A Taxonomy of Censors and Anti-Censors Part II:
Anti-Censorship Technologies

Christopher S. Leberknight, Department of Computer Science, William Paterson University, Wayne, NJ, USA

Mung Chiang, Department of Electrical Engineering, Princeton University, Princeton, NJ, USA

Felix Ming Fai Wong, Department of Electrical Engineering, Princeton University, Princeton, NJ, USA

ABSTRACT

This paper presents a conceptual study of Internet anti-censorship technologies. It begins with an overview of previous research on Internet anti-censorship systems and discusses their social, political and technological dimensions. Then for deployed Internet anti-censorship technologies, a taxonomy of their principles and techniques is presented, followed by a discussion of observed trends and implications. Based on the observations, the paper concludes with a discussion on the most critical design features to enable a successful and effective system.

Keywords: *Anti-Censorship, Circumvention Technology, Filtering, Internet Censorship, Taxonomy*

1. INTRODUCTION

The evolution of Internet censorship and anti-censorship technologies is an endless arms race: Internet users constantly apply new methods to circumvent blocks and filters imposed by online censors, and censors constantly update their deployed systems in response. With the ever-increasing speeds and capabilities of computers, one can only expect this arms race to be more dynamic. This paper is a sequel to the authors' previous paper on Internet censorship (Leberknight et al., 2012). One of the main objectives of this research is to advance the state of the art of circumvention technologies, by stimulating discussion on the directions and development of these systems.

Circumvention is approached in mainly three directions. The first is *anonymity*, which is to allow users to communicate undetected in a censored network. The second is *content protection*, which is to protect a communication channel from being attacked by censors. The last direction is *content filtering* or *detection evasion*, which is to evade detection even when message contents can be directly monitored. A successful system should exploit simultane-

DOI: jep.2012100102

ously a censorship system's vulnerabilities from the social, political and technological dimensions.

A main contribution of this conceptual paper is a taxonomy of Internet anti-censorship technologies. The taxonomy is presented at three levels of detail. At the *principles* level the paper presents a list of criteria for a system to be successful. At the *techniques* level these systems attempt to defeat blocking according IP addresses, URLs, or message contents. It is found that these systems usually implement some form of forwarding, with the help of computers located geographically outside a censorship system. Finally, at the *technologies* level the paper studies the available systems individually. Specifically, the systems are tabulated to show which techniques they apply, and the times of deployment of various censorship and anti-censorship technologies are visualized in a timeline. A number of interesting implications can be drawn from the taxonomy.

Even if an anti-censorship system is theoretically sound, it will not succeed if end-users refuse to adopt it for usability issues, or even worse, refuse to try it if they *perceive* it to be untrustworthy in terms of anonymity, content protection, or detection evasion. To address this, the paper discusses the most important design features to enable a successful and effective system. Trust is an important factor, both in terms of a user's social network (from which a new anti-censorship technology is learnt), and the technology itself (whether it is reliable and financially sustainable). A somewhat surprising fact that simpler and faster technologies are more popular suggests that performance is often a more dominant factor than trust.

2. PREVIOUS RESEARCH

Extant literature on circumvention technologies discusses several techniques and strategies for designing censorship resistant systems. There are two main dimensions: free *access* to information and free *publication* of information, the second being even more challenging than the first.

A key component for any censorship resistant system or circumvention technology is to ensure *privacy* by enabling users to communicate undetected in a censorship network. This is often accomplished by incorporating certain techniques such pseudonymity and anonymity into the system. However, previous research suggests that current techniques to ensure privacy still reveal a significant amount of identifying information (Rao & Rohatgi, 2000). Rao and Rohatgi (2000) indicate that techniques from linguistics and stylometry can use the identifying information to compromise pseudonymity. They suggest some countermeasures to address syntactic and semantic leaks of information. With respect syntactic leaks the authors suggest using a thesaurus tool, which could prompt the user to use alternatives while composing messages thereby reducing variations in vocabulary. For semantic leaks, they suggest translating the message to another language and then back again to the original language (Rao & Rohatgi, 2000).

In addition to addressing the limitations for ensuring privacy using tools, other research has introduces four properties: anonymity, unlinkability, unobservability, and pseudonymity, and a set of anonymity metrics, which can be used to improve the design and evaluation of censorship resistant systems (Danezis & Diaz, 2008). Expanding on research which has introduced tools, properties and metrics for ensuring privacy and specific applications to censorship resistant systems, privacy via anonymity has also been explored by investigating the limitation of different *network topologies and document storage techniques*. Due to the single point of failure or ability to conduct denial of service attacks on centralized designs, network topologies such as peer-to-peer approaches for addressing anonymity have been suggested. One example is a peer-to-peer protocol that guaran-

tees both anonymity and censorship resistance in semantic overlay networks (Backes et al., 2009). Other literature describing peer-to-peer methods document storage techniques for protecting access and publication of documents have also been investigated. For example Serjantov (2002) discusses a peer-to-peer architecture for a censorship resistant system with user, server and active-server document anonymity as well as efficient document retrieval. In addition, research by Waldman and Mazieres (2001) introduce a unique document storage mechanism known as entanglement in which newly published documents are dependent on the blocks of previously published documents.

