Talanda Williams
CST 300 Writing Lab
10/18/2016

The Ethics of Internet Anonymity

Internet anonymity is the action of purposefully hiding personal or identifiable information when interacting online. There are varying levels of how anonymity can be achieved, ranging from simple measures like a nondescript username choice on a per site level to using The Onion Router (Tor) for full network coverage. There is an ongoing discussion on internet anonymity with regard to government surveillance, freedom of speech, and the legality of surrounding issues. Edward Snowden, who will be discussed later in this paper, has brought on a new wave of public interest and scrutiny when it comes to anonymity and any potential rights United States citizens have. Simultaneously, problems with illegal activity on the 'dark web', also discussed within, cannot go ignored. The argument of internet anonymity, government surveillance, and the relation to privacy rights and freedom of speech is nothing new. This paper will seek to explain the background of internet anonymity, and apply it to these parties: regular people, criminals, cyberbullies, and governments.

The 1990s, when people were connecting to other networked computers for the first time, marks the start of this privacy debate (Bartlett, 2015). There was an abundance of illegal activity taking place anonymously including untraceable pedophiliac networks and hackers stealing intellectual property (Bartlett, 2015). The US Secret Service launched Operation Sundevil in May of 1990 to focus on eliminating this activity; at the same time laws were put in place to force telecommunication companies to provide data about their customers (Bartlett, 2015). To counteract these measures, a group of Californian libertarians calling themselves 'cypherpunks' started to create ways around these surveillance attempts which ultimately became the backbone of modern surveillance avoidance techniques (Bartlett, 2015).

During the same time frame, another US programmer, Phil Zimmerman, created the 'Pretty Good Privacy' (PGP) tool because "he felt alarmed at what seemed to him like a concerted and disproportionate push by the law into citizens' private space" (Bartlett, 2015). This sentiment is still held today by some, yet conversely there is also the belief that prior to the Internet, anonymity was still a rare thing; thus lacking privacy on the Internet would not be a breach of privacy or freedom of expression (Zhuo, 2010). These events of government action and civilian counter-action have been considered a 'crypto-war' (Bartlett, 2015). In the 1990s, the Internet was still in its infancy, and it was not until the early 2000s when more people were online and sharing personal information, purposefully or otherwise, that the question of digital rights and freedoms became more commonplace (Bartlett, 2015).

In the late 1990s and early 2000s, Yahoo! expanded its company from the United States, a government with First Amendment protection of hate speech, to France, where hate speech is illegal, which raised a court case against the company (Zajácz, 2013). The case surrounded the problem of offering Nazi memorabilia over the Internet to citizens in France, where they would be illegal to own. Yahoo! was not running the store but argued on its behalf (Zajácz, 2013). Yahoo! stated "imposing national regulation on the Internet was both impossible and undesirable"; it would lead to ripple effects with devastating consequences as the communication rules would become a 'race to the bottom' set by the most restrictive national law (Zajácz, 2013). It was also stated that Yahoo! did not know the location of their users, and therefore, could not limit their results specifically for France (Zajácz, 2013).

However, even when not using personally identifiable information on the Internet, there are other methods of gaining knowledge about a user. Internet geolocation technology is concerned with determining the physical location of a user and their devices (Muir, 2009). Geolocation showed that Yahoo! could determine the location of their users and had been using that information for targeted ads.

The French court considered the argument ‘overblown’ and ordered the removal of the material to French citizens or Yahoo! would have to pay a $13,000 per day fine (Zajácz, 2013). Yahoo! conceded to removing all Nazi material from the site, creating the first incident of indirectly regulating the Internet by government command. This shattered the long held belief that regulation would be nigh impossible (Zajácz, 2013). As we move into the 2000s, key events in the usage of internet anonymity unfold.

In 2002, The Onion Router (Tor) project launched bringing about a new way of anonymous internet activity (Alqahtani & El-Alfy, 2015). Tor is free and open source software that establishes anonymous network connections through a system of proxy servers with entry and exit nodes called onion routing (Savchenko & Gatsenko, 2015). It works, on a high level, by passing information through a chain of connections starting with an entry node and ending with an exit node that sends the message encrypted (Alqahtani & El-Alfy, 2015). Therefore, the user remains unidentified by the exit node or any relay nodes not immediately connected between the source and destination data (Alqahtani & El-Alfy, 2015).

