Tor and Other Browsers:

Why People Afraid of Privacy Breaches Don’t Encrypt Their Data with Tor

Anni Simpson

North Carolina State University

December 4, 2014

Abstract

The web browser Tor and the Tor add-on for other browsers (e.g., Mozilla Firefox) enables users to browse the web anonymously by encrypting personal data markers such as location, IP address, and search engines entries (Diffie and Landau 2007). Tor hides data using a technology called onion routing, which anonymizes online data as it is sent through network nodes called onion routers. As a result, users can “hide” their digital footprints from the NSA, private business (e.g., Facebook, Google, Apple), other law enforcement agencies (e.g., FBI), and Internet service providers (ISPs). Users have several reasons to hide their data (Verble 2014**)**, including hiding criminal behavior (e.g., torrenting) (Ernesto 2013), fears of a surveillance state, and loss of privacy (Solove 2006**)**. However, the use of Tor has recently been vilified as a “web browser for criminals” (Wold) with no differentiating between criminal behavior (e.g., torrenting songs illegally) and simply trying to avoid surveillance, because even just encrypting personal data creates a “law-free zone in this country” where “law enforcement needs to be able to [but can’t] access communications and information to bring people to justice” whether or not there is an warrant for aforementioned data (Masnick 2014). Not to mention there is a strong rhetoric against privacy, because law-abiding citizens “have nothing to hide” (Solove 2008).

The vilification of Tor seems unreasonable when one looks at its history. Onion routing and the original World Wide Web share many historical traits. Both were developed with funding from the United States government, both backed the concept of user “freedom” from its inception, both were released to the civilian public after research was “completed,” and both were reclaimed by the government that released it in the first place in order to control how users accessed it (Diffie and Landau 2007).

Current literature discusses the history of onion routing (Diffie and Landau 2007) but does not explain why how users use it if they do at all. Rather, current literature focuses on its historical development of onion routing/Tor (Diffie and Landau 2007) and the increasing problems of a self-enforced surveillance state in the digital realm (Solove 2008), which includes technology like Tor and other web browsers.

In this paper I suggest that following its entrance into the civilian world, the government is vilifying the use of onion routing to maintain control of the technology and the ability to spy on end users’ online behavior. To do that, I will (1) analyze the literature on the history of onion routing, (2) compare the ways in which normal civilians use each technology, and finally (3) compare the ways in which aforementioned normal use is vilified. I posit that by demonizing privacy, end users avoid privacy-focused web browser Tor and even other alternatives such as Mozilla Firefox.

**1. Literature Review**

*1.1 Onion Routing and Tor*

Onion routing is an Internet technology that anonymizes a user’s data on the web and other Internet applications (e.g., email) by “removing information that identifies him from his requests to Web [and other] servers and removing information from the connection itself that may identify him” (Reed et. al 2002). In essence, the user’s identifying information (e.g., public IP address) is dropped between the entrance node and the exit node; once the initial “request is transmitted to the server, the proxy blindly forward data in both directions between the client and server until the socket is broken by either side,” (Reed et. al 2002) effectively securing a user’s web browsing, email, and other online activity from being traced.

Onion routing works by “using keys determined by the proxy and each onion router as the circuit … [so that] only the client proxy is aware of all nodes on the path which the communication traverses” (Diffie and Landau 2007).

There doesn’t seem to be any data on how to encrypt about the entrance and exit communications (e.g., “clicking send” and the receiving of a communication), just the network communications inbetween. The initial and final communications may have the potential for exploitation alongside of the non-onion counterparts over the Internet, as well as surveillance. However, having middle communications blocked is still a feature unique to onion routing. It is not a feature one sees with typical packet switching.

Tor, or “the onion router” is an overlay Internet application similar to email, the World Wide Web, and FTP which has supposedly exploded in use, although the network has not released any details even on how many users they have for the purposes of protecting user data; they don’t even collect that information to begin with (Diffie and Landau 2007).

