Lucas Jennings

Dr. David Thaw

HONR 268E

13 December 2011

Internet Anonymity: Is it Worth the Risks?

People have always valued their privacy. They don't want strangers, or even friends, knowing everything about their lives. This desire to have certain things kept private is demonstrated in the structure and freedom of the internet. In cyberspace, many ways exist for users to remain anonymous while being online. Email and social media accounts can be created without any form of verification of identity, and methods exist that allow users to browse the web without revealing identifying information. It is now even possible to anonymously transfer money online. While most consumers enjoy this privacy, it also brings great risks. Current infrastructure provides an environment where hackers, scammers, predators, and organized crime can thrive. As the internet continues to grow, we must assess whether or not the benefits gained by allowing privacy on the internet are worth the risks of criminal acts stemming from anonymous activity over the web.

The current internet infrastructure allows many ways for people to gain the anonymity that they crave. While email and social media accounts often ask for some personal information, such as name, birthday, gender, and location, the services do not verify people's identities It is very easy for someone to create an account with false information, making the owner of such accounts a great uncertainty. This provides an

easy method for anonymous communication over the internet.

In addition to privacy in communication, methods exist by which users can make their browsing virtually untraceable by not revealing their IP address. One method by which to do this is to use an anonymous proxy server. This server requests the website that you want to view and then sends the page to the user. Since the web server receives a request from the proxy server rather than the user's computer, the website server receives the IP address of the proxy server instead of the user, thus allowing the user to remain anonymous (Gralla). Another simple method people use to prevent giving up their IP addresses is the Tor network. This service simply requires that users download some simple software and use the Tor browser. After starting Tor, all of a user's online activities are routed through a giant network of Tor servers, making the IP address of the user untraceable(CITE – Computer World).

Recently, online systems have emerged that even make anonymous money transfer online possible. These are the online equivalent of cash, allowing users to make transactions that do not leave detailed, traceable records linked to personal information. One example is a service called Bitcoin. Bitcoin is a unique digital currency used in many private online transactions. Bitcoins are originally generated by miners, computers who devote CPU power to running a special piece of software that works to solve puzzles. As these puzzles are solved, the machines are rewarded with bitcoins. Although all bitcoins originate from these miners, there are various exchanges set up where people can acquire bitcoins without having to use their computer to mine them. Physical bitcoins can be purchased in-person and redeemed for digital bitcoins online. In addition,

websites such as Mt. Gox run online bitcoin exchanges with up-to-date exchange rates between bitcoins and various real world currencies, allowing users to purchase bitcoins with Paypal, credit cards, or direct transfers from a bank. What sets Bitcoin apart from other forms of online payment, such as Paypal, is its ease of registration. Setting up a bitcoin account is much like setting up a common email account in that no verification of identity is required. There is no need for users to provide credit card information or link bitcoin accounts to physical bank accounts. Since these accounts are easily created, it is not only possible to have an anonymous account, but also to route transactions through several temporary accounts so that funds are not easily traceable. By mining bitcoins on one's own computer, buying them in person at a bitcoin exchange, or routing bitcoins purchased online with a credit card through numerous temporary accounts, users are left with many ways to convert cash into this anonymous online currency (Wallace).

People have always believed that privacy is an important value that needs to be upheld. The Constitution guarantees basic privacy rights by protecting against unreasonable searches and seizures in the Fourth Amendment. In the majority opinion of the Supreme Court case *Griswold v. Connecticut*, Justice William Douglas described a general “right to privacy” that comes from a combination of the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments ("The Supreme Court . Expanding Civil Rights . Landmark Cases . Griswold v. Connecticut (1965) | PBS"). When browsing the internet, people don't want to be tracked. Likewise, they do not want to have unnecessary information gathered about their habits. Most users don't want to reveal even simple information, such as their web browsing history. A recent Gallup Poll showed that 67%

of Americans opposed the use of targeted advertising based on past websites visited (Puzzanghera). People don't want detailed logs to be kept about their internet activity, and they do not like cookies gathering data about them as they browse the web. As a society, we prefer to keep most things to ourselves.

