Received 25 August 2015
Revised 25 August 2015
Accepted 7 September 2015

An analysis of tools for online anonymity

Stephanie Winkler and Sherali Zeadally
College of Communication and Information, University of Kentucky, Lexington, Kentucky, USA

Abstract

Purpose – The purpose of this paper is to examine the possible explanations for the slow adoption and development of online anonymity technology. The ability to remain anonymous while engaging in different activities, online is increasingly sought after by consumers with privacy concerns. Currently, the only way to maintain online anonymity is through the use of technology. This paper reviews and analyzes the tools currently available to consumers to maintain online anonymity. There are only four tools available to consumers to ensure online anonymity: anonymous remailers, rewebbers, The Onion Router (Tor) and the Invisible Internet Project (I2P). These tools provide the protection needed for an Internet user to remain anonymous but suffer from a lack of usability and adoption.

Design/methodology/approach – The authors have selected a few specific online anonymity technologies based on the following criteria: the technology satisfies our full anonymity definition, the technology is currently available for public use and the technology has been academically researched.

Findings – Few anonymity technologies are available for public use that offer the ability for full online anonymity, and these technologies are difficult for the average computer user to operate. Further research is still needed to help determine what the average user wants to see in an anonymity technology as well as ways to help users integrate the technology into their commodity software (such as Web browsers). Future online anonymity technologies should enable the user to decide when, how and with whom their information is shared if it is shared at all with ease and simplicity.

Originality/value – The authors identify, explain and analyze publicly available online anonymity technologies in terms of their usability. The authors identified ways as to how online anonymity technology can be improved to increase public adoption. The authors make pertinent recommendations on how the design and development of online anonymity technology can be improved in the future.

Keywords Privacy, Anonymity

Paper type Research paper

1. Introduction

Early in the history of the Internet, Web hosts were marked by researches as holding the potential to leverage an immense amount of control over information and Internet users (Adam, 1991). This can be seen today, as tracking the Web activities of individuals and storing the data has become pervasive in society with the increase of data mining and the lack of protection consumers have against these practices. Even when an individual uses software to tell companies they do not wish to be tracked, there is no guarantee that the parties involved will respect this wish and many of them do not (Mayer, 2011). Once this data are collected, the consumer has no control over how this data is used, who has access to it or how long the data exist. Data collected from an individual including browsing history, online forms, and Web searches can be relatively innocent when examined in the context of that individual. When that data are taken out of context, it can potentially be incriminating (e.g. a search history containing how to phrases

International Journal of Pervasive Computing and Communications
Vol. 11 No. 4, 2015
pp. 436-453

1742-7371
DOI 10.1108/IJPCC-08-2015-0030

referencing illegal activity). Data brokers are companies that exclusively deal with the collection of consumer data to sell for various reasons, the most common being to marketing firms for targeted advertising (Anthes, 2015). Data collected by Web sites can be used for improving features of the Web sites, such as suggested searches, and is typically considered a valuable part of research (Chen and Liu, 2004). However, this data can also be stored on servers for an indefinite period of time (Nunan and Domenico, 2013; Weber and Henrich, 2012), removing the data from the context of the individual. One solution to this is to make efforts to remain anonymous during online activities (Beato *et al.*, 2014) so that this wealth of information cannot be connected to the user instead of worrying about how the information is managed after the fact. Anonymous is defined as having no identity. However, defining what it means to be anonymous online has been a point of debate among experts in the field.

2. Online anonymity

Social science scholars who research anonymity online have defined it in numerous ways, mainly focusing on how a person's identity is seen by other online users. This has been separated into three levels: visual anonymity, disassociation with real and online identities and lack of identifiability (Morio and Buchholz, 2009). *Visual anonymity* is a level granted to nearly any form of online communication, as it refers to if someone can visually see an individual when they are conducting themselves online. *Disassociation* is something we are far more familiar with and is typically labeled as pseudoanonymity where an individual uses a pseudonym or username for the basis of communicating instead of their real name. The lack of identifiability ensures that someone cannot distinguish one person's online activities communication from another person which is typically found when there is an option to post without a username (e.g. using a default "guest") (Morio and Buchholz, 2009). It is worth pointing out that these three levels of anonymity are not true anonymity from a computer scientist perspective. For the computer scientist, regardless if a person cannot be identified by the name they post under, each computer when connecting to the Internet is assigned a unique Internet Protocol (IP) address. Therefore, it becomes possible to link all communication and online activity back to the real identity through matching the data to the IP address, the IP address of the computer and then the computer to the individual. In this paper, we define anonymity to be a lack of identifiability by other Internet users and the inability to link information back to the individual's offline identity (Morio and Buchholz, 2009; Backes *et al.*, 2013). There are two types of Internet users that could desire online anonymity. Both the sender of the message and the recipient of the message could desire anonymity. The receiver is typically only applicable in situations that feature potential two-way communication such as email and instant messaging. In the case of sender and receiver anonymity, the concern is with indentifiability of the users while unlinkability is characterized by protecting the message path from potential attackers.

2.1 Motivations for online anonymity

An individual may wish to remain anonymous when conducting online communications and activities for various reasons. The main argument against online anonymity boils down to users having a lack of accountability (Craig, 2004). This means that anonymity can harbor criminal activity by making the tracing of online activities more difficult, which is the main concern to authoritative institutions. This has been

proven through the existence of black markets such as Silk Road (now Silk Road 3.0) (Nelson, 2014) and the ability to fund criminal enterprises/terrorist organizations. Anonymity also provides a shield to those engaging in behaviors like cyberbullying and flaming. While not illegal, these behaviors can still cause harm to other Internet users, and anonymity is believed to be a contributing factor to the rise of these activities (Hughes and Louw, 2013). However, there are also many other uses for online anonymity that justify the need for such an ability. Online anonymity has been known to give protection to whistleblowers, allow for the exchange of sensitive information (Kizza, 2013), facilitate political discussion for marginalized groups (Rodrigues, 2008), encourage self-disclosure (Hollenbaugh and Everett, 2013) and encourage the reporting of criminal acts (Craig, 2004).