In 2003 (Diffie and Landau 2007), “Tor was originally designed, implemented, and deployed as a third-generation onion routing project of the U.S. Naval Research Laboratory. It was originally developed with the U.S. Navy for the primary purpose of protecting government communications” (Tor Project 2014). In an attempt to hide communications for troops stationed to the East, onion routing and Tor in particular were used by the Navy “to disguise their communication patterns” so that “[n]o one watching their ISP connection locally in country can learn their affiliation through tracking with which agency in the United States personnel contact” and so forth (Diffie and Landau 2007).

Considering the high-risk nature of sending troops on missions in other countries, as well as their need to secure highly sensitive data, it’s easy to see why the United States would fund both projects. However, in order to fully take advantage of the potential, the network had to expand.

In spite of the fact that there is “current law-enforcement concerns about tracking networked [civilian] users,” civilians were handed the network tool, because “a widely used anonymity system provides the Department of Defense users the best protection from prying eyes,” (Diffie and Landau), adding a whole host of additional data and communication to the pile of anonymous information.

*1.2 The Silk Road*

The Silk Road is an online marketplace that requires access to onion routing through the Tor browser, a website that “facilitates the sale of illicit drugs” (Martin 2013). Because of the anonymous nature of Tor and onion routing, the Silk Road and its successor, Silk Road 2.0, made it possible for users to buy drugs online with reduced physical and legal danger than buying them off the street. The FBI shut down the original Silk Road and arrested the site’s operator in October 2013 (Flitter 2013), as well as shut down Silk Road 2.0 in November 2014 (Cook 2014). Although not explicitly for drugs – other activities included tutorials on “hacking ATM machines, contact lists for black market connections and counterfeiters, and guns and hit men for sale” – the FBI claimed the Silk Road sold “hundreds of kilograms of illegal drugs” (Flitter 2013).

Without Tor, the trade would not have been possible because of the way it anonymized data (Martin 2013). Tor was not the *only* component in making illegal trade possible – bitcoin, an anonymous currency not tracked by the U.S. or specific to any country, was another tool – but it was certainly part of the equation (Flitter 2013). As a result of the Silk Road and the perceptions of Tor users, the browser bundle has been vilified as a “web browser for criminals” according to American Internet service provider Comcast (Wold).

The association between breaking the law or “having something to hide” is unfortunate, because there are positive uses to Tor and onion routing, as well. Tor has the ability to allow people the right of free speech and access to censored websites; when a user is anonymous and their activity can’t be tracked, banned material suddenly becomes accessible *so long as* the website being accessed allows connections from the Tor network, which isn’t always the case (e.g., Wikipedia.org) (Kuhn et. al 2007).

However, the main activities advertised by popular media seem to be narratives of using the technology to hide harm, not hide benign data.

*1.3 Privacy Concerns*

 For the purposes of this paper, I define privacy in the sense that a person wants (or needs or deserves) to be able to control who has their information and in what context. For example, a user might not want the NSA to know they used Google to search for. This includes both who has the data and knowing who has the data; Solove defines it better by stating that “[p]rivacy involves the ability to avoid powerlessness of having others control information that can affect whether an individual gets a job, becomes licensed to practice in a profession, or obtains a critical loan” (Solove 2006). Unfortunately, the current climate of U.S. affairs prevents users from having that kind of agency; all three entities (private enterprise, government, and Internet service providers) can access that data but do not inform their users what data they have or what they do with it.

 According to de Souza, “the way in which people understand privacy also changes” (de Souza 2011). In her location-focused study, she posited that “[p]eople are sharing their location with a restricted set of known friends, but they might feel their privacy is invaded if they are randomly approached,” and even in cases where the definition of “private” shifts based on the audience at hand, “privacy still matters” (de Souza 2011). This definition continues to support privacy as the desire to control who has access to what data. In the case of locational privacy, that may be only allowing friends to know where a user is.