Anonymity is particularly important to protect concerning political movements. This principle dates back far before the internet age. Between 1787 and 1788, a collection of articles known as The Federalist Papers were published in New York newspapers. These articles were persuasive political pieces arguing in favor of ratification of the Constitution and pointing out the benefits of the new system of government. All of these were signed with the alias Publius to protect the names of the authors, who are now believed to be Alexander Hamilton, James Madison, and John Jay (Whitten). Such political thought was considered radical at the time, and likely would have led to persecution of the authors, However, the anonymity provided by publishing under an alias allowed these men to voice their opinions without fear of harm.

Similar scenarios have occurred in recent history. During the political unrest following a hotly contested presidential election in Iran in 2009, anonymous internet communications played an important role in the unfolding of events. Supporters of the Moussavi campaign used facebook pages to voice their anti-government sentiments, organize protests, and warn of government police activity. When protests erupted, the government attempted to shut off communications by cutting off text-messaging and mobile services across the country. In response, Moussavi supporters turned to twitter to inform the outside world of what what going on inside Iran during this tumultuous time

(Nasr). The anonymity of these services allowed such supporters to do so without fear of being caught and harmed by the current government.

Even more recently, anonymous social media posts have had an effect on the start of a revolution in Egypt in early 2011. During this time, pro-democracy supporters, opponents of President Hosni Mubarak, used twitter and facebook to spread their messages and organize protests. Although these social media sites were subsequently blocked by the Egyptian government, the protesters were still able to anonymously spread news and their political opinions through a service set up by Google and Twitter. This service converted voicemails left on a specific phone number into tweets that would be posted with the "#egypt" hash tag (Iduqboe). Even though protesters were not able to use the internet to connect with each other, they were still able to publicly voice their concerns to the world without leaving any clues that might help them be identified by the Egyptian government.

Along with the benefits of internet privacy, there also come many great risks. The aforementioned techniques of hiding IP addresses help provide cover for lots of cyber crime. Anonymous activity allows hackers to carry out there work undetected. They can steal sensitive data, bring down websites through DDoS attacks, and reveal confidential documents without leaving behind information that will compromise their identity. In October of 2011, the hacking group Anonymous launched a DDoS attack on the website belonging to the Oakland Police Department. Due to the nature of these type of attacks, the police were not able to make any arrests in connection with the incident (Kovacs). Even more severe damage has been done by a group known as LulzSec. In addition to

DDoS attacks, LulzSec hacks into sites and leaks sensitive data to the public. In one very recent incident in early December 2011, LulzSec hacked into Portuguese government databases and released personal information, including name, rank, identification number, employment history, and contact information for more than 100 Portuguese police officers (Wilson). In a similar but even more costly incident in 2008, hackers compromised the Choicepoint database, which held sensitive information for thousands of US residents. In total, 13,750 people had personal information, including social security numbers, taken from this data breach (Krebs).

Likewise, scammers can carry out their schemes while remaining hard to trace, causing much loss to unknowing users. People are tricked into giving away sensitive financial information through promises of riches from foreign accounts they receive by email. Due to the ability to hide their IP addresses and the ease of creating email accounts with false information, the senders of these email scams are nearly impossible to catch.

The anonymous internet also creates an environment where sexual predators can thrive. Since no verifying information is required to open social media accounts, predators can easily provide fake information and pose as someone else. Many teenagers are being taken advantage of because there is no way to definitely know the owner of such accounts. In addition to the possibility of abduction, many children are displayed unwanted pornographic material through chat rooms and other methods of online communication. An astounding 25% of children say that they have been exposed to unwanted pornographic material online ("Online Child Predator Statistics"). With most

chat rooms not even requiring users to create accounts, these sexual predators continue to be able to prey freely.

Perhaps the most frightening illicit activities that are carried out anonymously on the internet are those involving organized crime such as weapons and drug trafficking, forgeries, and assassinations. Online marketplaces such as Silk Roads allow users to buy these products and services from brokers they would otherwise be unable to contact. The site must be accessed through Tor, so authorities are not able to trace users by their IP addresses. Sellers accept payment into temporary Bitcoin accounts that are deleted soon after the transaction is finished, eliminating any chance that they can be tracked by their payment ("USING SILK ROAD"). Such a reliable, hard to track system is made possible through all the anonymity allowed on the internet.

