

ANONYMITY ON THE INTERNET:  
HOW DOES IT WORK, WHO NEEDS IT,  
AND WHAT ARE ITS POLICY IMPLICATIONS?

I.	CHINA'S GOLDEN SHIELD .....	1396
II.	TOOLS THAT ALLOW CHINESE DISSIDENTS AND OTHER INTERNET USERS TO AVOID CENSORSHIP .....	1399
III.	FREE SPEECH AND ANONYMITY IN THE UNITED STATES.....	1405
IV.	REGULATION OF SPEECH VIA PUBLIC AND PRIVATE LAW ....	1409
V.	THE DANGERS OF SPEECH OVERREGULATION IN A WORLD WITH ANONYMOUS COMMUNICATION .....	1411
VI.	CRITIQUES & CONCLUSION .....	1415

Since its inception, most communications have passed through the infrastructure of the Internet without any attempt to hide their contents. Electronic mail, the web, and other forms of communication on the Internet have passed from computer to computer unencrypted and visible to any individual with the capability, access, and desire to observe the communication. Current proposals to monitor the Internet as a method to deter criminal activity assume that communications will occur in a plain unencrypted format between known users. However, as encryption technologies have become more available and widespread, law enforcement officers who attempt to intercept the communications via service providers may no longer be able to easily observe the content of some Internet communication or know the identities of the parties involved. Technology now exists that allows users to disseminate content on the Internet through secure anonymous channels, where neither sender nor receiver knows the other's true identity.

Many Americans incorrectly believe that the Internet confers some type of anonymity in their communications and that their normal daily communications are of little consequence to law enforcement; therefore, they believe that they have little use for tools that provide a greater guarantee of anonymity. This contrasts with Internet users in countries like China. Chinese Internet users are well aware that they access the Internet under highly regulated, observed, and censored circumstances. Users in

China who wish to access unfiltered information must bypass the government controls via encryption and anonymizing technology.

This Note argues that it is to the benefit of law enforcement if governments recognize that active censorship of content on the Internet may push Internet users, and their content, into the completely unregulated zones of the anonymous Internet, rather than eliminating the content. In contrast, if users generally do not feel the need to protect their communications from government intrusion, law enforcement may have an easier time preventing truly dangerous and illegal activity because the communication will be more readily apparent.

### I. CHINA'S GOLDEN SHIELD

The People's Republic of China, which has the world's most sophisticated Internet filtering regime, presents a good case study of how a government may successfully attempt to control what its citizens see, hear, and say. As of 2006, about 132 million individuals in China possess access to the Internet.<sup>1</sup> About 52 million of these individuals use fast broadband, while the remainder access the Internet through slower links, Internet cafes, and other methods.<sup>2</sup> With that many users, China has become the second largest Internet user base in the world, second only to the United States,<sup>3</sup> and will likely become the largest user base in the world in the near future.

In recent years, the Chinese communist government has begun a transition to capitalism and a free market economy. In order to sustain the rapid economic growth that has allowed many of its over one billion citizens to achieve higher levels of education and middle class lifestyles, the Chinese government has attempted to balance the need for its citizens to participate in the global economy with the current regime's desire for control over the information available to Chinese society. Realizing that profitable media markets and international trade require free movement of information, the Chinese government has allowed the Internet to exist within the country. In doing so, however, the government has sought to "have its cake and eat it too" by encouraging growth of the Internet for economic and entertainment purposes while tightly controlling its use for political purposes.<sup>4</sup> Thus, while the

---

<sup>1</sup> *China Sees Rapid Rise in Web Use*, CNN.COM, Dec. 29, 2006, <http://www.cnn.com/2006/TECH/internet/12/29/china.online.ap/index.html>.

<sup>2</sup> *Id.*; OPENNET INITIATIVE, INTERNET FILTERING IN CHINA IN 2004-2005: A COUNTRY STUDY 5, (2005), [http://www.opennetinitiative.net/studies/china/ONI\\_China\\_Country\\_Study.pdf](http://www.opennetinitiative.net/studies/china/ONI_China_Country_Study.pdf).

<sup>3</sup> OPENNET INITIATIVE, *supra* note 2, at 52.

<sup>4</sup> *See generally id.* at 52-53.

government recognizes the importance of information to its economy, it continues to implement information control policies out of fear for its own survival and stability.