So far the analysis of previous research has identified two main challenges for designing censorship resistant systems. These challenges include research focused on content protection and anonymity to ensure privacy. Other research has proposed novel *routing protocols* to address these two main challenges. An example of such research was conducted by Katti et al. (2005). Their research presented a protocol that uses a combination of information slicing and source routing to provide anonymous communication similar to Onion Routing but without a public key infrastructure (Katti, Katabi, & Puchala, 2005). Subsequently, a paper by Sovran et al. (2008) presents a peer-to-peer system of relays which enables users within a censored domain to access blocked content using restricted service discovery (Sovran, Libonati, & Li, 2008). Recently proposed systems include Telex (Wustrow et al., 2011) and Cirripede (Houmansadr et al., 2011) which employ a form of obfuscation known as decoy routing (Karlin et al., 2011). The main idea of decoy routing is implement circumvention at the router as opposed to a host or server since IP packets do not contain router IP addresses they are more difficult to filter. The client establishes a connection to an overt destination that traverses the Internet for a router that supports decoy routing. The overt destination redirects communication to the covert destination and due to the difficulty of filtering router traffic the censor does not detect malicious or suspicious communication with the covert destination. Vasserman, Jansen, Tyra, Hopper and Kim (2009) propose the concept of membership-concealment as the goal of preventing censors from identifying anti-censorship network participants while retaining robustness and efficiency. Flash proxies achieve this by providing a way to dynamically create a large number of short-lived proxies (Fifield et al., 2012). To address the issue of censors blocking the traffic of anonymous routing protocols altogether, research in protocol obfuscation aims to make anonymous traffic mimic innocuous-looking traffic, such as HTTP (Weinberg et al., 2012) and Skype (Moghaddam, Li, Derakhshani, & Goldberg, 2012).

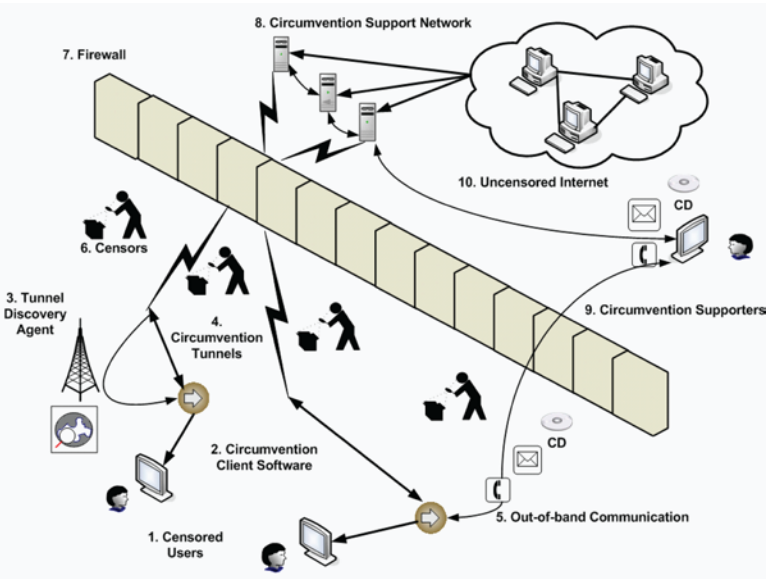
In addition to content protection and anonymity other approaches for designing censorship resistant systems have centered on issues related to *content filtering*. For example, previous research has proposed a variation of censorship resistance (CR) that is resistant to selective filtering even by a censor who is able to inspect (but not alter) the internal contents and computations of each data server, excluding only the server's private signature key (Perng, Reiter, & Wang, 2005). Further examples of research involving content filtering include a paper by Wolfgarten (2005). Wolfgarten (2005) analyzes large-scale, countrywide Internet content filtering and discusses techniques to effectively defeat censorship based on results from several tests. In addition, Crandall et al. (2007) presents an architecture for maintaining a censorship "weather report" for determining which keywords are filtered over time (Crandall et al., 2007). Subsequently, a recent study by Park et al. (2010) provides results from measurements based on filtering HTTP HTML responses in China. Their results suggest that the distributed nature of the Chinese filtering system and the problems inherent to distributed filtering are likely among the reasons it was discontinued, in addition to potential traffic load problems (Park & Crandall, 2010).

In summary, the main technical approaches for addressing challenges with designing censorship resistant systems include: (1) anonymity,

(2) content protection, and (3) content filtering. In addition to the technical approaches and research on censorship resistant systems discussed above, several *social and behavioral methods* have also been investigated. For example, the first economic model of censorship resistance based on conflict theory and node preferences in a peer-to-peer system was presented by Danezis and Anderson (2004). Their model assessed how two different design philosophies (random and discretionary distribution of resources) resist censorship. The main finding was that, under the assumptions of their model, discretionary distribution is better. The more heterogeneous the preferences are, the more it outperforms random distribution. Pachinko and Pimenidis (2007) also explore social and behavioral methods to address challenges with designing effective censorship resistant systems. In their research they define a model of a censorship resistant system based on a trusted directory. It is used in order to prolong contacts among peers based on their reputation in a way, that honest members get contacts only to other honest peers and colluded members remain isolated.

As surveyed above, many different approaches to design censorship resistant systems have been proposed. The approaches so far have consisted of possible solutions from both technical and social perspectives. However, after a thorough analysis of previous research no single approach has proposed a solution which synthesizes both perspectives. As illustrated in Figure 1 (Leberknight et al., 2012), a comprehensive and successful Internet censorship strategy involves collaboration and coordination among various social, political and technological entities. Correspondingly, a solution to Internet censorship must attempt to exploit the vulnerabilities within each entity. A solution to Internet censorship may evolve from a technological perspective provided it is designed with the optimal combination of features including an underlying or indirect motive to destabilize social and political structures. An important step in the direction to develop new circumvention technologies is to understand

Figure 1. Anti-censorship system (Global Internet Freedom Consortium, 2007)



the fundamental limits with existing censorship systems by presenting a classification of technological design criteria. The rest of this paper will present our taxonomy Internet and anti-censorship systems followed by a discussion of critical design features, concluding remarks, and future research directions.

3. ANTI-CENSORSHIP TAXONOMY

3.1. Principles

The primary objective of an anti-censorship system is to connect censored users to the uncensored Internet securely and anonymously. This can be accomplished by adopting one of the two anti-censorship principles:

1. Make it too costly to censor;
2. Lead in the technology evolution.

There are essentially four approaches to anti-censorship:

1. Volume-based;
2. Speed-based;
3. Covert channel-based;
4. New technology-based.

Similar to the eight criteria for censorship (Leberknight et al., 2012), there are seven critical design features for anti-censorship: SPASDUV:

1. **Security:** This is the most obvious dimension of an anti-censor;
2. **Performance:** How much will throughput and delay be degraded by using the anti-censor?
3. **Availability:** There is no use of an anti-censorship technology if the target users cannot access it;
4. **Scope:** How many modes of communication can be covered?
5. **Deniability:** If caught, how can a user deny her involvement?
6. **User-friendliness:** An often under-explored dimension, given the large population of users who are not technology-savvy;
7. **Verifiability:** How can a user verify that the software is not a monitoring tool from the government?