 According toSolove, “[a]lthough the government played an integral role in the development of massive dossiers of personal information, especially early on, businesses soon began to play an even greater role” because of the role of marketing to consumers (Solove 2006). Without information on consumer purchasing and viewing habits, businesses would have to rely on generalized marketing using census data; however, with access to “a digital dossier” that outlines more specific information about what kinds of people buy what kinds of products and services, business can utilize more “targeted marketing” (Solove 2006).
 Solove’s theorizing is supported by what actually happened with Edward Snowden and the National Security Administration (NSA); in June 2013, The Guardian published leaked information from NSA whistleblower Edward Snowden that claimed, among other things, that the NSA was collecting huge amounts of data on every American in part by requiring Verizon, Google, Facebook, and Apple to install backdoors into their systems so the NSA could extract user data without ever telling Americans that they were even being watched (Verble 2014). Snowden’s interaction with the NSA illustrates a real-world example of data being passed between the government and private enterprises for the purpose of data collection. The leak turned out to be true after the United States government defended the collection of data by arguing the government saved lives with their surveillance and their scope was narrow (Verble 2014).

However, the damage was done. Americans knew the government and big businesses were both spying on their phone calls, texts, instant messages, searches, browsing data, and more, and Edward Snowden’s escape to Hong Kong – then to Russia – illustrates the severity of his whistleblowing; he was going to be in very hot water with the U.S. government if he stayed for trial (Verble 2014).

The government and private businesses weren’t the only ones spying, either. Internet service providers have come under fire for their “six strikes” policies which end the relationship between provider and customer if a customer is caught downloading copyrighted data six times. For such a policy to work, the ISP would have needed to spy on its user activity. For example, Comcast and Time Warner Cable both warned users against peer-to-peer downloading (e.g., downloading a song from Napster or Kazaa) with implied suggestions against torrenting, as well (Ernesto 2013). In the case of Comcast, Comcast fails to inform users that “after four warnings they will be unable to browse the Internet” or “that the notice can be appealed” (Ernesto 2013). So in addition to spying on the customer, similar to the case with the NSA and backdoors installed into popular services (e.g., Facebook), the user is intentionally left ignorant of the whole story. They’re not supposed to know they’re being spied on, and they’re not supposed to know how to appeal ISPs in this endeavor.

Additionally, Comcast threatened briefly to restrict Internet access to their customers who used Tor, although they backpedaled on their original statement (Ernesto 2013).

Solove defines this as the “secrecy paradigm” in which users’ privacy “is invaded by watching and by [denying] public discourse of confidential information” (Solove 2006). Privacy is invaded on both levels by the secrecy of the NSA surveillance program, the ISP’s appeal process in the six strikes’ policies, and the backdoors installed in private services and applications to aid the NSA. However, in the secrecy paradigm, “[i]nformation about an individual … is often not secret but is diffused in the minds of a multitude of people and scattered in various documents and computer files across the country (Solove 2006).

If such a secrecy paradigm exists in American culture from all three levels, users may not know what to do to ensure their privacy is kept intact. The secrecy paradigm removes agency from the user, particularly ignorant users who may not know how to counteract these programs.

The secrecy paradigm is compounded by an American rhetoric that argues that if you have nothing to hide, you won’t mind other people viewing your data, especially when pitted against the counterclaim that an invasion of privacy leads to better security (Solove 2007). According to Solove, the “nothing to hide argument can be made by comparing the relative value between privacy and security” with notable tie-ins to the NSA security breaches called out by Snowden. The idea behind “nothing to hide is that “many people contend that a privacy harm exists only if skeletons in the closet are revealed,” positing that only criminals get caught in the web of surveillance; law-abiding citizens won’t (Solove 2007).

*1.4* *Gaps in the Literature*

As a result of the increasing culture of surveillance in the United States, it seems to be common sense that methods of encryption and privacy are vilified, but there isn’t much in the way of literature on why that is or how it manifests.

Onion routing and Tor are well-researched in current literature, but why the average person without “something to hide,” whether that something is reasonable (e.g., free speech) or not (e.g., buying cocaine), does to secure their privacy isn’t. When “the average person” wants to hide for reasons that don’t exist in either extreme, what are they hiding? Why are they hiding it? Are they even using tools like Tor to encrypt their data if they *do* want to hide their data? These questions aren’t addressed in the literature, and considering the very recent nature of some of the issues posed above, it’s not a surprise.