China implements this dichotomy of allowing free flow of information for economic purposes while prohibiting free flow of information for political purposes, via a massive censorship and surveillance regime that combines technological measures with human censors. The technological side, officially called Golden Shield and colloquially known as the Great Firewall of China, links various electronic databases, records of Internet use, and bank records, and may even include speech signal processing for phone calls.<sup>5</sup> China's Internet incorporates proxy servers which use internet protocol (IP), domain name system (DNS), and uniform resource locator (URL) blocking at the whim of country-wide, regional, and local governments.<sup>6</sup> These censorship proxies also examine the text of the URL for certain keywords (such as "Falun Gong")<sup>7</sup> and provide negative feedback in the form of temporary disconnection from the Internet to users who attempt to search for these keywords.<sup>8</sup> Many of these same keyword censoring mechanisms apply to Internet chat networks and phone text messaging (commonly known as SMS or short messaging service).<sup>9</sup>

---

<sup>5</sup> GREG WALTON, CHINA'S GOLDEN SHIELD: CORPORATIONS AND THE DEVELOPMENT OF SURVEILLANCE TECHNOLOGY IN THE PEOPLE'S REPUBLIC OF CHINA 5 (2001), available at [http://www.dd-rd.ca/site/\\_PDF/publications/globalization/CGS\\_ENG.PDF](http://www.dd-rd.ca/site/_PDF/publications/globalization/CGS_ENG.PDF).

<sup>6</sup> Steven Cherry, *The Net Effect*, IEEE SPECTRUM ONLINE, June 2005, <http://www.spectrum.ieee.org/jun05/1219>. IP and DNS blocking are simpler address-based methods which stop Internet traffic without the need to look into the contents of the communication. URL blocking requires an examination of the actual requests passing between a web user and a web server. For a more thorough explanation, see *Center for Democracy & Technology v. Pappert*, 337 F. Supp. 2d 606, 628-34 (D. Pa. 2004). A very comprehensive, though slightly dated, explanation is available in W. RICHARD STEVENS, 1 TCP/IP ILLUSTRATED: THE PROTOCOLS (1994).

<sup>7</sup> "Falun Gong, developed in 1992 by a former clerk named Li Hongzhi . . . combines traditional Chinese exercises and meditation with elements of Buddhism and Taoism." Elisabeth Rosenthal & Erik Eckholm, *Vast Numbers of Sect Members Keep Pressure on Beijing*, N.Y. TIMES, Oct. 28, 1999, at A3. The Chinese government began viewing the sect as a serious threat after over 10,000 members surprised the government with an illegal protest in China in 1999. Elisabeth Rosenthal, *Beijing Journal: Group's Morning Exercises Are Politically Suspect*, N.Y. TIMES, June 29, 1999, at A4; see also Seth Faison, *Followers of Chinese Sect Defend Its Spiritual Goals*, N.Y. TIMES, July 30, 1999, at A4 ("When the crackdown began last week, the authorities called Falun Gong the greatest threat to their security since the Tiananmen student movement of 1989, and orchestrated its largest political campaign since that time, revving up the nation's sprawling Communist Party apparatus to try to stamp out any practice of Falun Gong."). For general information about the Falun Gong movement, see Falun Dafa, <http://www.falundafa.org/> (last visited Nov. 29, 2006).

<sup>8</sup> Cherry, *supra* note 6.

<sup>9</sup> Kevin Anderson, *Breaking Down the Great Firewall*, BBC NEWS, Apr. 30, 2005, <http://news.bbc.co.uk/2/hi/asia-pacific/4496163.stm>. China has successfully implemented some version of URL filtering, which may include a periodic review of sites "properly" blocked. *Id.* This fact potentially stands in contrast to the *Pappert* court decision, which struck down a Pennsylvania child pornography filtering law in part due to the difficulty of implementing a local URL filter which was not overbroad. See generally *Pappert*, 337 F. Supp. 2d 606.