These metrics trade-off against each other, and the analysis and comparison of anti-censorship techniques can be carried out in the tradeoff space, e.g., scope-deniability vs. performance-availability or user-friendliness vs. deniability.

A typical anti-censorship system is comprised of many components working together (Global Internet Freedom Consortium, 2007). Conceptually, a censorship network can be viewed as a set of filters or a firewall and possibly coupled with manual processes which restrict users from accessing or publishing certain content. Figure 1 provides an illustration of the typical components comprising an anti-censorship system. The process to circumvent the censors can involve several steps as follows: censored users (1) use circumvention client software (2) on their computers to connect to circumvention tunnels (4), usually with the help of a tunnel discovery agent (3). Once connected to a circumvention tunnel, a user's network traffic will be encrypted by the tunnels and penetrate the firewall (7) without being detected by the censors (6). On the other side of the firewall, the network traffic will enter a circumvention support network (8) set up and operated by anti-censorship supporters (9). The computers, sometimes called nodes, in the circumvention support network act as proxies to access content from the unobstructed Internet (10) and send the information back, not necessarily taking the same route, to the censored user's computer (Global Internet Freedom Consortium, 2007). Initially, if a censored user knows nothing about the other side of the firewall, it is necessary to get them boot-strapped by employing

out-of-band communication channels (5). Such channels include emails, telephone calls, instant messages, and mailing of CD-ROMs. Sometime users can also take advantage of these channels to locate circumvention tunnels (4), if the client software in use does not have a tunnel discovery agent (3) (Global Internet Freedom Consortium, 2007). The key component in the overall system which facilitates covert communication within the censor network is primarily based on the software or tools and the underlying circumvention methodology.

3.2. Techniques

It has widely been reported that China has the most advanced censor network (Clayton, Murdoch, & Watson, 2007; Global Internet Freedom Consortium, 2007; MacKinnon, 2008; OpenNet Initiative, 2005; Palfrey et al., 2009). Consequently, the majority of research on Internet censorship including the evaluation of circumvention technologies has been investigated by analyzing various aspects of the censorship network controlled by the Chinese government. Due to the threat of diffusion and adoption of Chinese Internet censorship technologies and policies by less technologically-advanced regimes, it is useful that the subsequent discussions focus on online censorship in China in an attempt to hasten and undermine free thought and freedom of expression.

The most common type of online content blocking strategies in China consist of IP address blocking, DNS Hijacking, and Content Filtering, such as keyword or URL blocking (Clayton et al., 2007; Global Internet Freedom Consortium, 2007; Palfrey et al., 2009). IP address blocking operates by restricting users from accessing content by blocking the IP address where the content is hosted. IP blocking has the undesirable effect of over blocking since many sites can be hosted on a single IP address. Blocking the IP address of the site which contains "objectionable" content will also block all other sites on the same IP address which may not contain "objectionable" content.

DNS hijacking is finer grained compared to IP blocking, but it still is susceptible to over blocking. DNS hijacking allows operators to block access to content by blocking the name of the site instead of the IP address. For example, DNS hijacking would block or redirect users to another site when they tried to access http://www.google.com. Therefore, if multiple sites are hosted from one IP address only the sites containing the name to be blocked will be restricted. However, in the event some news article needs to be censored on a particular website the contents of the article cannot be censored without blocking the entire site. To address this limitation advances in content filtering such as keyword or URL filtering have been implemented to enable a higher degree of accuracy and granularity. The tradeoff between operational costs versus accuracy was illustrated in Figure 1 (Leberknight et al., 2012).

Several anti-censorship techniques have been developed to circumvent the aforementioned technical filtering methods. While there are many academic projects actively engaged in the development of circumvention technologies our focus for this research is on the most common and popular commercial applications used for Internet censorship circumvention. The variety of commercial anti-censorship applications is based on one of the following circumvention methods described in Table 1 (Palfrey et al., 2009).

3.3. Technologies

There is a wide range of anti-censorship technologies developed over the past 15 years. We categorize them into eight main types:

1. User anonymization (JAP, ANON, Tor onion router);
2. Covert channel (Infranet);
3. Deniable publishing (Publius, Tangler, i2p);
4. Web proxy server (Triangle Boy, Garden, UltraSurf, DynaWeb, Gpass);
5. Turn PC into encrypted server (psiphon, peacefire);

Table 1. Circumvention methods (Palfrey et al., 2009)

Method	Definition
HTTP Proxy	HTTP proxying sends HTTP requests through an intermediate proxying server. A client connecting through an HTTP proxy sends exactly the same HTTP request to the proxy as it would send to the destination server unproxied. The HTTP proxy parses the HTTP request; sends its own HTTP request to the ultimate destination server; and then returns the response back to the proxy client
CGI Proxy	CGI proxying uses a script running on a web server to perform the proxying function. A CGI proxy client sends the requested URL embedded within the data portion of an HTTP request to the CGI proxy server. The CGI proxy server pulls the ultimate destination information from the data embedded in the HTTP request, sends out its own HTTP request to the ultimate destination, and then returns the result to the proxy client.
IP Tunneling	Some of the most common tools used for IP Tunneling include virtual private networks or VPNs. VPNs give the user client a connection that originates from the VPN host rather than from the location of the client. Thus a client connecting to a VPN in a non-filtered country from a filtered country has access as if he is located in the non-filtered country.
Re-Routing	Re-routing systems route data through a series of proxying servers, encrypting the data again at each proxy, so that a given proxy knows at most either where the traffic came from or where it is going to, but not both.
Distributed Hosting	A distributed hosting system mirrors content across a range of participating servers that serve the content out to clients upon request. The primary advantage of a distributed hosting system is that it provides access to the requested data even when the original server cannot, for instance if the original server has been overwhelmed by traffic or even taken down by a denial of service attack

6. Application tunneling (Relakks, Guardster, HTTPTunnel);
7. Web tunneling (Anonymizer, Freegate, GhostSurfer);
8. Google Cache and RSS aggregator.