The closest we get to an explanation is de Souza’s work on locational privacy. de Souza argues that “[w]ith most commercial [location-based services] LBSs, location is traded for convenience and entertainment,” and that “many people are willing to share their location and be surveilled for the convenience of using LBS” or even the “possible serendipitous social encounters enabled by [location-based social networks] LBSNs” (de Souza 2011). The case study on locational privacy was, of course, specific to location-based services (e.g., FourSquare) and locational-based social networks (e.g., Yik Yak), but it gives the literature a starting point for where one might start looking when they look for the discrepancy between user behavior and user concerns. It also doesn’t suggest that users are thinking of the government, of businesses, or of Internet service providers when they think about who they want to share their data with.

The literature that does look at privacy concerns tends to look at the overall picture of what those concerns are or breaks them down into component parts (e.g., *government* surveillance or *private enterprise* surveillance). Even literature on “nothing to hide” as a rhetorical device is problematic when legal browsers like Tor are painted as criminal, when legal methods of obtaining data are associated with illegal abuses of them (e.g., torrenting), and when the digital landscape is changing so dramatically and so quickly, it’s hard to keep up with what is legal, what isn’t, and what lies are being caught in the noise.

**2. Methods**

I relied both on academic and popular literature for my literature review. The literature on Tor, onion routing, and user privacy concerns is a currently growing field. I ended my analysis of popular media review in October 2014 for the sake of time.

Before we can describe how users secure their data online, we first need to define what people are doing online. In order to analyze normal behavior, I developed a survey using Google Drive’s Survey creation feature. The survey was six questions long and asked users (1) what they use the Internet for, (2) what web browser they use most, (3) how they access the Internet (i.e., phone, tablet, desktop/laptop), (4) who they are afraid of collecting their data, and (5) what information they want to protect (e.g., IMs, medical history). The survey was disseminated online via Internet- and privacy-related sub-communities on reddit.com. Specifically, I sought responses from the following subreddits: samplesize, darknet, privacy, and technology.

For all questions but the question about primary web browser, respondents could select more than one answer, as well as add in a write-in (e.g., “none,” “ID theft”). These answers were also automatically added to the spreadsheet.

I received 258 anonymous answers, which were automatically added to Google Drive in spreadsheet format.

 From the survey results, I coded the answers by online activity, privacy concerns, preferred browser, and platform (e.g., desktop vs. mobile). I looked for raw numbers on each of these topics and made simple bar graphs from them. I also analyzed all of the “other” responses to see if there was overlap (e.g., write-in for “none” happened more than once for privacy concerns). To search for number of responses, I transferred the spreadsheet into a searchable Word document and searched for the number of responses for specific phrases used in the spreadsheet. This was to ensure that I didn’t count incorrectly or leave anything out, although I did go through all of the responses manually and highlighted all of the “other responses” using a color-coding scheme.

 I also compared the privacy statements of five of the different browsers used: Mozilla Firefox, Google Chrome, the Tor bundle, Microsoft Internet Explorer, and Apple Safari against the data from the respondents’ primary browser.

The reason I chose to compare Firefox, Chrome, and Tor was that theses browsers, up until recently, were considered alternatives to the default web browsers: Internet Explorers for Windows computers and Safari for Apple computers. The default web browser for some users has changed since the proliferation of smartphones and tablets, however; Android-powered devices use Google Chrome as their default. However, for desktop users, it is still an alternative.

 The reason I chose to compare Internet Explorer and Safari was because they are defaults on Windows and Apple platforms respectively. If you purchase a Windows or Apple device, the web browser associated with it will be installed and ready to use right away.

 The distinction of an “alternative” browser is important, because it requires the user to seek out and download that browser. Some agency, an external or internal motivator, is required for an end user. Specifically, the end user will have to open up the default browser to download and install their preferred browser instead.
 I analyze the browser privacy policies from most secure to least secure.