Onion routing, the name stemming from each message being covered by various levels of encryption analogous to the vegetable, was developed by US Naval Research Laboratory in the late 1990s (Alqahtani & El-Alfy, 2015). Tor started as a research project and became an open-source charity aimed “at ensuring that civil rights activists and journalists [could] browse the net safely around the world” (Bartlett, 2016). Tor would later be used to send information from Chelsea Manning, then known by Bradley, to WikiLeaks for sharing 718,030 sensitive documents with the public. WikiLeaks describes themselves as a not-for-profit media organization, whose purpose is the “disseminating [of] original documents from anonymous sources and leakers” (Zittrain & Sauter, 2010). Founded in 2006,

they accept restricted or censored material of significance but no rumors or opinions (Zittrain & Sauter, 2010). Julian Assange, the spokesperson and probable founder of WikiLeaks, has a personal philosophy against “secrecy-based authoritarian conspiracy governments” (Zittrain & Sauter, 2010). In April, July, and October 2010, WikiLeaks released video and logs relating to the Afghan and Iraq war (Zittrain & Sauter, 2010). In November 2010, WikiLeaks started releasing 251,287 diplomatic cables bringing the total to those 718,030 documents obtained allegedly from Manning.

WikiLeaks has used five news organizations to release this and other information, including classified material. WikiLeaks not only releases information that pertains to wars, but its releases are usually political in nature. In December 2007, WikiLeaks released its first document: a manual instructing US Army soldiers on how to deal with prisoners in Guantanamo Bay (CNN Library, 2016). In 2008 they released internal documents from the Church of Scientology, emails from Sarah Palin, and names and addresses of members of the British National Party. The most recent release was the July 2016 leak of 20,000 emails between the Democratic National Committee suggesting favoritism of Hillary Clinton over Bernie Sanders (CNN Library, 2016).

When talking about internet anonymity, Julian Assange and Edward Snowden are considered the ‘poster boys’ (Bartlett, 2016). In 2013, Snowden, through the Washington Post and the Guardian publications, released information of the National Security Agency’s (NSA) domestic surveillance (Kaplan, 2014). Snowden also released information about the NSA’s interception of Taliban fighter emails, phone calls, and radio transmissions in Pakistan, and other surveillance worldwide including hacking computers in China and Hong Kong (Kaplan, 2014). It has been a contentious topic whether Snowden is a traitor or a whistleblower. Snowden and WikiLeaks often disagree on the method of releasing information, even though they both view these as essential; Snowden has criticized WikiLeaks

on their refusal to curate their documentation (Chokshi, 2016).

With recently perceived governmental overreach into our digital space, we begin our descent into a second crypto-war over the right to privacy (Bartlett, 2015). The right to privacy is the idea that the personal information of a citizen is confidential and kept from public scrutiny (Sharp, 2013). However, the term 'right to privacy' is not stated in the US Constitution explicitly, but is split among various amendments including the First, Third, Fourth, Fifth, Ninth, and 14th Amendments, depending on level of interpretation (Sharp, 2013).

The First Amendment provides freedom of speech, another debated aspect of internet anonymity and the privacy of beliefs (Sharp, 2013). The Third Amendment is privacy of the home against housing soldiers, while the Fourth Amendment is similarly home related against unreasonable searches (Sharp, 2013). The Fifth Amendment provides protection for self-incrimination which infers privacy of personal information and lacking particular disclosures (Sharp, 2013). The Ninth Amendment has been used to justify privacy based on the Bill of Rights (Sharp, 2013). Debatably, most argued on the subject of the right to privacy is the Due Process Clause of the 14th Amendment which government surveillance would seem to undermine if internet privacy rights were detailed.

Internet anonymity can be seen from various different angles, making it difficult to pick a specific law to credit or discredit as a right. For instance, tracking cookies can be considered an invasion of privacy; they are small amounts of data captured during Internet usage that can be sent back to the host website which requested it (Sharp, 2013). The information in your tracking cookies may not specifically carry identifiable information, but combined with information like location, history, and Internet Service Provider (ISP) can be used to discover such information. However, tracking cookies are not illegal, and are typically used for non-nefarious reasons like targeted advertising or market research (Sharp, 2013).

In addition to basic internet browsing, internet anonymity varies with the exact website visited as well. Internet anonymity remains in high focus when discussing social media platforms such as Facebook, Twitter, Instagram, and forums like Reddit or Tumblr. Information added to any of these sites can be public facing (in some cases are only such), and can have a profound impact ranging from personal information being used to judge employment worthiness to cyberbullying. Internet anonymity may have previously been important to specific subsections of people but that distinction now applies equally to everyone. Thus, the remainder of this paper will focus on the importance of these combined histories on four groupings and their ethical frameworks: regular people, criminals, cyberbullies, and governments.