Fundamental research questions remain to be addressed in many of the above. For example, web proxy server technologies are among the most often used anti-censors. Yet there is only limited quantification on how to use a large number of hidden proxies with independence, memorylessness, and costly discovery properties to achieve fundamental limits on how long can users discover proxies but censors cannot.

As soon as the Internet became available in China in the mid-1990s, the Chinese government began to develop technical filtering methods (Freedom House, 2009). It has been reported that the three technical filtering methods used in China: IP blocking, DNS Hijacking, and Content Filtering first emerged in 1999 and 2002 (Global Internet Freedom Consortium, 2002). Since 1999, many circumvention technologies employing one of the circumvention methods, described in Table 1, have been developed. A timeline of the most common circumvention technologies alongside the emergence of the different technical censorship methods are presented in Figure 2 and Table 2. The information in Figure 2 provides insight into the trends and evolution of the various circumvention technologies and with respect to the emergence of the three technical filtering methods. During the time this manuscript was written, no detailed information was available for the most recent technologies developed in 2010.

Consequently, the proceeding analysis excludes the Anonymizer Universal and the Xi Xiang Project which was both developed in 2010. Out of the remaining 15 circumvention tools only 11 are still actively used, suggesting that circumvention technologies have a very short lifespan. After the acquisition of the company which developed Triangle Boy, development for the tool ceased to exist and was no longer supported after 2003 (lifespan 1993-2002) (Global Internet Freedom Consortium, 2007).

Figure 2. Timeline of circumvention and censorship methods

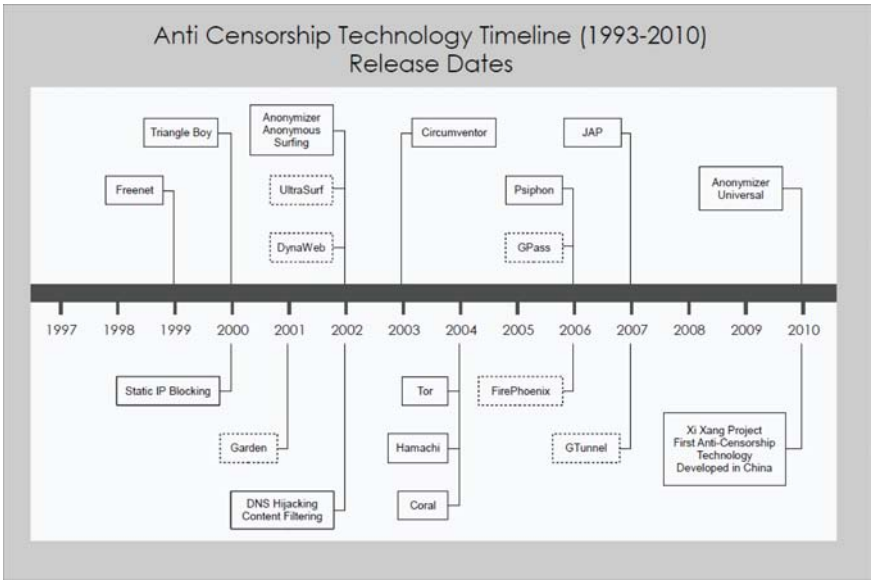


Table 2. Circumvention tools and methods

Tool	Year Released	HTTP Proxy	CGI Proxy	Re-Routing	IP Tunneling	Distributed Hosting
Freenet	1999	✓				
Triangle Boy	2000	✓				
Garden	2000	✓				
Anonymizer	2002	✓				
DynaWeb	2002	✓				
UltraSurf	2002	✓				
Circumventor	2003		✓			
TOR	2004			✓		
Coral	2004					✓
Hamachi	2004				✓	
Firephoenix	2006				✓	
GPass	2006				✓	
Psiphon	2006		✓			
GTunnel	2007				✓	
JAP	2007			✓		
Total		6	2	2	4	1

In addition, TOR has declined in use and popularity following the blocking of 80% of its relays in September 2009 (lifespan 2004-2009) (Wikipedia, n.d.; Phobos, 2009), and GPass abruptly stopped working in March 2009 with no explanation from the developers regarding the present or future status of the software (lifespan 2006-2009) ("GPass not working," 2009). The inactivity and availability of these systems over time indicates the average lifespan for circumvention technologies are on average 4 ½ years. This is a rough approximate due to the limited availability of data, but it may be inferred that, while there may be many reasons for the decline of a particular anti-censorship system, one definitive contributor is China's advanced filtering methods and ability to adapt its methods to combat new circumvention technologies.

To increase the ability to combat online censorship several organizations have joined an alliance known as the Global Internet Freedom Consortium (GIFC), which was formed in 2006. The GIFC is an alliance of organizations that develop and deploy anti-censorship technologies for Internet users residing in oppressive regimes (Global Internet Freedom Consortium, 2007). This alliance allows members to combat online censorship through technical advancements, promotion and support by leveraging the combined strengths and capabilities of each member organization. The grey shaded boxes in Figure 2consist of anti-censorship systems which are all provided by the GIFC (http://www.internetfreedom.org/). The boxes outlined in bold font indicate the year in which the Chinese Government instituted technical filtering methods. Together the side by side comparison of anti-censorship technologies and Internet censorship filtering methods, in Figure 2, provides some indication of how anti-censorship technologies have evolved. Specifically, it can be observed that the disproportionate number of circumvention technologies compared to the limited number filtering methods implies either that these filtering methods are extremely effective, and there are other factors at play which empower the Chinese governments' ability to enforce Internet censorship. The effectiveness of Internet censorship is due to a combination of strategies designed at various social, political and technological levels.