**3. Results**

*3.1 Survey Results*

Nearly every user (97.29 percent) cited concerns that their Internet service providers (ISP), the government, or private enterprises (e.g., Facebook) were “spying” on their behavior online. That means more than half of respondents were afraid that each of the three main categories (“ISP,” “private enterprise,” and “government”) were violating their privacy. It’s relevant to note that “none” was *not* listed as an option; all respondents who said “none” or “don’t care” wrote the answer in. The same is true of “other,” which included “identity theft” and “employer.” However, there is a significant response towards a fear of privacy invasion when you compare the five none responses to over 150 for ISP, private enterprise, and government *each*. Because I allowed for multiple answers, there was overlap between them. Many users were afraid all three of the main categories were violating their privacy in some way. *See figure 1.*

Figure 1

Only 23.64 percent of respondents reported using Mozilla Firefox as their primary browser, with a shockingly low number of respondents reported using Tor (1.16 percent). Considering some of the subreddits I submitted the survey to (namely “privacy” and “darknet”), this was a little shocking.

The vast majority of respondents (68.22 perfect) used Google Chrome, followed by Firefox at 23.64 percent, followed by Apple Safari at 4.65 percent. Google was the clear winner of the respondents’ browser preference. See figure 2.

Figure 2

The vast majority of respondents (93.80 percent) also stated they used a personal desktop/laptop computer at least part of the time. Following personal desktop/laptops, 76.74 percent of respondents used their phones to access the Internet; 36.82 percent of respondents used their work desktop/laptop; 31.01 percent of respondents used their tablet, and 11.24 percent of respondents used a school desktop/laptop. Respondents were allowed to select as many devices as they actually used, rather than just their primary source of connectivity. See figure 3.

Figure 3

*3.2 Privacy Policies*

Tor makes *explicit* promises to protect customer privacy:

“The Tor software protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, it prevents the sites you visit from learning your physical location, and it lets you access sites which are blocked” (Tor Project 2014).

While Tor encrypts user data to prevent identifying information from being paired with an individual user or their browsing habits, Mozilla Firefox also states in its privacy policy “mission statement” that privacy is a primary concern, stating that Mozilla as a corporation only gathers information after the users gives Mozilla permission to do so:

“Your privacy is an important factor that Mozilla (that's us) considers in the development of each of our products and services. We are committed to being transparent and open. This Mozilla Privacy Policy explains generally how we receive information about you, and what we do with that information once we have it … When we have asked and received your permission to share it” (Mozilla 2014).

However, Google Chrome makes no such promises about avoiding data collection:

“When you use any browser, including Chrome, to contact Google's servers, by default Google receives standard log information including your system’s IP address and one or more cookies … Information that Google receives when you use Chrome is processed in order to operate and improve Chrome and other Google services. Information that other website operators receive is subject to the privacy policies of those websites. Chrome stores information on your system in order to improve Chrome’s performance and to provide you with useful features and services” (Google 2014).

Microsoft similarly admits to collecting data from its users, admitting to using it to improve Microsoft products (which are not named) and improve features/usability for the end user:

“The information we collect from you'll be used by Microsoft and its controlled subsidiaries and affiliates to turn on the features you're using and provide the services or carry out the transactions you've requested or authorized. It may also be used to analyze and improve Microsoft products and services. In order to offer you a more consistent and personalized experience in your interactions with Microsoft, information collected through one Microsoft service may be combined with information obtained through other Microsoft services” (Microsoft 2014).

 For Safari, the privacy policy depended on the user’s location. For the purposes of this study, I surveyed American users, so I chose the “United States, Canada, & Puerto Rico” region with a focus on the United States. Safari had the worst privacy violations in their privacy policy based on the earlier definition. They not only collect data but admit that the data they collect isn’t anonymized and that it’s used for advertising in addition to the improvement of its services:

“Personal information is data that can be used to identify or contact a single person. You may be asked to provide your personal information anytime you are in contact with Apple or an Apple affiliated company. Apple and its affiliates may share this personal information with each other and use it consistent with this Privacy Policy. They may also combine it with other information to provide and improve our products, services, content, and advertising” (Apple 2014).