Regular people are defined as law-abiding citizens and are further broken down into those concerned or not with anonymity. Criminals are any persons involved in illegal activities, although this paper will focus on online illegal activity such as drug dealing or buying and persons seeking child pornography. Cyberbullies, depending on the severity and location of their bullying or trolling, may be engaged in legal or illegal activity, but do require anonymity, and are therefore specifically separate from the regular people above. Lastly, governments are majorly represented by the views of the United States government unless specified. These subsection will also be classified as a particular ethical framework, namely either Ethical Egoism, Kant's Ethics, or Utilitarianism.

Starting with regular people unconcerned with anonymity: these are everyday people who have either formed an opinion that 1) having privacy concerns are only for those with things to hide or 2) people potentially just unconcerned with the argument entirely. They have a low interest in the specifics of anonymity or privacy as it pertains to their daily lives. Since they have the view that they themselves have nothing to hide, they may also tend to find it acceptable for some private details to be available for

government surveillance if it assists in the capture of criminals. This subcategory of people appear to follow the Ethical Egoism framework; they do not see the benefit of internet anonymity in their own lives, therefore they do not see why others would need it. According to a privacy and surveillance survey by Pew Research Center in 2015, the percentage of Americans who explicitly dislike internet anonymity is 16 percent.

Those 16 percent of Americans may get their rationale from the numerous negative effects anonymity has on people while online. Psychological research has proven multiple times over that anonymity does increase unethical behavior (Zhuo, 2010). A pervasive form of which is known as trolling: "the act of posting inflammatory, derogatory or provocative messages in public forums" (Zhuo, 2010). And while trolling itself is fairly new, the concept relating to anonymity and immortality goes back centuries. Plato remarked about anonymity, believing that without full disclosure, humans would behave unjustly knowing they wouldn't be held accountable for their actions (Zhuo, 2010). This certainly rings true for cyberbullies who often post in droves on popular news sites and forums with statements unfathomable in face-to-face conversations.

Americans concerned with privacy tend to be focused on attempting to maintain it for a number of reasons not limited to work/life balance, interpretation of legal rights including due process, and the general expectations of permission and publicness. This subcategory of people appear to follow Kant's Ethics; they view their First Amendment right as covering internet anonymity and the various good results of preserving that right. They also are wary of providing too many freedoms to be restricted or quantified by the government, a slippery slope sort of notion. That the most rational conclusion is the protection of these rights and the cornerstone of internet activity.

Based on the graphic below from the Pew Research Center survey results, the importance of

controlling their information is nuanced, with different opinions based on information such as who can access it, why they need it, and who they can in turn provide it to. It also noted that permission and publicity are important for influencing views on surveillance, with 88 percent saying it is important to not be watched or listened to without their permission (Madden Additionally, these privacy-concerned regular people have very low expectancy levels of their data remaining safe, even if it is given freely: 31 percent believed government agencies could keep their records private and secure with some level of confidence (Madden & Rainie, 2015).

As for companies, 31 percent also felt varying levels of confidence in landline telephone companies with the safety of those records, and slightly higher at 38 percent confidence in the records at credit card companies (Madden & Rainie, 2015). These people feel that they do not have a lot of control over how much information is currently collected on them and how that data might be used. Despite this, according to the same survey, few have changed their behavior to lessen their ability to be tracked as easily (Madden & Rainie, 2015). This could be due to their belief that even with internet anonymity, motivated people or organizations would be able to discover private details fairly easily, a notion held by 64 percent of responders (Madden & Rainie, 2015). & Rainie, 2015).

Of the regular people concerned with anonymity and privacy, if there was a greater awareness of governmental monitoring programs, it directly correlated to lessening or eliminating the length of time they believed some records should be retained (Madden & Rainie, 2015). When asked specifically about data the government collects in anti-terrorism efforts, 65 percent believe there are not adequate limits on what internet or telephone data they can collect (Madden & Rainie, 2015). 55 percent of Americans, based on the survey, support the idea of internet anonymity for at least some kind of unspecified internet activity. It seems that the citizens and government back and forth privacy dispute has not been lost on the regular American.