To further elucidate the way in which anti-censorship technologies are evolving, Table 2 presents the circumvention methods employed in each of the 15 tools presented in Figure 2, sorted by the year each tool was released. Two interesting observations can be made based on this information.

First, it is evident that, overall, many more tools based on the HTTP proxy method have been developed compared to any other tool. While there are many factors that can influence the adoption and diffusion of any technology, the most likely candidate in this particular case is performance. A recent study evaluated the amount of delay or response time for a particular anti-censorship tool to return the content from a particular censored site. The results demonstrated that the tools based on the HTTP proxy method had the highest performance followed by the CGI proxy tools and the re-routing tools (Palfrey et al., 2009).

The second observation is that around 2003 there was a shift from developing HTTP proxy tools to IP Tunneling tools. This coincides with the time in which China began to implement and enforce content filtering. IP Tunneling is especially useful for coping with content filters since the specific nature and addressing of the original datagrams are hidden. In addition, when IP Tunneling is combined with IPsec it can be used to create a virtual private network (Wikipedia, n.d.).

This method therefore makes it very difficult for filters to inspect the actual contents of the communication and rely on more expensive methods, such as stateful traffic analysis. However, even though some of the more recent tools are based on IP Tunneling, there is still some evidence that older HTTP proxy tools, such as UltraSurf and DynaWeb are the most popular

and widely used anti-censorship technologies (Global Internet Freedom Consortium, 2007). In addition, to the superior performance of these two tools compared to the other tools evaluated another contributing factor for the success of UltraSurf and DynaWeb may the users trust in the system.

Trust is one critical feature which should be considered when designing censorship resistant systems. The following section discusses the role of trust and several other essential design features.

4. ANTI-CENSORSHIP DESIGN CONSIDERATIONS

Understanding a user's perception of trust in an information system and especially in circumvention technologies is a critical factor influencing technology adoption and acceptance. Several IS studies have examined trust and trusting intention (Gefen, Karahanna, & Straub, 2003; Grazioli & Jarvenpaa, 2000; Li, Hess, & Valacich, 2006; McKnight, Choudhury, & Kacmar, 2002), but there has been little focus on trust relating to circumvention technologies. For circumvention technologies, trust can be broadly divided into two categories, trust within the user's social network and the user's trust within the technology. These determinants of trust are illustrated in Figure 3.

Trust within the social network is influenced by out of band communication and the user's ability to avoid corrupt nodes. Often times to communicate new methods or new censorship resistant technologies individuals in a censored network rely on the exchange of information using emails, instant messaging, CD-ROMs, and telephone calls. This requires a strong degree of trust with other individuals in the network, and individuals who may be trying to penetrate or infiltrate the covert social network.

Equally important is the user's trusting beliefs in the circumvention technology. This involves not only the user's ability to trust the organization or developers of the technology but also the user's trust in other aspects such as the organizations' supporting infrastructure and financial sustainability. For example, as the number of users increase, more investments will most likely be required to operate, expand, and maintain the organizations' server infrastructure (Palfrey et al., 2009). Therefore, users must have trust in an organizations' financial sustainability. In addition, there are other technical aspects influencing a user's trusting intention that are related to the architecture and method employed for each circumvention technology. A decomposition of the different architectures, tools and the placement of trust are illustrated in 4.

Based on the information in Figure 4, existing circumvention technologies are either based on centralized or P2P architectures, and implement a variety of methods such as HTTP Proxy,

Figure 3. Determinants of trust

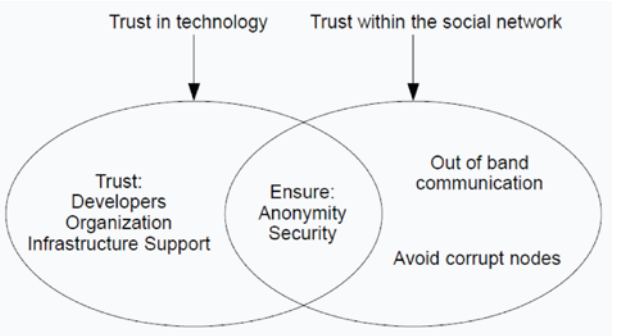
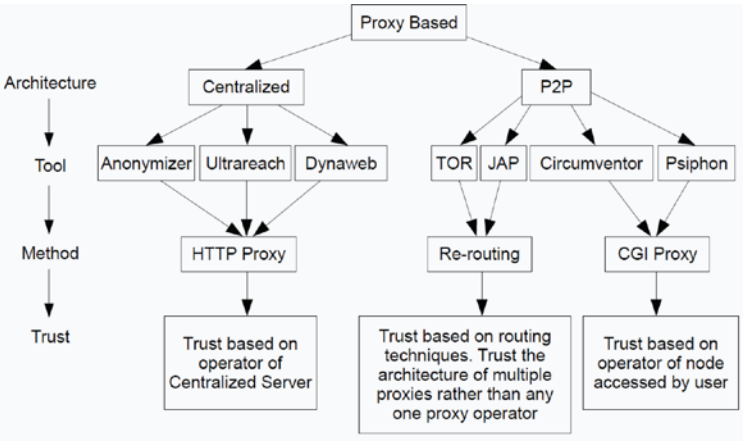