Although the Chinese Internet backbone likely does not filter e-mail content for keywords, individual Internet Service Providers (ISPs) may do so at the behest of the government.<sup>10</sup>

Human censors in China include a government-employed Internet police force with between 30,000 and 50,000 members, and employees of cooperating ISPs and content providers.<sup>11</sup> By law, all ISPs must obtain licenses to operate, and all Internet users must register with the police.<sup>12</sup> Because Chinese law holds ISPs and content providers criminally liable for the activity of their users,<sup>13</sup> those services will actively filter and censor user-generated content, such as e-mail, bulletin board postings, and chat networks.<sup>14</sup> Thus, the human component of China's censorship mechanism includes not only government employees, but also corporations, which provide the infrastructure of China's Internet. In addition to censoring content, as required by national and local governments, service providers must retain records of use for sixty days, and must turn this information over to police upon request.<sup>15</sup> Service providers must also monitor and report suspicious or banned content, or employees may face criminal penalties.<sup>16</sup>

China's national and local governments have followed through on their censorship threats; users and employees of service providers who have placed banned content online have faced arrest and severe criminal penalties.<sup>17</sup> However, despite the risks involved with obtaining and distributing banned content, Chinese use of the Internet and other information technologies has opened up the country in ways unimaginable even ten years ago. Although discussion of democracy, Tibet, and the Falun Gong remains tightly controlled, today the Chinese media has more freedom to report on subjects such as AIDS, crime, and corruption.<sup>18</sup> The government has perhaps recognized that it cannot realistically maintain total control over the information available to Chinese citizens who use the Internet, and so has become more selective in its censorship activity.<sup>19</sup>

In one case that illustrates the limits of Chinese censorship,

---

<sup>10</sup> OPENNET INITIATIVE, *supra* note 2, at 46.

<sup>11</sup> Cherry, *supra* note 6.

<sup>12</sup> OPENNET INITIATIVE, *supra* note 2, at 9-11.

<sup>13</sup> *Id.*

<sup>14</sup> *Id.* at 13-18.

<sup>15</sup> *Id.* at 10-14.

<sup>16</sup> *Id.* at 16-18.

<sup>17</sup> *Id.* at 10.

<sup>18</sup> Dan Griffiths, *China's Breakneck Media Revolution*, BBC NEWS, Aug. 19, 2005, <http://news.bbc.co.uk/2/hi/asia-pacific/4156458.stm>.

<sup>19</sup> As the Chinese have embraced the Internet, 36.8 million web log ("blog") sites have been created within China. Howard W. French, *Chinese Discuss Plan to Tighten Restrictions on Cyberspace*, N.Y. TIMES, July 4, 2006, at A1.

protesters used SMS text messages and social networking web sites to organize anti-Japanese rallies.<sup>20</sup> Rather than call the event a “protest,” a word that would likely be censored, the organizers used the term “spring outing.”<sup>21</sup> When the government eventually caught on to their trick, the censors decided that it would be futile to completely stop the protests. At first they used a lighter hand to quell the protests by sending an ambiguous SMS text message to all users asking them “to express [their] patriotic passion through the right channel, following the laws and maintaining order.”<sup>22</sup> Only after weeks of protests did the government crack down via arrests.<sup>23</sup>

Despite the growth of information freedom, the government continues to operate under a veil of secrecy, and absolutely prohibits any open communication about certain subjects. If, for example, the protesters had desired to protest Chinese policies on Falun Gong, the government might have cracked down much earlier, and possibly in a more violent fashion. Fear of arrest prevents users from discussing politics on internal Chinese web sites, but the censorship mechanism also prevents Chinese users from accessing certain political sites that exist outside of China. Chinese Internet users who wish to view an uncensored Internet must somehow bypass the censorship mechanism. A number of Internet utilities have evolved that allow users in China and other authoritarian countries to do exactly that.

## II. TOOLS THAT ALLOW CHINESE DISSIDENTS AND OTHER INTERNET USERS TO AVOID CENSORSHIP

Not all tools that provide users with the ability to avoid Internet monitoring and censorship have evolved because of authoritarian regimes like China.<sup>24</sup> However, the user base of

---

<sup>20</sup> Anderson, *supra* note 9.

<sup>21</sup> *Id.*

<sup>22</sup> *Id.*

<sup>23</sup> *Id.* The Chinese government is currently contemplating additional monitoring for cell phones in order to make it more difficult to organize protests. French, *supra* note 19.

<sup>24</sup> Johan “Julf” Helsingius, who created anon.penet.fi in Finland, one of the first known public anonymous remailers on the Internet, has explained his reasons for creating an anonymous service:

It's clear that for things like the Usenet groups on sexual abuse, people need to be able to discuss their own experiences without everyone knowing who they are. Where you're dealing with minorities—racial, political, sexual, whatever—you always find cases in which people belonging to a minority would like to discuss things that are important to them without having to identify who they are.