Criminals doing illegal activities, however, are typically very interested in the anonymous aspect needed to maintain their identity a secret and avoid prosecution. Despites its humanitarian roots, 44 percent of websites accessible through Tor are criminal (Bartlett, 2016). These websites use the same protocols as Tor to stay hidden, and can sell a variety of illegal items or activities (Bartlett, 2016).

Known as the ‘dark net’, these websites are not indexed by search engines and, therefore, unreachable otherwise. Criminals have a high stake in being able to purchase or sell drugs or guns online through the dark net, specifically high profile sites like the Silk Road. Criminals can also use Virtual Private Networks, with or without Tor, to provide further anonymity for themselves, although not exclusively. This subset of people, like those non-considered with privacy, appear to follow the Ethical Egoism framework. They are motivated by actions that affect themselves and their own circumstances.

Another way that criminals may use internet anonymity is by doxing, although legality depends on each state. Doxing is the intentional public release of personal and/or private information onto the Internet (Douglas, 2016). Doxing is split into three forms: providing the identity of someone previously anonymous, releasing private information to reveal specific details of an individual’s private circumstance, or revealing intimate personal information in an attempt to damage the credibility of that individual (Douglas, 2016). Doxing can be used for vigilantism or whistleblowing as well, but tends to assist illegal activities such as stalking or harassment (Douglas, 2016).

With the variety of reasons for internet anonymity, it is important to consider how governments view and handle these situations. Governments find a high sense of importance in being able to identify their citizens’ activity which may be useful in spotting, or proving, illegal activities. State and Federal judges have continuously been subject to cases trying to balance citizen’s First Amendment rights with the government’s ability to be effective (Kosseff, 2014). Common occurrences surround defamation cases, where identification of the defendant is key, attempting to subpoena their ISP for their name and address (Kosseff, 2014). The Supreme Court, however, has not ruled the specific right for internet anonymity in speech, and thus the various lower courts have conflicting results (Kosseff, 2014). Although most of these examples are people or companies trying to get information from other people o

r companies, sometimes it's on a larger governmental scale.

The Department of Defense, for instance, has the goal to have a secure uninterrupted flow of information among its allies or internally while obstructing the ability for adversaries to do the same (Zajácz, 2013). They find that having the most amount of data possible does not impede any rights, but is used to help further find criminal activity. If anyone is affected, the governmental view would be that it is minor in the grand scheme of keeping the entire country safe. This would appear to follow the Utilitarianism framework, where the justification of trying to break anyone's internet anonymity is for the greater good of the whole.

To counterbalance all of these competing views and ethical frameworks, there seems to be three options for moving forward in this space. 1) The classification of online privacy and internet anonymity as protected Freedom of Speech exclusively. 2) The dismantlement of the dark web and increased monitoring of internet users. 3) The creation of policy and procedure to specifically classify online activity as Freedom of Speech but also processes for government to access company data of individuals. We will address these three options one by one, with potential positive and negative effects of each.

Although there are nefarious reasons for remaining anonymous, there are still many highlights on the need for it. Option one seeks to cover this important rationale, requiring internet anonymity to be a protected Freedom of Speech exclusively and to increase its usage. Proponents of this theory cite the many proper reasons such as facilitating the flow of information, protection of reputation and assets or avoiding persecution, aiding unbiased assessments, or a range of more rationales (Douglas, 2016). A survey of people on popular website Stack Exchange shared their views on a forum post in 2011. Jeff Ferland asked "why does one need a high level of privacy/anonymity for legal activities?" and he rece

ived responses highlighting their importance. Rory Alsop's answer was the example of privacy when showering, no one is doing anything wrong but there is a high expectation of privacy; that this expectation should be the baseline unless consciously and deliberately waiving it. Conversely, proponents argue that internet anonymity is negatively affecting not only our laws and terrorism efforts but impacting our youth. They face numerous effects including enhanced peer pressure due to group conformity, cyber bulling or insults, sexual harassment or identity theft from a survey of children averaging 15 years old (Keipi & Oksanen, 2014).

For option two, dismantling the dark net would not be an easy task, based on the decentralized nature of onion routing. Additionally, the non-discriminatory monitoring of all internet users would come at a high cost, but potentially provide a high value as well. Removing the ability to be anonymous would greatly curb many hateful things said online, after all how many people would continue their vitriol if their name was attached? The government would be able to openly collect data and decide what of it is useful information in the fight of terrorism domestic and internationally. On the other hand, what if the rules that the government decides change? What if they are not following the essential morals of right and wrong? Sometimes, opponents argue, laws must be broken for process to occur; think about the legality of homosexuality or desegregation (Alsop & Ferland, 2011). They argue that framing the question as privacy is only for those doing wrong, is misleading and that it is really an argument of liberty versus tyranny (Alsop & Ferland, 2011).