With so much crime occurring online because users are able to remain anonymous in their activities, a solution must be found to help stop these hackers, scammers, predators, and traffickers. There must be measures put in place to help identify the perpetrators of such crimes. However, the restrictions put in place must be carefully considered so as to protect the personal privacy of most internet users.

A common suggestion as to how to help alleviate this problem is to implement a system of internet driver's licenses. But what exactly constitutes an internet driver's license? There is much debate surrounding what this type of system would look like.

The simplest idea of an internet driver's license is a simple set of credentials that allow you to log on to all of the websites that require authentication. This is very similar the current multiple sign-on services offered today. A user would have one identity and

password that would allow them to log in to the restricted areas of all sites on the internet to which they should be granted access. This identity would be supplied by a third-party company. Proponents of this plan include Facebook, who is making a push to use Facebook accounts as this centralized log in system (Smith).

This plan would still allow some privacy for the user, as they would still be able to anonymously browse sites that would normally not require an account or log-in. It would also likely help reduce sexual predators, as they would not be able to create false accounts on social media sites and chat rooms in order to exploit children. Email scam artists would be unable to function since they would no longer be able to create anonymous accounts. Illicit drug and arms trade would also be made considerably harder since all communication and financial tools would require the user's central log-in credentials.

However this method also has several drawbacks. Under this plan, anonymous political speech would cease to exist. Oppressed peoples that were previously able to use the internet to speak out against their government regimes would be easily tracked by those in power. These political advocates would have to remain silent or face punishment. This method would also create a much greater risk if a user's credentials were compromised. A hacker that gained access to a user's account would not only have a false identity under which to communicate, but also access to all of a user's personal and financial information. The feasibility of being able to implement such a plan is also very low. It would be difficult for a third-party company to verify the identity of each user, and a system would have to be devised to keep users from creating multiple

accounts. While this plan might solve a couple of the internet anonymity problems, it is definitely not a useable solution.

In early 2011, US Commerce Secretary Gary Locke announced a similar idea for solving the problem. Under his plan, a private company would create a centralized payment identity for each user that would be used at other online retailers. Sites not dealing with financial transactions would not use this form of authentication (Wagenseil).

This plan, targeted primarily at decreasing identity theft, would do little to solve any of the internet anonymity problems. While it would decrease the number of online financial accounts that users would have to keep, it would also give a hacker access to all of a user's e-commerce power if their identity were to be compromised. Even though the number of potential targets for identity theft would less, the severity of damage caused per account hacked would be much greater. This plan would do nothing to alleviate the problems that come from anonymous communication, including sexual predating and email scamming, as these forms of communication would continue to remain completely anonymous. Along with not stopping these problems, this plan would continue to make anonymous political speech possible. It would also continue to allow users to browse the internet privately, as they would only be required to be authenticated when they were making a financial transaction. While being ineffective against stopping untraceable communication, it would help to slow down drug and arms trafficking online by making online payment impossible without proper credentials. Even though criminals would still be able to communicate privately online, their inability to transfer money anonymously would be a hindrance. This government plan may be a viable option if combined with

other measures. However, it is not a total solution by itself.

One of the more complex solutions has been suggested by Craig Mundie, Microsoft's chief research and technology officer. He envisions a three-tiered system, with separate levels of identification for people, machines, and programs. He indicates that the system should work much like the physical world, where only certain places require identification. Users would still be able to browse the web anonymously, but they would be required to provide authentication for financial transactions and the like (Kiviat).

While explicit details of this plan have not been released, it has the potential to solve some of the major problems caused by internet anonymity. By requiring multiple forms of authentication to make financial transactions online, it would eliminate any hope criminals had of being able to transfer cash in an untraceable manner. Authenticating based upon not only the user, but also the machine, would make it much more difficult for hackers to steal someone's identity and financial information.