2.2 Contributions of this work

We summarize the main research contributions of this work as follows:

- We identify, explain and analyze publicly available online anonymity technologies in terms of their usability.
- We identified ways as to how online anonymity technology can be improved to increase public adoption.
- We make pertinent recommendations on how the design and development of online anonymity technology can be improved in the future.

Remaining anonymous online is easier said than done. Unlike maintaining privacy online, anonymity can only be managed with the use of specialized technology. Online privacy relates more to protecting the information sent between parties and who has access to that information. Online privacy can be achieved while still having no anonymity, and an individual can also have no privacy but complete anonymity. This would be the case if a company gathered a complete profile on an individual but have no way of linking that profile back to the offline person. While a complete guarantee of online anonymity is not possible with today's technology, it is possible to remain anonymous online.

3. Enabling technologies for online anonymity

The technologies that offer the Internet user the protection of anonymity are numerous, and many of them share common features. Each available technology enables online anonymity by hiding the user's IP address. This can be accomplished in several different ways, some of which are more effective than others. Several of the technologies provide an additional layer of security by hiding the user's Web traffic in addition to the IP address, achieving complete anonymity according to our definition. We will discuss the various technologies used to achieve anonymity below. Many of these technologies include a broad range of anonymity enablers. We have selected a few specific online anonymity technologies based on the following criteria: the technology satisfies our full anonymity definition, the technology is currently available for public use and the technology has been academically researched. This ensures that the technology provides complete anonymity, has been verified as being secure and has been fully developed for individuals to use to achieve anonymity.

3.1 Anonymous remailers

An anonymous remailer is a way to send email while hiding the identity of the individual who sent the email. Anonymous remailers are a broad category of anonymity technology, and they do not all function the same way, even though the fundamental result is the same. From the user end, two main methodologies are associated with an anonymous remailer. From a technical standpoint, there are three methodologies (Jones, 2004; Gritzalis and Kyrloglou, 2001). From the user's perspective, the two types of remailers are Web based or software based. When operating a remailer through a Web page, the email is sent without the sender's information. A software-based remailer requires an application to be installed on the user's computer to receive the email from one sender, readdresses it and then sends it to another person (Gritzalis and Kyrloglou, 2001).

From a technical standpoint, anonymous remailers are based on the same basic methodology known as a Mix (as shown in Figure 1). A Mix uses a variety of sources to receive pieces of a message. This means that any user that is using this particular Mix will have his/her message sent to the same place as other users. After this step, the emails are decrypted and are then sent to their respective recipients (Jones, 2004). A Type 1 remailer is nothing different from the Mix described above. Due to the major security issues present in a Type I remailer, this technology only satisfies part of the anonymity definition. A Type I remailer does not protect against an attacker attributing a message back to a Mix user because the emails emerge from the Mix in the same order which they were received. In addition to this, an attacker can also gain some measure of information from the contents of the message by examining the message size (Jones, 2004). The ability for a Type I anonymous remailer to provide unlinkability to the sender is highly unlikely because of these flaws. Since the emergence of remailers, they have undergone two major improvements resulting in Types II and III remailers. Each of these types is based on the technology used in the first remailer. Type II remailers fix several potential security issues with Type I remailers by introducing message padding, message pools and reply blocks. Message padding assures that each message is the same length which helps to protect against attacks that use traffic analysis

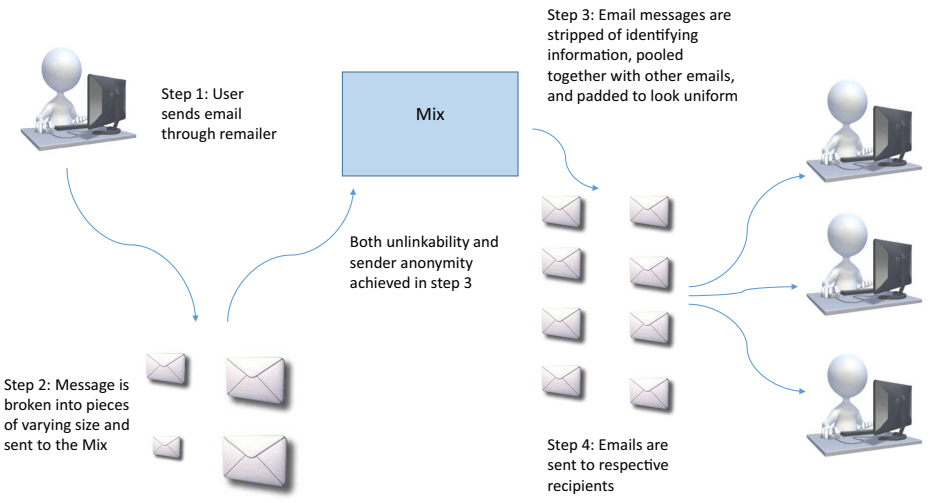


Figure 1.
Type II anonymous remailer

(Weiler, 2001). A Type II remailer does not send a message out immediately. Instead, it sends all messages received within a certain time period at the same time. The addition of message padding and message pools allows for this type of remailer to satisfy the condition of unlinkability in addition to sender anonymity. In addition, a Type II remailer also provides addition protection by including a reply block, a set of instructions that tells the receiver how to reply to the message, so that the sender's anonymity is protected (Jones, 2004). Type III remailers use all techniques used by Type II remailers with the support of Nym servers. Nym servers store virtual pseudonym reply block pairs that are sent with a message, and each reply block is used only once (Danezis *et al.*, 2003). This helps to ensure receiver anonymity because senders no longer have to send the email to the receiver's real email address (Jones, 2004). In this way a Type III remailer supports the highest level of anonymity. Both Types II and III remailers satisfy the full anonymity definition when subjected to basic attacks on a user's anonymity. Type I remailers fail to meet the unlinkability requirement when traffic analysis is taken into account and also fail to provide sender anonymity if the sender wishes a reply from the recipient of the anonymous email.