Joshua Quittner, *Anonymously Yours—An Interview with Johan Helsingius*, WIRED MAG., June 1994, available at <http://www.wired.com/wired/archive/2.06/anonymous.1.html>; see also The anon.penet.fi Anonymous Server (Long) (Dec. 1, 1992),

these utilities has certainly grown as individuals living in countries that provide tightly controlled access to the Internet realize the potential to obtain uncensored information and possibly participate anonymously in political conversations.<sup>25</sup> In addition, both governments and political organizations have provided financial support to some anonymizing tools for the specific purpose of encouraging free discourse within authoritarian regimes. For example, the United States government funds UltraSurf, an anonymizing proxy produced by followers of Falun Gong in the United States.<sup>26</sup> As of 2001, one report claimed that ten percent of Internet users in China admitted to using proxy services in order to avoid the “Great Firewall of China.”<sup>27</sup> Currently, UltraSurf and Freegate, a similar type of software, claim 100,000 daily users from China.<sup>28</sup>

Internet users in China, especially those who make use of these anonymizing tools, know all too well that the Internet provides little anonymity and privacy to ordinary users. The experience of users in China and other countries that censor and monitor Internet traffic stands in sharp contrast to the expectations of privacy and security assumed by users in the United States. Prior to the recent spate of lawsuits against those who shared copyrighted content on the Internet, many Americans assumed, incorrectly, that the medium provided anonymity sufficient to guarantee that “[o]n the Internet, nobody knows you’re a dog.”<sup>29</sup>

Instead of providing privacy and security, most communications on the Internet—including e-mail, web browsing, messaging, and discussion forums—easily reveal the IP address, and thus the likely physical location, of the user. Most data flows between users in unprotected plain text. Users know the location of web servers, web servers know the location of users, and any “man in the middle”<sup>30</sup>—whether a Chinese censor or an FBI investigator empowered by the Communications Assistance for

---

<http://groups.google.com/group/alt.sex.movies/msg/d79822cd09a9e2ee?> (announcing the availability of anonymous remailer anon.penet.fi).

<sup>25</sup> Geoffrey A. Fowler, *Great Firewall: Chinese Censors of Internet Face ‘Hacktivists’ in U.S.*, WALL ST. J., Feb. 13, 2006, at A1 (showing that “[u]se of programs to defeat Chinese censors surges when news does.”).

<sup>26</sup> Philip P. Pan, *Free Software Takes Users Around Filters*, WASH. POST, Feb. 21, 2006, at A11.

<sup>27</sup> WALTON, *supra* note 5, at 8.

<sup>28</sup> Fowler, *supra* note 25.

<sup>29</sup> Peter Steiner, *Cartoon*, NEW YORKER MAG., July 5, 1993, at 61.

<sup>30</sup> A man in the middle “describes an attacker that is situated (physically or logically) between communicating parties.” IAN GREEN, *DNS SPOOFING BY THE MAN IN THE MIDDLE* 4 (2005), [http://www.sans.org/reading\\_room/whitepapers/dns/1567.php](http://www.sans.org/reading_room/whitepapers/dns/1567.php) (last visited Dec. 11, 2006).

Law Enforcement Act (CALEA)<sup>31</sup>—can easily discover the identity of the sender, receiver, and content of information. The lack of anonymity and secrecy allows both easy censoring of information and the identification and prosecution of those involved in the illegal exchange of information.

Some services on the Internet have taken a basic step towards providing at least some protection of users' secrecy regarding the information transmitted between users. Encryption prevents a man in the middle from knowing the contents of any communication between two users, such as between a web browser and a web server. Banks and login servers use encryption to protect users' financial information and passwords.<sup>32</sup> Messaging software could easily use encryption to hide the contents of a conversation. Encrypted web browsing would prevent China's censors from filtering search requests based on URL filtering. Encryption, however, only protects the content of the communication; it does not prevent censors or snoopers from discovering the end points of the conversation, and does not prevent the end points from finding out each other's identity. A man in the middle could easily discover that a user was accessing content from CNN.com even though the precise nature of the content accessed or posted would remain unknown without more direct surveillance of the endpoint users' computers. Therefore, even with encryption, Chinese censors could easily block the IP or DNS address of servers with offending content.