The unavoidable trade-off with this plan involves exposing scam artists and predators at the cost of stopping anonymous political speech. With sexual predators, email scammers, and political activists all using similar communication tools, it is difficult to come up with any system that would allow people to speak out against a government without fear of punishment while at the same time identifying those who scam others out of money and prey on children. At this point it is unclear whether Mundie's plan would allow anonymous communication for all of these groups or force them all to identify themselves. In either case, his plan cannot be totally successful

unless there is a way to differentiate between those hiding their identities for political speech and those who are hiding them because they are participating in criminal activity

An good solution would erase all of the problems of fraud and anonymity while still allowing unidentifiable political speech and basic user privacy. Such a solution would combine Mundie's idea of multi-layer authentication with new tools to help distinguish between motives for anonymous communication. The system would require users to register in person with proper credentials to prove their identity. Each user would then be issued a personal identity, along with a removable drive containing other identification information. Each drive would be uniquely paired with the owner's identity, creating a unique combination. While browsing the web would still be anonymous, financial transactions would, however, require both user identity and password as well verification from the portable drive. Most online communication tools, including social media and email would use the personal identification and accompanying drive as log-in information, The drive would have information such as a person's name, birth date, and gender so that users would not be able to attempt fraud. However, a few regulated online communication tools would still exist that would not require authentication. Such tools would not have accounts and would not allow communication between users. Rather, these services would allow users to anonymously post their thoughts into public space.

This system would prevent identity theft by hackers, as the dual verification system would require physical possession of the drive in order to authenticate. This verification system would prevent anonymous transfer of funds, crippling criminals '

ability to trade illicit substances online. The linking of a user's identity information to communication accounts used to interact with other users would stop fraud by predators as well as schemes by email scammers. However, this system would still keep a reasonable level of privacy for those do not wish to be closely monitored, as users would not have to be signed into the verification system to browse the general web and visit sites that did not have financial or communication tools. It would also not too greatly inhibit political activists. While they would not be able to use the internet to communicate privately among each other, those who wanted to speak out against a government or political group would still be able to anonymously spread their thoughts through the public forum without fear of being harmed.

Although this plan isn't quite ideal, it does address the primary issues associated with the debate over internet privacy. However, implementing this plan would not be feasible without a vast change in internet infrastructure and international cooperation. The entire layout of the internet would have to be revised, such that all the services requiring verification would communicate with users through secure authentication servers. Offices would have to be set up across the globe to verify identities and issue personal internet identities and accompanying drives. An international organization would have to be formed that oversaw the program, including the verification offices and authentication servers. In addition, this organization would have to have protocol for licensing all of the online financial and communication tools, as access to the authentication servers would have to be tightly controlled. This organization would also need to devote a division to detecting illicit web tools that provided a means of user-to-

user interaction that did not go through the authentication servers.

All of these requirements show that even with the proper technology, implementation of this type of plan is not foreseeable anytime in the near future. In addition to likely public opposition for the extra complications that would be associated with using the internet, this plan would require worldwide cooperation on an unprecedented level. Funding such a project would also prove to be a burden, as the cost of undertaking such a project would certainly be very great.

Despite a wide variety of ideas, there is not yet an ideal solution to the problems that are posed by the current anonymous internet structure. Almost all plans requiring centralized identification techniques would be hard-pressed to get every country to agree to their terms. The public would likely not agree to any change that would result in less privacy for users browsing the internet. In addition, there is a virtually unsolvable trade-off between giving users privacy in browsing the internet and identifying cyber criminals. Criminals are constantly inventing new tools of communication and finance that cannot be tracked. Until a new solution emerges, the problem lies in deciding whether or not the benefits are worth the risks in regards to internet anonymity. Is letting people browse the internet unmonitored worth the potential risk of identity theft by hackers? Is the gain from stopping sexual predators and email scam artists worth the cost of giving up anonymous political and revolutionary speech over the internet? As a society, these are the questions we must answer in order to come up with worldwide policies regarding the acceptable level of privacy and anonymity that should exist on the internet.

Works Cited

Gralla, Preston. "How to Surf Anonymously without a Trace - Computerworld." *Computerworld - IT News, Features, Blogs, Tech Reviews, Career Advice*. 12 Mar. 2007. Web. 13 Dec. 2011. <http://www.computerworld.com/s/article/9012778/How_to_surf_anonymously_without_a_trace?taxonomyId=16>.