Both option one and two argue utilitarianism ideas, on different sides of the spectrum on internet anonymity. I agree and argue that internet anonymity is crucial to American rights and democracy and claim option three as a virtue ethics framework. Internet anonymity enables commenters to discuss unpopular political views, expose government corruption, or seek information on sensitive topics safely

(Kosseff, 2014). In some form, American democracy is based on anonymity; the Federalist Papers, a symbol of our nation's founding, were published under the pseudonym Publius (Kosseff, 2014). Internet anonymity should be covered under Free Speech and with the ability to be disclosed legally. Governments can have access to anonymous data by going through the proper channels of due process and legal obtainment, rather than spying on its citizens as disclosed by Edward Snowden. If governments can responsibly use the power associated with breaking anonymity, then citizens can accept the privacy restrictions when it helps to protect the overall country. It requires all subset groups to keep the balance by remaining responsible, which admittedly, would be difficult.

The laws would have to be wide enough to not just cover the specifics of internet activity, but the devices that usage occurs on. We could not be allowed to remain anonymous on our computer while our cellphones, work environments, or location data is being monitored or harvested. Just as we cannot have our telephone tapped without legal action and warrant, we should have protection on our electronic devices of communication. While these protections would still allow governments to monitor criminal activity, it would not deter hurtful but not illegal activities of cyber bullying. However, I think that is a separate law consequence of needing more specific restraints around electronic harassment. We cannot stand to further stay in this grey area of ambiguity.

References

Alsop, R., Ferland, J. (2011, September 28). Why does one need a high level of privacy/anonymity for legal activities? - Information Security Stack Exchange. Retrieved from http://security.stackexchange.com/questions/7666/why-does-one-need-a-high-level-of-privacy-anonymity-for-legal-activities

Alqahtani, A., & El-Alfy, E. (2015). Anonymous connections based on onion routing: A review and a visualization tool. *Procedia Computer Science, 52*, 121-128.

Bartlett, J. (2015, January 14). Will online anonymity win the war of openness vs privacy? – Jamie Bartlett | Aeon Essays (E. Lake, Ed.). Retrieved from https://aeon.co/essays/will-online-anonymity-win-the-war-of-openness-vs-privacy

Chokski, N. (2016, July 29). Snowden and Wikileaks clash over how to disclose secrets - The New York Times. Retrieved from http://www.nytimes.com/2016/07/30/us/snowden-wikileaks.html

CNN Library (2016, August 3). WikiLeaks Fast Facts - CNN.com. Retrieved from http://www.cnn.com/2013/06/03/world/wikileaks-fast-facts/

Douglas, D. (2016). Doxing: A conceptual analysis. *Ethics and Information Technology, 18*(3), 199-210.

Keipi, T., & Oksanen, A. (2014). Self-exploration, anonymity and risks in the online setting: Analysis of narratives by 14–18-year olds. *Journal of Youth Studies, 17*(8), 1097-1113.

Kosseff, J. (2014). Do we have a right to online anonymity?. *The News Media and the Law (Online), 38*(1), 32-33.

Madden, M., Rainie, L. (2015, May 20). Americans' attitudes about privacy, security, and surveillance | Pew Research Center. Retrieved from http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Muir, J., & Oorschot, P. (2009). Internet geolocation: Evasion and counterevasion. *ACM Computing Surveys (CSUR), 42*(1), 1-23.

Savchenko, I., & Gatsenko, O. (2015). Analytical review of methods of providing internet anonymity. *Automatic Control and Computer Sciences, 49*(8), 696-700.

Sharp, Tim. (2013, June 12). Right to privacy: Constitutional rights & privacy laws. Retrieved from http://www.livescience.com/37398-right-to-privacy.html

Zajácz, R. (2013). Wikileaks and the problem of anonymity: A network control perspective. *Media, Culture & Society, 35*(4), 489-505.

Zhuo, J. (2010, November 29). Online, Anonymity Breeds Contempt - The New York Times. Retrieved from http://www.nytimes.com/2010/11/30/opinion/30zhuo.html

Zittrain, J., Sauter, M. (2010, December 9). Everything you need to know about Wikileaks. Retrieved from https://www.technologyreview.com/s/421949/everything-you-need-to-know-about-wikileaks/