Figure 4. Trust based architectures



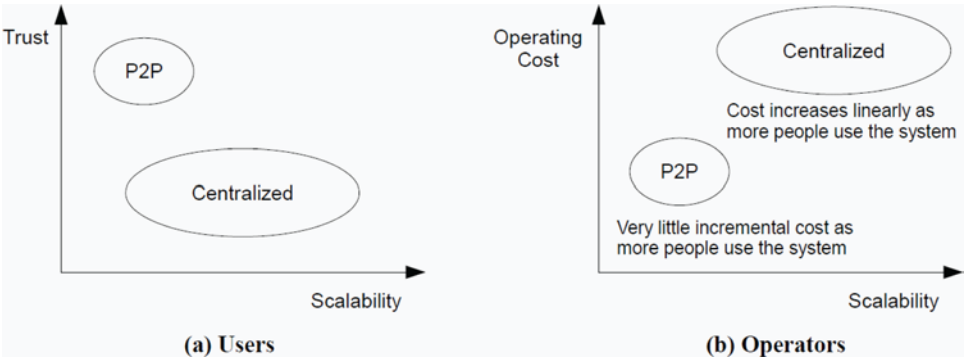
Re-routing and CGI Proxy. Each technology or tool has different advantages and disadvantages regarding trust. For example, due to the distributed nature of P2P architectures, trust is displaced among many users. This may seem like a desirable feature since users will be more confident using a system if they believe several attacks on different peers will be necessary to compromise the system. If users had such faith in P2P systems, we would expect to see a larger P2P user base compared to a centralized user base. However, this is not the case. It has been reported that centralized tools such as DynaWeb and UltraSurf are among the most popular circumvention technologies (Global Internet Freedom Consortium, 2007). The P2P tools were all developed after 2003 (Table 2) and the centralized tools were all developed prior to 2003. This is the dividing point between pre and post content filtering methods. Based on a review of previous literature, centralized tools such as DynaWeb and UltraSurf outperformed other P2P based applications (Global Internet Freedom Consortium, 2007). Therefore, while the newer P2P tools may be more capable at combating the latest content filtering methods, which were employed in 2003, it appears that performance still played a larger part in the users decision to use a particular tool.

While P2P applications reduce the case of a single point of failure and they also distribute trust, P2P applications still suffer from one major disadvantage. The main disadvantage is that the authorities can infiltrate the network by masquerading as a collaborator. In a centralized system if the organization can demonstrate that they are trustworthy than there's less risk of infiltration from corrupt nodes. While P2P applications have the advantage of distributing trust, they also have the disadvantage of not being able to enforce control over corrupt nodes. The ability to determine the exact amount of trust provided by a particular system is somewhat opaque, but this is the very nature of any covert communication system.

Even though trust may influence an individual's decision to use the system, a more likely reason for determinant of behavioral intention to use is performance. Based on our analysis of existing research and popularity of different anti-censorship technologies, it seems that users are more likely to value performance over trust. This does not imply users are not concerned about trust, we believe that a certain degree of trust must exist but performance will still play a more integral role in a user's decision to use a particular technology. The tradeoff between trust and performance for users is illustrated in Figure 5a.

P2P applications are more susceptible to infiltration and corrupt nodes compared to centralized systems, but as Figure 5a demon-

Figure 5. Centralized vs. P2P



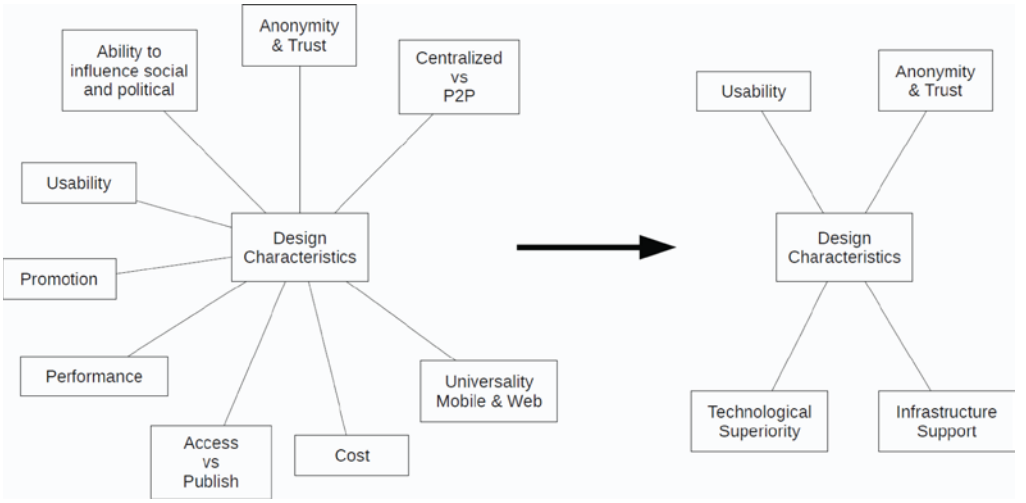
strates they still offer a higher degree of trust. However, the higher degree of trust comes at the expense of performance. This is one likely reason why centralized systems have gained greater popularity. From the operators' perspective in Figure 5b, even though the centralized architectures scale much better, they are much more costly to maintain as the user base increases. This may be one of the main reasons why more P2P tools were developed after 2003. While P2P technologies may be less costly to maintain, their poor performance has swayed users in oppressive regimes that frequently experience online censorship to use centralized systems. However, such users will be severely impacted if organizations that develop centralized systems cannot obtain considerable financial support. Perhaps a consortium such as the GIFC is one strategy for addressing rising costs by combining resources and technical efforts. However, a better solution would be to lobby for government backed support and funding (Caylan, 2010). Fortunately, for many citizens in oppressive regimes, recently there have been several U.S. backed efforts to support projects, organizations and technologies which promote Internet freedom (Figliola, Nakamura, Addis, & Lum, 2010).

While trust is one key factor influencing the adoption and use of anti-censorship tools, there are many other design factors that should also be considered, such as the seven criteria in Section 3. There are a number of circumvention or anti-censorship tools available, and the most appropriate tool is predicated upon several factors such as the specific task to be executed (i.e., access or publish content) and the user's requirements. A diagram illustrating all of the features we have identified and the features that are most crucial to the design and acceptance and success of any anti-censorship system is provided in Figure 6.