Of all the browsers, Tor promises the most security in terms of anonymizing user data, as well as not actually collecting other data so that it can’t be used against a user. Mozilla Firefox follows in kind by promising that security and privacy are important to them and they secure user’s permission before they collect or utilize the data they receive from their users.

It’s interesting to note that Google, Microsoft, and Apple all announce that they collect data with no mention of asking the user. By using their products, it’s implied a user consents to the collection of data for whatever purposes the company may want it for. That isn’t necessarily a bad thing, but there is a difference between asking for consent and assuming consent.
 Google, Microsoft, and Apple take it a step further by stating they use data from their users to improve services, to optimize the user experience, and in Google and Apple’s cases, target advertising they believe will be relevant to individual users. This is a far cry from not collecting data at all the way Tor handles privacy. Targeted advertising means the collection of data isn’t anonymous and can be traced back to individual people.

**4. Discussion**

It’s interesting to note that although nearly all respondents cited at least one privacy concern, very few of them chose to “do” something about it in the way of choosing a “privacy” friendly (as defined earlier) browser. Although Google Chrome freely admitted to cataloguing and utilizing their user’s data, they were by a wide margin more popular than any other browser.

A couple of factors may explain its popularity. For one, Android smartphones and tablets require a Google account to use, which integrates into the device’s email and web browsing functionalities. The default browser on Android devices is Google Chrome. However, even on desktop computers, Google integrates its web apps (e.g., Google Chrome and Google Drive, Google Calendar, and Gmail). The ease of integration is compounded by the mobility of Chrome’s features. If a user signs into Google on their browser on one device, the bookmarks and settings can be transferred to another.

I think that de Souza’s findings on locational privacy are applicable here. Google offers a lot of products that can sync with one another: Google Drive (formerly Docs), Gmail, Google Calendar, Google Maps, Google search, Google+, Picasa, Google Chrome, and Google Analytics for those who run a personal website. All of these apps are linked to one account, and information in one app (e.g., searching Google Maps in Chrome) is applicable everywhere else on the same account (e.g., pulling up the same search on Google Maps on a phone as one’s getting ready to drive somewhere). Even if someone doesn’t use all of the aforementioned apps, the functionality to integrate them if a user ever decides to use another app is there. de Souza found that users were willing to trade privacy for convenience, and the same may be true here. There’s a lot of convenience and removed redundancy in searching and adding in data to be had if a user turns to Google for what can amount to *life management*.

Tor doesn’t offer *that*.

These reasons may explain the discrepancy between user desires for privacy and their desire for convenience and feature-heavy applications. However, without further data, it’s impossible to say.

Considering the vilification of Tor as “criminal,” it’s easy to see why people don’t use it. However, Tor can be used as an add-on for other web browsers, as well (including Google Chrome and Firefox). Only three people took the survey noted that they used Tor, and in every instance, they noted they were using an extension for Mozilla Firefox instead of the Tor browser.

Although Firefox has the second-strongest commitment to privacy and the ability to log into the same account in order to preserve settings, it isn’t a default browser on iOS, Mac OS, Windows, or Android, it doesn’t integrate with other apps, and offers no secondary service (e.g., Drive) at all.

However, leaning towards the default and offering features can’t explain everything. Only two people total used Internet Explorer, and Microsoft offers a comprehensive set of features comparable to Google, as well as installs as the default browser in Windows. In fact, it’s such a strong default that it requires extra effort just to remove the browser; it can only be uninstalled through the Windows features section of Windows instead of the Uninstall a Program window.

Based on the literature review, it’s hard to argue that the reason people don’t use Tor is because they don’t know what it is. It exists as a focal point in both popular press and academic articles, but by and large, the popular press reports negative things about Tor. A popular Internet service provider, one that provides caps and throttles users, actually called it a “web browser for criminals.” This background leads me to the conclusion that consumers are using “safe” web browsers rather than ones that can actually protect user data. I reach that conclusion based on the *second highest* web browser used, which was Mozilla Firefox and the second most “private” browser. If ISPs can and do spy on data and come out against Tor, it’s not surprising that users don’t use it during normal use. And there’s always the possibility that they do use Tor – just not as the primary web browser.