3.2 Rewebber

Rewebber is an anonymity technology that allows an individual to browse the Web anonymously. To ensure anonymity when browsing the Internet, rewebber uses an anonymizing HyperText Transfer Protocol (HTTP) proxy server. This server removes all potentially identifying information from a message (e.g. IP address) (Figure 2).

Some rewebbers now have the ability to handle additional tasks typically associated with Web browsing such as Uniform Resource Locator (URL) links embedded in Web pages. While these URL links would typically pose a risk on user anonymity, many rewebbers now have the ability to use a chain of anonymizing proxy servers. This chain works by removing information linking the request back to the original server, making it difficult to link the information request to the individual (Oppliger, 2005) (Figure 3).

Figure 2.
Information removed a message

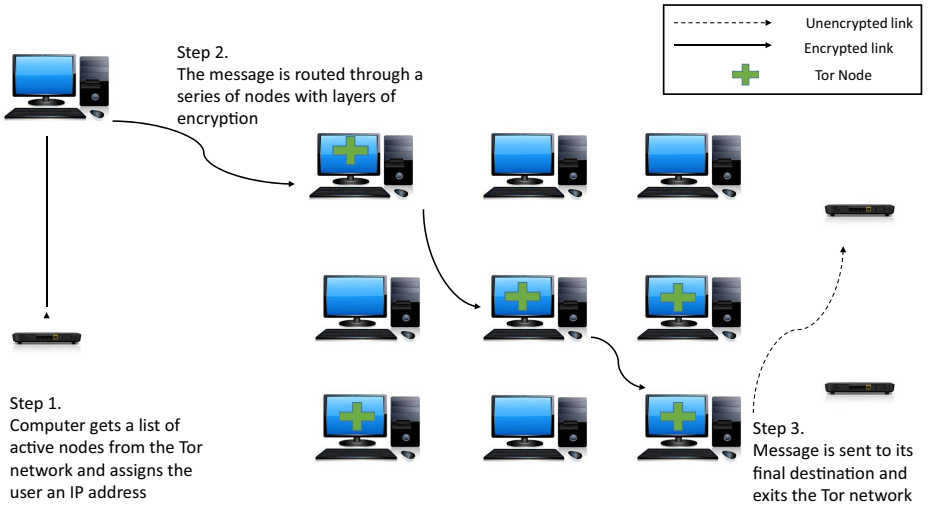
Figure 3.
Rewebber chain constructed using three rewebbers

A rewebber satisfies the first part of the anonymity definition when it strips the message of identifying information. However, it is questionable if rewebbers satisfy the unlinkability requirement of the anonymity definition. As rewebbers do not form a chain without the user taking the initiative, it could be relatively easy to trace the message back to a particular sender. Only by using multiple rewebbers can the message be considered truly anonymous using the definition established earlier in this paper.

3.3 Onion routing

Onion routing is a method that can provide anonymity in a variety of different contexts. This method of routing encrypts the path that the message takes from the sender to receiver so that the message cannot be linked to the participants. When a sender uses onion routing, the information packet is encrypted in layers, much like an onion. The first computer the message is routed to decrypts the first layer of encryption to discover the next destination of the message. Each router the message is routed through follows suit so that no one router knows the complete path of the message. Routers are only aware of the next routing destination, and the computer they received the message from (Hoang and Pishva, 2014; Sassone *et al.*, 2010). This satisfies the unlinkability condition in the anonymity definition (Figure 4).

The Onion Router (Tor) is the main technology that uses onion routing. Tor, in addition to onion routing, provides each user with a dummy IP address in place of the one assigned to the user's computer. This fulfills the unidentifiability condition of our anonymity definition. Tor currently has two main applications that provide anonymity to users: the Tor browser and an android smartphone application (Torbot) combined with the browser ("Software and services"). Tor can be downloaded for free as part of the Tor Project ("Tor"). Anyone with a minimal amount of computer knowledge can use Tor.



Source: Tor (2015)

Figure 4.
Onion routing

3.3.1 Garlic routing. Garlic routing is an extension of onion routing. This technique still routes messages through multiple nodes using layers of encryption with the added ability to transmit more than one message in the innermost encryption layer at a time (Ehlert, 2011). This separates the technology from Tor by including a return path with the original message which makes it an ideal medium for two-way anonymous communication. Specifically, this type of routing uses a pair of tunnels (an inbound and an outbound) for each user. Each user is not aware of the tunnels that are assigned to the other user (Timpanaro *et al.*, 2011). This type of routing provides a high level of protection inside the network itself; however, it does not allow for easy communication outside of the onion network. Unless a Web site or application is housed within the garlic routing network, it is not impossible for the user to access it when using garlic routing (Figure 5).

The Invisible Internet Project (I2P) uses garlic routing ("The invisible Internet project"). The main technology associated with this project is the software application that allows the user to connect to the I2P network which allows anonymous communication. I2P is still a relatively new technology in comparison to the other anonymity enablers discussed in this work. I2P is highly versatile compared to other anonymity enablers because its primary goal is to host a series of applications within the anonymity network. While this does not make it ideal for searching the clear Internet because of the lack of out proxies, it allows for the use of a host of other services anonymously (e.g. chat, email, publishing and file sharing). Similar to onion routing, garlic routing satisfies our anonymity definition because of the inherent design of the technology. However, I2P is better suited for the use of other Internet applications over Web browsing.