Iduqboe, Douglas. "How Twitter Is Helping with the Egyptian Revolution | Smedio." *Smedio I The New Media and Social Web Online Magazine*. 4 Feb. 2011. Web. 13 Dec. 2011. <http://smedio.com/2011/02/04/how-twitter-is-helping-with-the-egyptian-revolution/>.

Kiviat, Barbara. "Microsoft's Craig Mundie Wants Driver's Licenses for the Internet | The Curious Capitalist | TIME.com." *The Curious Capitalist | Commentary on the Economy, the Markets, and Business | TIME.com*. 30 Jan. 2010. Web. 13 Dec. 2011. <http://curiouscapitalist.blogs.time.com/2010/01/30/drivers-licenses-for-the-internet/>.

Kovacs, Eduard. "Anonymous Launches DDoS Attack on Oakland Police Website - Softpedia." *Latest News - Softpedia*. 28 Oct. 2011. Web. 13 Dec. 2011. <http://news.softpedia.com/news/Anonymous-Launched-DDoS-Attack-on-Oakland-Police-Website-230677.shtml>.

Krebs, Brian. "Security Fix - ChoicePoint Breach Exposed 13,750 Consumer Records." *Blogs & Columns, Blog Directory - The Washington Post*. 19 Oct. 2009. Web. 13 Dec. 2011.

<http://voices.washingtonpost.com/securityfix/2009/10/choicepoint_breach_exposed_137.html>.

Nasr, Octavia. "Tear Gas and Twitter: Iranians Take Their Protests Online - CNN.com." *CNN.com - Breaking News, U.S., World, Weather, Entertainment & Video News*. 15 June 2009. Web. 13 Dec. 2011. <http://www.cnn.com/2009/WORLD/meast/06/14/iran.protests.twitter/index.html>.

"Online Child Predator Statistics." *SentryPC - Parental Control Software*. Web. 13 Dec. 2011. <http://www.sentrypc.com/statistics.htm>.

Puzzanghera, Jim. "What Internet Users Want | Nearly 7 of 10 Internet Users Don't Want Targeted Ads, Poll Finds - Los Angeles Times." *Featured Articles From The Los Angeles Times*. 23 Dec. 2010. Web. 13 Dec. 2011. <http://articles.latimes.com/2010/dec/23/business/la-fi-do-not-track-20101223>.

Smith. "Privacy and Security Fanatic: Facebook Wants to Issue Your Internet Driver's License." *Network World*. 12 Jan. 2011. Web. 13 Dec. 2011. <http://www.networkworld.com/community/blog/facebook-wants-issue-your-internet-drivers-li>.

"The Supreme Court . Expanding Civil Rights . Landmark Cases . Griswold v. Connecticut (1965) | PBS." *PBS: Public Broadcasting Service*. Dec. 2006. Web. 13 Dec. 2011. <http://www.pbs.org/wnet/supremecourt/rights/landmark_griswold.html>.

"USING SILK ROAD." *Gwern.net*. Web. 13 Dec. 2011. <http://www.gwern.net/Silk

%20Road>.

Wagenseil, Paul. "Feds Propose Universal Internet “Driver’s License” | SecurityNewsDaily." *Daily Security News Protecting Home, Internet & Identity Theft | Internet Virus & Scams, Spam Filtering | SecurityNewsDaily*. 10 Jan. 2011. Web. 13 Dec. 2011. <http://www.securitynewsdaily.com/feds-propose-universal-internet-drivers-license-0417/>.

Wallace, Benjamin. "The Rise and Fall of Bitcoin | Magazine." *Wired.com*. 23 Nov. 2011. Web. 13 Dec. 2011. <http://www.wired.com/magazine/2011/11/mf_bitcoin/all/1>.

Whitten, Chris. "Federalist Papers." *Founding Fathers*. Web. 13 Dec. 2011. <http://www.foundingfathers.info/federalistpapers/>.

Wilson, Tim. "Resurgent LulzSec Attacks Government Sites In Portugal - Dark Reading." *Dark Reading | Security | Protect The Business - Enable Access*. 8 Dec. 2011. Web. 13 Dec. 2011. <http://www.darkreading.com/security/attacks-breaches/232300133/resurgent-lulzsec-attacks-government-sites-in-portugal.html>.