Nor can the ease of Google’s integration with one’s personal devices account for all of the support it received from the data. A large portion of the respondents stated that they used a personal desktop or laptop – more than any other platform. While Chrome certainly supports integration across devices, Mozilla Firefox and Microsoft (using Bing as a basis) offer these features, as well. And as I stated above, Mozilla Firefox was still the second most popular browser even after Safari (which comes with iOS and Mac OS) and Internet Explorer (Windows Phone and Windows OS). When given a browser that’s safe from criticism, that seems to be what people chose *in spite of the convenience of using the default web browser*.

It’s worth mentioning that for a long time, Google appeared to support privacy, as well. Although they have backdoors for the NSA *now*, their original company motto was “don’t be evil” (Thompson 2014). This motto originated under the original leadership of Eric Schmidt (who is now gone) and Larry Page (Thompson 2014) and likely helped develop brand loyalty as Google was in its fledgling state, only offering a web browser before it ever offered Google Maps, Gmail, hardware (e.g., Android tablets), or even Google Chrome. This image may have something to do with its popularity here, as well as its impact on user perceptions.

**5. Conclusion**

 Based on my findings, I believe that users trade their privacy for convenience to the browser that offers the most features. In spite of privacy violation concerns and Google admitting they use user data for their own purposes (and to make their features work more fluidly). And because Google has a history of “do no evil,” it would be easy to trust them to continue this policy (although it no longer is a part of their policy), they may appear to be the least evil of all options if one wants to use their extensive life management services.

 I also believe that based on Google’s former goodwill

 Because my scope was so limited, it’s hard to make generalizations about the general population. I would suggest further examinations into people’s browsing habits, as well as take additional information into account, including (1) demographics (age, income level, race, etc.), (2) operating system used, (3) operating system with browser taken into account (e.g., Safari on iOS), (4) distinguish between Tor and the Tor add-on for other browsers and (5) *if* there are any privacy concerns in the future, possibly using statistical data rather than a survey for operating system and browser preference across the general population. While I believe that this is a matter worth investigating, the scope I took on for this paper was far too limited.

 Another possible area of study may include looking at how users handle add-ons. There are a number of add-ons that claim they protect a user’s privacy available for Google Chrome and Mozilla Firefox, as well as other browsers, including: Ghostery, Disconnect, AdBlockPlus, HTTPS Everywhere, and ShareMeNot. My study did not take into account how users handle add-ons, although it’s relevant to the conclusions of my study.

Works Cited

Apple. (26 November 2014). “Apple – Legal – Privacy Policy.” Retrieved from

<https://www.apple.com/legal/privacy/en-ww/>.

Cook, James (6 November 2014). “FBI Arrests Former SpaceX Employee, Alleging He Ran The

'Deep Web' Drug Marketplace Silk Road 2.0.” *Business Insider*. Retrieved from

<http://www.businessinsider.com/fbi-silk-road-seized-arrests-2014-11>.

De Souza E Silva, A. and Frith, J. (2012) *Mobile interfaces in public spaces: Locational privacy,*

*control and urban sociability,* New York: Routledge.

Diffie, Whitfield and Susan Landau. (2007). *Privacy on the Line: The Politics of Wiretapping*

*and Encryption*. Boston: MIT Press.

Ernesto. (3 March 2013). “Comcast’s “Six Strikes” Email with Infringement Details Surfaces.”

*TorrentFreak*. Retrieved from

[http://torrentfreak.com/comcasts-six-strikes-email-with](http://torrentfreak.com/comcasts-six-strikes-email-withinfringement-details-surfaces-130303/)

[infringement-details-surfaces-130303/](http://torrentfreak.com/comcasts-six-strikes-email-withinfringement-details-surfaces-130303/).