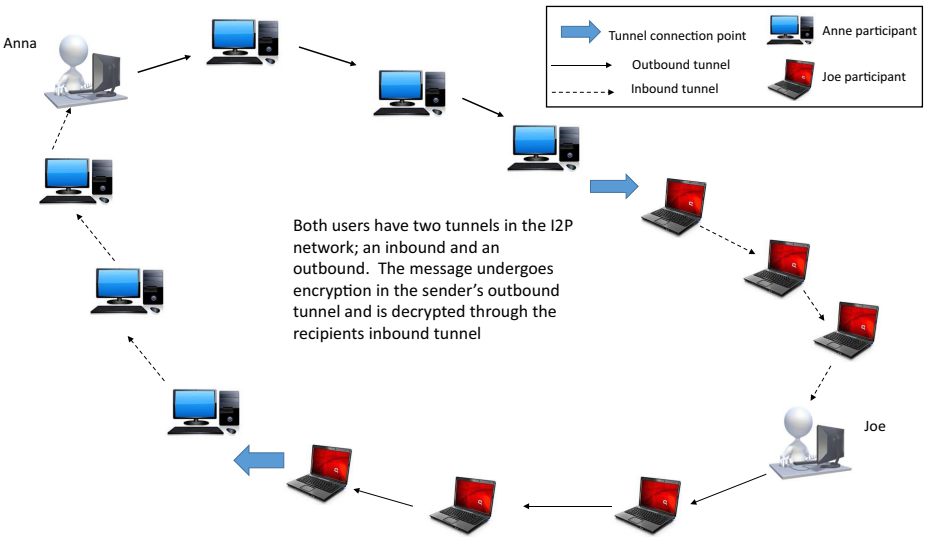


Figure 5.
Garlic routing tunnel system

Source: Timpanaro *et al.* (2011)

4. Evaluation of anonymity technologies

Each technology described in the previous section has its own weaknesses and strengths depending on what the user is looking for with the technology. We evaluate the anonymity technologies using the following criteria: level of protection, user friendliness, latency, monetary cost, versatility and the need for additional security protections:

- *Level of protection*: The level of protection the technology provides refers to how secure the technology is from cyber threats and attacks. No technology is completely infallible, each one has some weakness. Some of these weaknesses are easier to exploit than others. A technology can provide a high-, medium- or low level of security. A high level of protection means that the chance of the user's identity being discovered or the data linked back to them are low. A medium level of protection means that the technology protects the user from cyber attacks that have a moderate level of sophistication; however, the user would be vulnerable from highly sophisticated cyber attacks. The low level of protection classification is assigned to technologies that offer a minimal amount of protection to the user.
- *User-friendliness*: User-friendliness refers to how easy the technology is to use effectively. Each technology will be assigned a difficulty level of easy, moderate and difficult. A technology with an easy rating requires little to no computer skill to use correctly and effectively, while a technology assigned a difficult rating would require a high amount of computer knowledge to use the technology effectively.
- *Latency*: Latency refers to how long it takes the user to download the content of a Web page in a Web browser (Fabian *et al.*, 2010). Latency is typically a point of frustration for Internet users when operating online and can result in the cancellation of Web requests. Generally, anonymity technologies are separated into two latency categories: high latency and low latency (Oppliger, 2005; Edman and Yener, 2009). A technology that is assigned a high latency rating will have slow performance and may frequently time out when in use, whereas a technology with a low latency rating would operate at a quicker speed, and the user may notice relatively no difference in Internet activities.
- *Monetary cost*: The monetary cost refers to how much money the user would have to spend to gain access to and/or implement the technology. Some technologies are freely available while others need to be purchased.
- *Versatility*: The versatility of a technology refers to how many functions it can serve for the user. For example, a technology that has a high versatility rating could be used for numerous tasks (e.g. browsing, online purchases and email) and on different devices (e.g. laptop and smartphone). A technology with a low versatility rating would be capable of fewer functions in a user's life (e.g. a technology strictly used for email).
- *Need for additional security precautions*: The last area of evaluation for anonymity technologies is the need for additional security precautions. Most technology used for anonymity requires some sort of behavior change from the user in addition to using the technology for the maximum amount of protection. Some of these changes are fairly straightforward, such as refraining from giving out a large

about of information about oneself (Carmagnola *et al.*, 2013). Other precautions are less straightforward and require a conscious effort from the user such as not using peer-to-peer applications, accessing only Web sites that are secure, etc.

4.1 Anonymous remailers

Currently, there are numerous anonymous remailers available for public use. As such evaluating the specifics of this technology is problematic, as each remailer can vary in the level of protection it offers, user-friendliness, monetary cost, latency and the supplemental precautions needed. However, it is possible evaluate the technology as a whole and give a range for each criteria that a given anonymous remailer would be placed. Anonymous remailers can provide the user with a wide range of protection starting from a very low minimal level to a relatively high level. This is due mainly to the different types of the anonymous remailers listed in the previous section and the technological measures each takes to protect the user's identity.

Anonymous remailers are generally easy for the typical Internet user to use, as many of those available to the public consist of a simple online form that is filled out on a Web browser. This allows a user with even the most basic amount of skills to use this technology effectively. However, as demonstrated by the remailer Paranoia (Type II remailer), as the level of protection increases, the user-friendliness of the technology decreases ("Paranoia remailer"). Some anonymous remailers are available to Internet users free of charge, while others such as ultimate privacy require a monthly subscription to use the technology ("Ultimate privacy"). One of the potential problems with services that require a subscription to use is that the Internet user is required to disclose information to the service before ever being able to use the anonymity technology. This places a large amount of trust on the entities operating the technology that they will not share identifying information.

Remailers typically have one use, sending email anonymously. While this offers no versatility for potential users, it does make the need for quick response time nearly obsolete. This is good, as anonymous remailers fall into the category of high-latency anonymity technology which means that it could take up to a few days for the email to be sent. Generally, email is considered a task that is less time sensitive; however, in recent years, with introduction of the smart phone, Internet users have gotten used to nearly instantaneous speeds for electronic communications. As such, the high-latency aspect of anonymous remailers might be considered more problematic now than in the 1990s when they were originally launched (Weiler, 2001). Unlike other technologies that offer a high amount of versatility, anonymous remailers also require nearly no supplemental precautions. To remain anonymous, the user simply must be careful how much identifying information is disclosed to the email recipient.