5. CONCLUSION

The main objective of this paper is to provide a taxonomy of circumvention technologies and set of critical features to aid designers in developing new techniques to combat online censorship. There are many different tools and each tool has a specific function and advantage. Currently no single tool exists which can be used to accomplish every task, but it is the intention of this research to highlight the most critical factors for the success and adoption of a anti-censorship system. Out of the nine features presented in Figure 6, the following four features should be considered when designing censorship resistant systems: (1) anonymity and trust, (2) usability, (3) technological superiority, and (4) infrastructure support. Trust and anonymity play a very crucial role in an individual's decision to use the system. In addition, previous research has also suggested that usability or how easy it is to use the system is

Figure 6. Design characteristics for anti-censorship technologies



also a key determinant for behavioral intention to use. Subsequently, technological superiority must also be addressed to ensure the system operates at acceptable performance rates. Lastly, infrastructure support is listed as a key factor even though it is more of an operational consideration as opposed to a design factor. However, the lack of infrastructure support implies that as the user base increases so must the organizations ability to support the technology. Now more than ever this is becoming a reality due to recent announcements by the U.S. government to fund certain anti-censorship tools and projects (Caylan, 2010; Figliola et al., 2010).

While technology can play an integral role in combating Internet censorship, ultimately success can only be achieved if the technologies are designed to exert economic and political pressures. For example, leading in the technology evolution may have some short term positive effects, but designing a system which increases the operational costs for the censorship organization will have a much greater impact. A list of existing and potential future technological solutions is provided in Table 3. Those techniques that are under-explored to date are highlighted in grey.

For example, based the analysis of several online censorship methods illustrated in Figure 2 (Leberknight et al., 2012), the exploration of strategies such as changing keywords using a randomized chain reaction will be costly to effectively filter. In addition, the development of new anti-censorship techniques and tools will help to shed light on appropriate methods for quantifying the effectiveness of existing online censorship technologies. Our future research will investigate new quantitative metrics to help understand the existence and achieving of fundamental limits for future anti-censorship technologies.

ACKNOWLEDGMENT

The authors wish to thank Prateek Mittal (UC Berkeley) for his helpful suggestions on recent anti-censorship research literature.

Table 3. Future anti-censorship technologies

Number	Anti-Censorship Techniques
1	Alternative DNS servers/names
2	Open proxy
3	Hopping IP servers and to popular servers
4	Chopping up content across packet boundaries
5	Conceal payload content by stegano/crypto methods
6	Fountain code / network code / spreading code
7	Change keywords with randomized chain reaction
8	Social media
9	Secure cloud computing (Google doc)
10	Remote log in to another computer
11	Secure phase for pre-agreement of protocol
12	Timing covert channels
13	Extensive caching/translation

REFERENCES

Backes, M., Hamerlik, M., Linari, A., Maffei, M., Tryfonopoulos, C., & Weikum, G. (2009, November). Anonymity and censorship resistance in unstructured overlay networks. In R. Meersman, T. Dillon, & P. Herrero (Eds.), *Proceedings of the Confederated International Conferences of On the Move to Meaningful Internet Systems* (LNCS 5870, pp. 147-164).

Caylan, F. (2010, January 20). What Hillary Clinton, Google can do about censorship in China. *The Washington Post*. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2010/01/20/AR2010012002805.html

Clayton, R., Murdoch, S. J., & Watson, R. N. M. (2007). Ignoring the great firewall of China. *I/S: A Journal of Law and Policy for the Information Society, 3*(2), 273-298.

Crandall, J. R., Zinn, D., Byrd, M., Barr, E., & East, R. (2007, October-November). Conceptdoppler: A weather tracker for Internet censorship. In *Proceedings of the 14th ACM Conference on Computer and Communications Security*, Alexandra, VA (pp. 352-365).

Danezis, G., & Anderson, R. (2004, May). The economics of censorship resistance. In *Proceedings of the Third Annual Workshop on Economics and Information Security*, Minneapolis, MN.

Danezis, G., & Diaz, C. (2008). *A survey of anonymous communication channels* (Tech. Rep. No. MSRTR-2008-35). Redmond, WA: Microsoft Research.

Fifield, D., Hardison, N., Ellithorpe, J., Stark, E., Boneh, D., Dingledine, R., & Porras, P. (2012, July). Evading censorship with browser-based proxies. In Proceedings of the 12th International Conference on Privacy Enhancing Technologies (PETS 2012), Vigo, Spain.

Figliola, P. M., Nakamura, K. H., Addis, C. L., & Lum, T. (2010, April 5). *U.S. initiatives to promote global Internet freedom: Issues, policy, and technology*. Congressional Research Service. Retrieved from http://www.fas.org/sgp/crs/misc/R41120.pdf

Gefen, D., Karahanna, E., & Straub, D. (2003). Trust and TAM in online shopping: An integrated model. *Management Information Systems Quarterly*, *27*(1), 51–90.

Global Internet Freedom Consortium. (2002, July). *Internet blocking exposed*. Retrieved from http://www.internetfreedom.org/files/WhitePaper/InternetBlockingExposed.pdf

Global Internet Freedom Consortium. (2007, November 21). *Defeat Internet censorship: Overview of advanced technologies and products*. Retrieved from http://www.internetfreedom.org/archive/Defeat_Internet_Censorship_White_Paper.pdf

GPass not working. (2009, March 29). *How-to-Hide*. Retrieved from http://www.how-to-hide-ip.info/2009/03/24/gpass-not-working

Grazioli, S., & Jarvenpaa, S. (2000). Perils of Internet fraud: An empirical investigation of deception and trust with experienced Internet customers. *IEEE Transactions on Systems, Man, and Cybernetics. Part A, Systems and Humans*, *30*(4), 395–410. doi:10.1109/3468.852434

Houmansadr,A., Nguyen,T.,G., Caesar, M. and Borisov, N. Cirripede: Circumvention Infrastructure using Router Redirection with Plausible Deniability. In Proceedings of the 18th ACM conference on Computer and Communications Security, CCS '11, pages 187-200, 2011.

Katti, S., Katabi, D., & Puchala, K. (2005). *Slicing the onion: Anonymous routing without PKI* (Tech. Rep. No. MIT-CSAIL-TR-2005-053). Cambridge, MA: MIT Computer Science and Artificial Intelligence Laboratory.