Ernesto. (17 June 2013). “Six Strikes “Copyright Alert” Warns Subscribers for Dangerous P2P

Software.” *TorrentFreak*. Retrieved from

[https://torrentfreak.com/six-strikes-copyright](https://torrentfreak.com/six-strikes-copyrightalert-warns-subscribers-for-dangerous-p2p-software-130617/)

[alert-warns-subscribers-for-dangerous-p2p-software-130617/](https://torrentfreak.com/six-strikes-copyrightalert-warns-subscribers-for-dangerous-p2p-software-130617/).

Flitter, Emily. (2 October 2014). “FBI shuts alleged online drug marketplace, Silk Road.” *Yahoo*

*News*. Retrieved from

[http://news.yahoo.com/fbi-raids-alleged-online-drug-market-silk](http://news.yahoo.com/fbi-raids-alleged-online-drug-market-silkroad-153729457.html)

[road-153729457.html](http://news.yahoo.com/fbi-raids-alleged-online-drug-market-silkroad-153729457.html).

Google. (14 November 2014). “Google Chrome Privacy Notice.” Retrieved from

<https://www.google.com/chrome/browser/privacy/>.

Martin, James. (7 October 2013). “Lost on the *Silk Road*: Online drug distribution and the

cryptomarket.” *Criminology and Criminal Justice*, 14, 351-367.

Masnick, Mike. (16 October 2014). “FBI Director Continues His Attack On Technology, Privacy

And Encryption.” *TechDirt*. Retrieved from

<https://www.techdirt.com/articles/20141016/11531128849/fbi-director-continues-his-attack-technology-privacy-encryption.shtml>.

Microsoft. (26 November 2014). “Internet Explorer 11 privacy statement.” Retrieved from

<http://windows.microsoft.com/en-us/internet-explorer/ie11-preview-privacy>

statement#ie=ie-11.

Mozilla Corporation. (13 November 2014). “Mozilla Privacy.” Retrieved from

<https://www.mozilla.org/en-US/privacy/>.

Reed, M.G., P.F. Syverson, and D.M. Goldschlag. (6 Aug 2002). Anonymous connections and

onion routing. *Selected Areas in Communications*, *16*(4), 482-494. Retrieved from

<http://ieeexplore.ieee.org.prox.lib.ncsu.edu/xpls/abs_all.jsp?arnumber=668972&tag=1>.

R. Dingledine, N. Mathewson and P. Syverson, (1 October 2007). “Deploying Low-Latency

Anonymity: Design Challenges and Social Factors.” *Security & Privacy, 5*(5), 83-87. Retrieved from <http://ieeexplore.ieee.org.prox.lib.ncsu.edu/xpl/articleDetails.jsp?arnumber=4336287&tag=1>.

Solove, Daniel J. (2006). *The Digital Person: Technology and Privacy in the Digital Age.* New

York: New York Press.

Solove, Daniel J. (7 February 2008). “‘I’ve Got Nothing to Hide’ and Other Misunderstandings of Privacy.” *San Diego Law Review, 44*, 745-772.

Thompson, Cadie. (19 August 2014). “Does 'Don't be evil' still apply to Google?” *CNBC*.

Retrieved from <http://www.cnbc.com/id/101923422>.

Tor Project. (14 November 2014). “What is the Tor Browser?” Retrieved from

[https://www.torproject.org/projects/torbrowser.html.en. 14 Nov. 2014](https://www.torproject.org/projects/torbrowser.html.en.%2014%20Nov.%202014).

Verble, Joseph. (3 September 2014). “The NSA and Edward Snowden: surveillance in the 21st

century.” *ACM SIGCAS Computers and Society, 44*(3), 14-20. Retrieved from

<http://dl.acm.org.prox.lib.ncsu.edu/citation.cfm?doid=2684097.2684101>.

Wold, Nathan. (13 September 2014). Comcast Declares War on Tor? *DeepDotWeb*. Retrieved

from <http://www.deepdotweb.com/2014/09/13/comcast-declares-war-tor/>.