4.2 Rewebber

Rewebbers are typically more difficult to find than anonymous remailers. The majority of the sites that at one time hosted rewebbers have been shut down or no longer have a working form of the technology available for use. After an exhaustive search for rewebbers, one result actually led to a functioning rewebber known as the Cloak ("the Cloak"). Generally, rewebbers provide a low level of user protection on their own. However, the user has the option to increase the amount of protection by using a

rewebber chain. A rewebber chain uses multiple rewebbers to access one Web site which makes the user more difficult to link to the visited Web site. A rewebber is used to access another rewebber, then another rewebber before accessing the desired Web site. A rewebber chain can be as long or as short as the user desires. The difficulty in this is that the user typically has to create the rewebber chain themselves which is difficult because of the lack of publically available rewebbers and the technical skill needed to implement such measures. When a user decides to utilize only one rewebber for Web browsing, the technology is fairly straightforward to use. For example, Cloak requires no download for an individual to use. The only requirement of the individual is to pick the filtering options (i.e. selection of the types of content are allowed to run on the specified Web page) and to type in the URL for the desired Web page to visit. The filtering options allow for additional protections because Java, Javascript, cookies and advertisements can pose threats to anonymity. The more filtering options the individual utilizes, the more protection the individual has.

As a whole rewebbers are considered to be a low-latency anonymity technology because of the need for a high server download speed, as there is generally a high expectation for low loading times during Web browsing (Oppliger, 2005). Even as a low-latency technology, there is a downside to using rewebbers. Each Web site must be typed in individually into the rewebber. A rewebber cannot be used to follow hyperlinks embedded in another Web page. A user has to invest a large amount of their time to use rewebbers to ensure anonymity while Web browsing. Each Web site that a user wants to access anonymously must be typed in individually into the rewebber to access the site, including any hyperlinks the user might want to use on that page. For example, to access Facebook, a user would first have to type in the Facebook URL. Once on the Facebook homepage, they would have to go back to the rewebber and type in the URL of any page they wanted to visit while on Facebook instead of clicking the direct link from the page. This limits the versatility of the technology because unless the user uses a rewebber chain, it is unlikely that search engines would be manageable using this technology while still protecting the user's identity. Cloak is available for Internet users free of charge; however, the possibility cannot be ruled out that other rewebbers exist that are a subscription-based service. As the Cloak's design includes filtering options to make Web browsing more secure, the user has to take few supplemental precautions to use the technology (i.e. not entering personal information into any site). Other rewebbers could be designed differently to where more supplemental precautions are necessary, but generally if the user confines himself/herself to Web browsing, only the need for supplemental precautions is minimal.

4.3 Tor

TOR is currently one of the best anonymity technologies publicly available (Hoang and Pishva, 2014) and has the largest anonymity network at this time (Ruiz-Martinez, 2012). Tor's main weakness lies at the exit node, which could be targeted by professional hackers (Hoang and Pishva, 2014). This is because the message has no more layers of encryption after this point, and the receiver of the message is revealed. Despite this weakness, Tor has been shown to hold up against a variety of cyber attacks (Backes *et al.*, 2013), enabling it to provide a high level of protection. Tor has many other advantages for use, including an easy to understand interface, low cost and a high amount of versatility. For an Internet user to use Tor for anonymity, the user only has to

download the correct software from their Web site, then install it on his/her computer. The Android application, Torbot, takes a little more effort to set up for it to work with multiple applications (e.g. Twitter), but the Web site details precise instructions complete with pictures and video of how to set up a smartphone for TOR use. This ensures that a user with only a basic level of computer knowledge would be able to make use of Tor.

The other two major advantages to using Tor is its low monetary cost and high versatility. Tor and all its associated software are completely free. This allows a high level of access to the software, which is beneficial, as the more users that Tor has, the more protection it can offer (Hoang and Pishva, 2014). As mentioned earlier, Tor has multiple applications as part of the project outside of its Web browser. While most technologies for anonymity can only provide protection on one platform, Tor can run on multiple platforms (e.g. PCs and mobile devices). Currently, the project has software for Android, desktop computers and even a portable software that can run from a USB on any desktop/laptop computer ("Software and services").

Tor has two major drawbacks: a fairly high level of latency and the need for supplemental protection. Like many technologies that use encryption, Tor suffers from a relatively high latency. Latency is the time it takes for a computer to display a Web page or load an application after the request has been made to access it. The level of latency that an Internet user is willing to tolerate is about 3 seconds (Everts, 2012). A delay that exceeds 4 seconds results in a fourth of the requests to be canceled by the Internet user (Everts, 2012). Currently, the majority of Tor requests are slower than direct requests for downloading Web pages with a latency of 16.99 seconds which leads to roughly an 88 per cent cancellation rate by users (Fabian *et al.*, 2010). Due to the high level of frustration that latency can cause, Tor might be a difficult tool to use on a regular basis for Internet activities. However, it is worth mentioning that while relative to technologies that provide no anonymity, Tor is high in latency, but compared to other anonymity technologies, Tor is considered to have low latency (Oppliger, 2005). The second disadvantage is something that will be found with any technology, the need to take supplemental precautions to protect anonymity. The technology alone cannot protect the user unless the users were to change some of their own habits. With Tor, any use of Java, peer-to-peer torrenting or a non-secure site can increase the likelihood of an adversary discovering the user's identity.

4.4 Invisible Internet Project (I2P)

I2P is an extension of onion routing, and as such, it has many of the security features that Tor has including layered encryption. The developers of I2P also used what was learned from security attacks (Sybil and Eclipse attacks) on Tor to defend against future attacks (Egger *et al.*, 2013; Timpanaro *et al.*, 2011). I2P also has some security benefits by design because it does not depend on a central location for communication, as the architecture is highly distributed and decentralized. Each I2P user creates its own tunnels for anonymous communication. This distribution alleviates the need for the user to be completely dependent upon one technology for his/her anonymity. In the I2P network, it is far more difficult for an attacker to deanonymize a large amount of users at once, as each individual user creates his/her own tunnels instead of being routed through a central location. I2P for now can only provide a medium level of security given that the technology is fairly new. Despite the various studies that have tested I2P against various cyber attacks (Herrmann and Grothof,

2011; Egger *et al.*, 2013), the technology is largely untested when compared to onion-routing based networks such as TOR.