Karlin, J., Ellard, D., Jackson, W., A., Jones, E., C., Lauer, G. Mankins, P., D. and W. T. Strayer, T., W. Decoy routing: Toward unblockable Internet communication. In N. Feamster, editor, 1st USENIX Workshop on Free and Open Communications on the Internet (FOCI'11). USENIX Association, Aug. 2011.

Leberknight, C., Chiang, M., & Poor, H. V., & Wong, Ming-Fai, F. (2012). A taxonomy of censors and anti-censors: Part I: Impacts of Internet censorship. *International Journal of E-Politics*, *3*(2), 52–64. doi:10.4018/jep.2012040104

Li, X., Hess, T. J., & Valacich, J. S. (2006, September). Using attitude and social influence to develop an extended trust model for information systems. *ACM SIGMIS Database*, *37*(2-3), 108–124. doi:10.1145/1161345.1161359

MacKinnon, R. (2008). Flatter world and thicker walls? Blogs, censorship and civic discourse in China. *Public Choice*, *134*(1), 31–46. doi:10.1007/s11127-007-9199-0

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, *13*(3), 334–359. doi:10.1287/isre.13.3.334.81

Moghaddam, H. M., Li, B., Derakhshani, M., & Goldberg, I. (2012, October). SkypeMorph: Protocol obfuscation for Tor bridges. In Proceedings of the 19th ACM Conference of Computer and Communications Security (CCS 2012), Raleigh, NC.

OpenNet Initiative. (2005). *Internet filtering in China in 2004-2005: A country study*. Retrieved from http://www.opennetinitiative.net/studies/china

Panchenko, A., & Pimenidis, L. (2007, May). Using trust to resist censorship in the presence of collusion. In *Proceedings of the IFIP TC-11 22nd International Information Security Conference*, Sandton, South Africa.

Park, J. C., & Crandall, J. R. (2010, June). Empirical study of a national-scale distributed intrusion detection system: Backbone-level filtering of HTML responses in China. In *Proceedings of the 30th International Conference on Distributed Computing Systems*, Genoa, Italy.

Perng, G., Reiter, M. K., & Wang, C. (2005, June). Censorship resistance revisited. In M. Barni, J. Herrera-Joancomarti, S. Katzenbeisser, F. Perez-Gonzalez (Eds.), *Proceedings of the 7th International Conference on Information Hiding* (LNCS 3727, pp. 62-76).

Phobos. (2009, September 27). *Tor partially blocked in China* [Web log post]. Retrieved from https://blog.torproject.org/blog/tor-partially-blocked-china

Rao, J. R., & Rohatgi, P. (2000, August). Can pseudonymity really guarantee privacy? In *Proceedings of the Ninth USENIX Security Symposium*, Denver, CO (pp. 85-96).

Serjantov, A. (2002, March). Anonymizing censorship resistant systems. In *Proceedings of the First International Workshop on Peer-to-Peer Systems*, Cambridge, MA (pp. 111-120).

Sovran, Y., Libonati, A., & Li, J. (2008, February). Pass it on: Social networks stymie censors. In *Proceedings of the Seventh International Workshop on Peer-to-Peer Systems*, Tampa Bay, FL.

Vasserman, E., Jansen, R., Tyra, J., Hopper, N., & Kim, Y. (2009, November). Membership-concealing overlay networks. In Proceedings of the 16th ACM Conference of Computer and Communications Security (CCS 2009), Chicago, IL

Waldman, M., & Mazieres, D. (2001, November). Tangler: A censorship-resistant publishing system based on document entanglements. In *Proceedings of the Eighth ACM Conference on Computer and Communications Security*, Philadelphia, PA (pp. 126-135).

Wikipedia. (n.d.). *Internet censorship in the People's Republic of China*. Retrieved May 1, 2010, from http://en.wikipedia.org/wiki/Internet_censorship_in_the_People's_Republic_of_China

Wikipedia. (n.d.). *IP tunneling*. Retrieved February 1, 2010, from http://en.wikipedia.org/wiki/IP_tunnel

Wolfgarten, S. (2005). *Investigating large-scale Internet content filtering* (Unpublished master's thesis). Dublin City University, Dublin, Ireland.

Wustrow, E., Wolchok, S., Goldberg, I., and Halderman, A. J. Telex: Anticensorship in the network infrastructure. In D. Wagner, editor, 20th USENIX Security Symposium. USENIX Association, Aug. 2011.

Christopher S. Leberknight received the BA degree in Computer Science from Rutgers University, New Brunswick, NJ, the MS degree in Computer Science and the PhD degree in Information Systems from the New Jersey Institute of Technology (NJIT), Newark, NJ. He is currently an Assistant Professor of Computer Science at William Paterson University, Wayne, NJ. He also worked as a Postdoctoral Research Associate in the Department of Electrical Engineering at Princeton University. His primary research interests are in the technological applications and computational methods for modeling human behavior and decision making. In addition to his academic experience he also has over 10 years of industry experience as a systems engineer and technical systems manager. Dr. Leberknight is a member of the Association of Computing Machinery, IEEE and the Association for Information Systems.

Mung Chiang is a Professor of Electrical Engineering at Princeton University, and an affiliated faculty in Applied and Computational Mathematics, and in Computer Science. He received his BS (Hons.), MS, and PhD degrees from Stanford University in 1999, 2000, and 2003, respectively, and was an Assistant Professor 2003-2008 and an Associate Professor 2008-2011 at Princeton University. Chiang's research in networking received awards such as the IEEE Tomiyasu Award, PECASE, TR35, ONR YIP, NSF CAREER, Princeton Wentz Faculty Award, and several best paper awards. His inventions resulted in five issued patents and several technology transfers to commercial adoption, and he founded the Princeton EDGE Lab in 2009. He is currently writing an undergraduate textbook 20 Questions about the Networked Life.

Felix Ming Fai Wong received the BEng degree in computer engineering from the Chinese University of Hong Kong, in 2007, and the MSc degree in computer science from the University of Toronto, in 2009. He is currently a PhD student in electrical engineering at Princeton University. His research interests are in computer networks and online social networks.