Charlie (2010, September 27). U.S. Tries to Make it Easier to Wiretap the Internet. *The New York Times* from https://www.nytimes.com/2010/09/27/us/27wiretap.html?pagewanted=1&_r=1&hp

records and charge higher premiums to someone that frequents bars?[28] The public is slowly becoming aware of the potential downsides of having their locations tracked on a continuous basis. Locational privacy is a topic that should be debated at a national level and limits to its data use must be considered now before Corporate America claims this data as theirs.

The question this paper tried to pose is whether the loss of online privacy is inevitable? Corporate America's answer seems to be a resounding yes, the U.S. government's answer is still out, and consumers are unclear on the ramifications of the question. Before consumers can answer this question they must be informed on the extent of Internet tracking and how their personal information is being used and sold as a commodity. Currently, most consumers are oblivious to what personal data they are giving up every time they download an application. We often hear: "if you don't like what a company does with your data, don't use the service." The reality, however, is that it's become impractical not to use some Internet services. Now that the U.S government is studying online privacy it should consider first and foremost the need for privacy policies to be transparent. Easy to understand videos on privacy policies should be required. Consumers should have access to the information collected about them and who the data has been shared with - similar to how credit reports work. Before information is transmitted to third parties there should be a need for confirmation by the consumer. Consumers should have the right to opt-out from being tracked or from having their data transmitted to third parties. Companies should be heavily fined for online privacy violations; no longer should the claim of unintended online privacy violations be acceptable. This country has tried self-regulation and this approach has failed. Now it's time to focus on informing the public of behavioral tracking and profiling. It's time to educate the public on the mechanisms that exist to protect their private online information. It's time to make online privacy policies transparent and easy to understand.

[28] Blumberg, A.J. & Eckersley P. (August, 2009). Electronic Frontier Foundation. On Locational Privacy, and How to Avoid Losing it Forever.