Although I2P is still new it shows great promise in terms of its high versatility. This is a direct result behind the development of I2P: providing a method for other applications to be housed and run inside the anonymous network (Timpanaro *et al.*, 2011). This goal allows users to engage in activities such as file sharing/torrenting, instant messaging, email, and Web development from their own Internet browser. The drawback is that to freely engage in these activities without the need of additional security precautions (like Tor allows) is that the technology is not suitable for regular Web browsing. This is because of the lack of outproxies in the network. Outproxies allow a user to access any Web site or application that is not housed inside the anonymity network. I2P has less than five outproxies which substantially increases latency when accessing Web sites and applications outside of the network. Tor incurs roughly a 17 second latency for complete Web pages display. In contrast with I2P the latency incurred is 103.19 seconds (almost a six-fold increase) (Ehlert, 2011).

A unique strength of I2P is its customizability. This particular technology can be executed on a user's own Web browser, the applications and plugins available on the start page can be changed, and the user has the ability to monitor the use of bandwidth, and alter other functions of the technology for their own use.

The high amount of customizability comes at the cost of user-friendliness. I2P is not an easy technology to set up for the average computer user because it typically requires a more advanced knowledge of computer system capabilities and Internet settings to properly configure the technology for particular computer and Internet speed. After downloading the software from I2P, the user must set up their Internet browser to connect to a proxy server. Once the connection to the I2P network has been established the user accesses the network the same way that he/she would typically access the Internet; starting the Web browser (e.g. Chrome, Firefox, Internet Explorer) they typically use. Herein lies the next difficulty, as long as the Internet preferences are set to connect to the proxy server, it is not possible to browse the Internet outside of the I2P network. Simply shutting down the I2P connection is not enough, the user must change the Internet options and disable the proxy server connection.

As we stated earlier I2P is also considered to be more of a high-latency network than other onion-routing based technologies and therefore the user is advised against using it for applications such as streaming and Web browsing due to the potentially long response times (Ehlert, 2011; Timpanaro *et al.*, 2011). Currently the software is available for free and it is constantly undergoing development. Right now I2P may not be best choice to use for anonymity for the average computer user, but this could easily change in the future as the technology becomes more user-friendly.

We summarize the evaluation of the various anonymity technologies discussed in this work using the criteria above in Table I.

5. Discussion: challenges and limitations of online anonymity technologies

The development of anonymity technology has been ongoing before the Internet was available for public use. This development started with David Chaum's research in (1981) on Web mixes, which laid the foundation for anonymous remailers

(Chaum, 1981). Despite the long history that anonymity technologies have, there are only a few technologies that have been fully developed to the point that they can be used by members of the public. Many technologies that are researched academically never make it passed the theoretical stage (e.g. Crowds [Jing *et al.*, 2010]; [Gritzalis and Kyrloglou, 2001]; [Gritzalis, and Kyrloglou, 2001). Other technologies have been developed and then later abandoned as new technologies emerged (Li *et al.*, 2013). Mixminion, the piloted type III anonymous remailer, as of 2013 is no longer in active development (Matthewson, 2013). Remailers are no longer seen as practical for continued use for anonymity, at a time where it is nearly impossible to send an email to someone that is private, let alone anonymous.

5.1 Economics

One of the reasons why there are so few anonymity technologies could be due to the cost of developing these technologies for public use. Anonymity technologies cost money to develop, run, and maintain. However, many eventual users of the technology are unwilling to pay for the services (Acquisti *et al.*, 2003). By paying for the service the user is forced to reveal their identity to the entity running and maintaining the software which requires a large amount of trust from the user that this entity is in no way malicious. The unlikelihood of achieving some sort of monetary gain from these technologies discourages investment of them outside of the research phase. There is a potential solution to this problem that could help spur further development past the research phase. One such solution is to make the software open source.

The two strongest online anonymity technologies that are currently available (Tor and I2P) to users are considered to be open source projects which allow anyone who desires to help improve the technology to access the source code, make changes, and submit the modified/enhanced code back to the organization (Corbly, 2014). By making the technology open source it is possible for the technology to develop quickly and helps to ensure the technology will remain free to use. However, once a technology has made the jump to an open source economic model it is impossible to go back to wanting potential users to pay for the technology (Kort and Zaccour, 2011). If a company wants to profit from the technology, it would be easy for copycat technologies to pop up independently since the source code is readily available. Making a technology open source can be helpful, but only solves the problem of development. In most cases a source of funding is still needed to implement the technology and run routine maintenance. More research is needed to discover other alternatives for funding anonymity technology other than a for-profit business model.

Table I. Evaluation of anonymity technologies

Technology	Level of protection	User-friendliness	Monetary cost	Latency	Versatility	Supplemental protections
Anonymous remailer	Varies	Varies	Varies	High	Low	Few
Rewebber	Medium	Easy	Varies	Low	Low	Few
Tor	High	Easy	Free	Low	Medium	Numerous
I2P	Medium	Medium	Free	Medium	High	Few

5.2 User-friendliness

Currently, while many scholars, activists, and technology experts have agreed that there is a need for online anonymity, the anonymity technology does not have widespread use (Li *et al.*, 2013). Tor currently has 2.5 million daily users worldwide and has been labeled as the most popular anonymity technology to date (Parliamentary Office of Science and Technology, 2015). However, in the grand scheme of things the number of individuals using Tor pales in comparison to how many daily users Facebook has which is currently estimated to be about 70 per cent of Facebook's 6 billion users (Duggan *et al.*, 2015). The people using the technology are those who typically have a concern about privacy issues and have technological skills beyond those of the average Internet user. As a whole anonymity technology is not easy to use. Even after installing the software users must change many Internet habits that are not always intuitive even with the simplest of technologies. For instance some of these technologies require the Internet user to change the settings on their computer. A typical user is looking for something easy to use that does not require many habits to be altered. A possible model to look towards is something closer to Google Incognito (Whitten, 2012), which is a form of private browsing offered by the Chrome browser. All a user has to do to use this technology is to click a button, and it is done. The browser takes care of the rest without the user ever having to think back. Something this simple would be more likely to gain a larger amount of users.

5.3 Web integration

Simply making the technology more user friendly will still not make the technology attractive for daily use for many Internet users. There is a second problem associated with the integration and compatibility of the technology with popular Web sites. Many popular sites that users frequent online have barriers that make it difficult to use anonymity technology, sometimes to the point of treating the users like criminals. One of the most basic issues is the slow adoption of HTTP secure (HTTPS) by many companies and organizations including the government. HTTPS is necessary for Tor to be completely secure and many times Tor will warn the user when visiting a site that does not use HTTPS that their identity could be compromised. The more concerning problem is found on social media sites which can be illustrated best by examining what happens when a Tor user decides to log into his/her account. One of Facebook's security features is to match a user's IP address to his/her account to minimize potential unauthorized access. This becomes problematic when using Tor because this technology automatically changes the individual's IP address when accessing the network. When logging into one's Facebook account the user is immediately greeted with a message stating that the device being used cannot be recognized and requests that the user identifies photographs of friends to verify his/her identity. This process can demonize Tor users and also potentially compromise the user's identity. Before anonymity technology can gain wide acceptance with mainstream Internet users, popular Web sites need to adopt different security measures such as Personal Identification Numbers (PINs) to check for unauthorized users which are commonly used on Tor based Web sites. Further research should focus on approaches to integrate the use of anonymity technology into the daily Internet use of the average individual as well as ways current Web sites can be adapted to allow the use of such technology while still protecting users and their business model.

As Internet technology becomes more advanced, so does the surveillance of online activities. However, it is interesting to note that many of the technologies available to manage online privacy started development over a decade ago, before a lot of the Internet surveillance was made public knowledge. While the concern about online anonymity has increased, the technology that offers the strongest amount of protection to Internet users has slowed down in development. This concerning trend merits further investigation because it is doubtful that economics alone is the sole cause of the decrease when societies that are less capitalistic in nature would not be as concerned with monetary gain.

6. Conclusion

In recent years, Internet anonymity and privacy have become more important with the increase of corporate tracking and the revealing of large surveillance programs implemented by agencies such as the National Security Agency in the USA. We reviewed the current online anonymity technologies that users have at their disposal to maintain their anonymity during their online activities. We have reviewed each of these technologies by focusing on the level of security provided and the ease with which an individual could use these technologies on a regular basis using criteria such as user friendliness, monetary cost and versatility. Anonymity technology is under constant development, and with the increased concern over how data are retrieved and managed by third parties in the future, there is likely to be an increase in the sophistication of the technologies available. Further research is still needed to help determine what the average user wants to see in an anonymity technology as well as ways to help users integrate the technology into their commodity software (such as Web browsers). Future online anonymity technologies should enable the user to decide when, how and with whom their information is shared if it is shared at all with ease and simplicity.

References

Acquisti, A., Dingledine, R. and Syverson, P. (2003), "On the economics of anonymity", *7th International Conference on Financial Cryptography*, Guadeloupe, 27-30 January, pp. 84-102.

Adam, R. (1991), "Laws for the lawless: ethics in (information) science", *Journal of Information Science*. Vol. 17 No. 6, pp. 357-372.

Anthes, G. (2015), "Data brokers are watching you", *Communications of the AMC*, Vol. 58 No. 1, pp. 28-30.

Backes, M., Kate, A., Manoharan, P., Meiser, S. and Mohammadi, E. (2013), "ANOA: a framework for analyzing anonymous communication protocols unified definitions and analysis of anonymity properties", *IEEE 26th Computer Security Foundations Symposium (CSF)*, New Orleans, LA, 26-28 June, pp. 163-178.

Beato, F., Cristofaro, E.D. and Rasmussen, K.B. (2014), "Undetectable communication: the online social networks case", *2014 Twelfth Annual Conference on Privacy, Security, and Trust (PST)*, Toronto, ON, 23-24 July, pp. 19-26.

Carmagnola, F., Osborne, F. and Torre, I. (2013), "Escaping big brother: an empirical study on factors influencing identification and information leakage on the web", *Journal of Information Science*, Vol. 40 No. 2, pp. 180-197.

Chaum, D. (1981), "Untraceable electronic mail, return addresses, and digital pseudonyms", *Communications of the ACM*, Vol. 24 No. 2, pp. 84-90.

Chen, S.Y. and Liu, X. (2004), "The contribution of data mining to information science", *The Journal of Information Science*, Vol. 30 No. 6, pp. 550-558.

Corbly, J. (2014), "The free software alternative: freeware, open-source software, and libraries", *Information Technology & Libraries*, Vol. 33, pp. 65-75.

Craig, S.R. (2004), "Benefits and drawbacks of anonymous online communication: legal challenges and communicative recommendations", *Free Speech Yearbook*, Vol. 41 No. 1, pp. 127-141.

Danezis, G., Dingledine, R. and Mathewson, N. (2003), "Mixminion: design of a type III anonymous remailer protocol", *Proceedings, 2003 Symposium on Security and Privacy, 11-14 May, IEEE*, pp. 2-15.

Duggan, M., Ellison, N.B., Lampe, C., Lenhart, A. and Madden, M. (2015), "Social media update 2014", available at: www.pewinternet.org/2015/01/09/frequency-of-social-media-use-2/ (accessed 23 August 2015).

Edman, M. and Yener, B. (2009), "On anonymity in an electronic society: a survey of anonymous communication systems", *ACM Computing Surveys*, Vol. 42 No. 1, pp. 5-535.

Egger, C., Schlumberger, J., Kruegel, C. and Vigna, G. (2013), "Practical attacks against the i2p network", *16th International Symposium on Research in Attacks Intrusions and Defense (RAID)*, Rodney Bay, St. Lucia, 23-25 October, pp. 432-451.

Ehlert, M. (2011), "I2p usability vs tor usability a bandwidth and latency comparison", Seminar conducted at Humboldt University of Berlin, Berlin, available at: http://userpage.fu-berlin.de/~semu/docs/2011_seminar_ehlert_i2p.pdf (accessed 23 August 2015).

Everts, T. (2012), "Our need for web speed: it's about neuroscience, not entitlement", *Web Performance Today*, available at: www.webperformancetoday.com/2012/03/21/neuroscience-page-speed-web-performance/ (accessed 23 August 2015).

Fabian, B., Goertz, F., Kunz, S., Müller, S. and Nitzsche, M. (2010), "Privately waiting-A usability analysis of the tor anonymity network", *16th Americas Conference on Information Systems, AMCIS 2010*, Berlin, 12-15 August, pp. 63-75.

Gritzalis, D. and Kyrloglou, N. (2001), "Consumer online privacy and anonymity protection using infomediary schemes", *Computer Science Society*, pp. 115-123.

Herrmann, M. and Grothof, C. (2011), "Privacy-implications of performance-based peer selection by onion-routers: a real-world case study using i2p", *11th International Symposium, PETS 2011*, Waterloo, ON, 27-29 July, pp. 155-174.

Hoang, N.P. and Pishva, D. (2014), "Anonymous communication and its importance in social networking", *16th International Conference on Advanced Communication Technology, Korea, 16-19 February*, pp. 34-39.

Hollenbaugh, E.E. and Everett, M.K. (2013), "The effects of anonymity on self-disclosure in blogs: an application of the online disinhibition effect", *The Journal of Computer-Mediated Communication*, Vol. 18 No. 3, pp. 283-302.

Hughes, M. and Louw, J. (2013), "Playing games: the salience of social cues and group norms in eliciting aggressive behavior", *South African Journal of Psychology*, Vol. 43 No. 2, pp. 252-262.

Jing, X., Zhenxing, W., Liancheng, Z. and Qian, W. (2010), "Recipient anonymity: an improved crowds protocol based on key sharing", *2010 WASE International Conference on Information Engineering*, Beidaihe, Hebei, 14-15 August, pp. 60-64.

Jones, A. (2004), "Anonymous communication on the internet", paper presented at WWW@10: The Dream and the Reality, Terre Haute, IN, 17 September, available at: www10.csse.rose-hulman.edu/Papers/Jones.pdf (accessed 23 August 2015).

Kizza, J.M. (2013), "Anonymity, security, privacy, and civil liberties", *Ethical and Social Issues in the Information Age*, Springer, London, pp. 75-96.

Kort, P.M. and Zaccour, G. (2011), "When should a firm open its source code: a strategic analysis", *Production & Operations Management*, Vol. 20 No. 6, pp. 877-888.

Li, B., Erdina, E., Gunes, M.H., Bebis, G. and Shipley, T. (2013), "An overview of anonymity technology usage", *Computer Communications*, Vol. 36 No. 12, pp. 1269-1283.

Matthewson, N. (2013), "Mixminion: a type III anonymous remailer", available at: http://mixminion.net/ (accessed 23 August 2015).

Mayer, J. (2011), "Tracking the trackers: early results", available at: http://cyberlaw.stanford.edu/blog/2011/07/tracking-trackers-early-results (accessed 23 August 2015).

Morio, H. and Buchholz, C. (2009), "How anonymous are you online? Examining online social behaviors from a cross-cultural perspective", *AI & Society*, Vol. 23 No. 2, pp. 297-307.

Nelson, S. (2014), "Silk road 3.0 opens for business", *US News & World Report*, available at: www.usnews.com/news/articles/2014/11/07/silk-road-30-opens-for-business (accessed 23 August 2015).

Nunan, D. and Domenico, M.D. (2013), "Market research and the ethics of big data", *International Journal of Market Research*, Vol. 55 No. 4, pp. 2-13.

Oppliger, R. (2005), "Privacy-enhancing technologies for the world wide web", *Computer Communications*, Vol. 28 No. 16, pp. 1791-1797.

"Paranoia remailer", available at: http://remailer.paranoici.org/howto.php (accessed 23 August 2015).

Parliamentary Office of Science and Technology (2015), "The darknet and online anonymity", Post Note No. 488, available at: www.scribd.com/doc/258187467/UK-Briefing-on-Tor#scribd (accessed 23 August 2015).

Rodrigues, R. (2008), "Digital identity and anonymity", *Proceedings of the Third IFIP International Federation for Information Processing on the Future of Identity in the Information Age Society, Karlstad University, Karlstad, 4-10 August*, pp. 359-374.

Ruiz-Martinez, A. (2012), "A survey on solutions and main free tools for privacy enhancing web communications", *Journal of Network and Computer Applications*, Vol. 35 No. 5, pp. 1473-1492.

Sassone, V., Hamadou, S. and Yang, M. (2010), "Trust in anonymity networks", *21st International Conference, CONCUR 2010*, Paris, 31 August-*3* September, pp. 48-70.

"Software and services", available at: www.torproject.org/projects/projects.html.en (accessed 23 August 2015).

"The cloak" available at: www.the-cloak.com/anonymous-surfing-home.html (accessed 23 August 2015).

"The invisible internet project", available at: https://geti2p.net/en/ (accessed 23 August 2015).

Timpanaro, J.P., Isabelle, C. and Olivier, F. (2011), "Monitoring the i2p network Report No", RR-7844, available at: HAL-Inria website: https://hal.inria.fr/hal-00653136/document (accessed 23 August 2015).

"Tor", available at: www.torproject.org/ (accessed 23 August 2015).

"Ultimate privacy", available at: https://ultimate-anonymity.com/signup.htm (accessed 23 August 2015).

Weber, R.H. and Henrich, U.I. (2012), "Anonymity challenges in the internet", in *Anonymization, Springer Briefs in Cybersecurity*, Springer, London, pp. 11-21.

Weiler, N. (2001), "Secure anonymous group infrastructure for common and future internet applications", *17th Annual Computer Security Applications Conference*, New Orleans, LA, 10-14 December, pp. 401-410.

Whitten, A. (2012), "We protect your data", *USA Today*, available at: http://usatoday30.usatoday.com/news/opinion/editorials/story/2012-04-03/Alma-Whitten-Google-privacy/53966770/1 (accessed 23 August 2015).

Further reading

Venkateswaran, R. (2001), "Virtual private networks", *IEEE Potentials*, Vol. 20 No. 1, pp. 11-15.

Corresponding author

Sherali Zeadally can be contacted at: szeadally@uky.edu