A better solution to plain encryption involves using a computer designated as a proxy. A user inside China who wishes to access forbidden web content would configure his or her computer to send all requests through a proxy server, rather than directly to the blocked web site. The proxy, which exists outside of China's censored network, would then serve as an intermediary between the user inside China and the banned content outside of China. Because most useful anti-censorship proxies employ encryption between the user and the proxy, the Chinese censoring system would be unable to decipher the contents or ultimate destination of packets<sup>33</sup> sent to the outside proxy. Under the

---

<sup>31</sup> CALEA mandates access to certain types of communication by law enforcement. 47 U.S.C. § 1002 (2006).

<sup>32</sup> See, for example, Citibank's web site that allows account holders to access their bank accounts online, and which uses the encrypted https protocol for security of communication. Citibank Online, Welcome, <https://web.da-us.citibank.com/cgi-bin/citifi/portal/1/1.do> (last visited Nov. 21, 2006).

<sup>33</sup> "Data travels on a network in the form of *packets*, each of which consists of a header and a payload. The header tells where the packet came from and where it's going . . . . The payload is the data to be transferred." EVI NEMETH ET AL., UNIX SYSTEM ADMINISTRATION HANDBOOK 246 (2d ed. 1995) (emphasis in original).

proxy system, the user knows the identity and destination of the communication, but the receiving web server has no information about the sender other than the proxy's IP address.<sup>34</sup>

This model for anonymous Internet communication provides security and privacy to those wishing to circumvent China's Great Firewall, so long as the censors themselves do not know the IP or DNS addresses of the proxy servers. If the censors learn this information, however, those addresses may be blocked just as easily as any other IP address on the Internet. Proxy services intended for users in China, such as UltraSurf and Freegate, claim to have discovered methods to avoid discovery by Chinese censors.<sup>35</sup> Most likely, these methods involve rapid change in IP addresses coupled with a secure method for informing users of the new servers. Because China's mechanism for Internet censorship cannot instantly respond to new "threats," each proxy IP probably has a limited useful lifespan before the Great Firewall adapts.

Proxies have one major drawback, however. The proxy itself is a known entity—in the case of UltraSurf and Freegate, known entities incorporated in the United States—which can itself be subject to legal process. Should a man in the middle gain control over the proxy itself, then the proxy server would easily reveal all of its secrets. Thus, the privacy, security, and anonymity provided by a proxy could be instantly compromised by something as simple as a police warrant.<sup>36</sup>

A still more secure method for accessing the Internet, which eliminates the problem of the compromised proxy server, exists in services like Tor and I2P.<sup>37</sup> Every user of Tor software chooses to

<sup>34</sup> In the United States, savvy students have used proxies such as HideMyAss.com to circumvent their school districts' Internet filters. Stefanie Olsen, *School Filters vs. Home Proxies*, C|NET NEWS.COM, May 3, 2006, [http://news.com.com/School+filters+vs.+home+proxies/2009-1041\\_3-6067716.html?tag=nefd.top](http://news.com.com/School+filters+vs.+home+proxies/2009-1041_3-6067716.html?tag=nefd.top).

<sup>35</sup> Fowler, *supra* note 25.

<sup>36</sup> The anonymous remailer anon.penet.fi, *supra* note 24, was forced by a Finnish court to reveal the identity of an individual who used the service to criticize Scientology. Tom W. Bell, *Anonymous Speech*, WIRED MAG., Oct. 1995, available at <http://www.wired.com/wired/archive/3.10/cyber.rights.html>. As a result of these types of legal attacks, Helsingius eventually shut down the service. Amy Harmon, *Internet Figure Pulls Plug on His Anonymity Service; Technology: Supporters Say 'Remailer' Promoted Free Speech, Critics Blame It for Crime, Pornography*, L.A. TIMES, Aug. 31, 1996, at A1.

<sup>37</sup> Tor: Anonymity Online, Tor, <http://tor.eff.org> (last visited Nov. 21, 2006); Welcome to I2P, <http://www.i2p.net> (last visited Nov. 21, 2006). It is beyond the scope of this Note to explain the technical differences between these two services. From the perspective of the lay user, Tor and I2P are very similar services. See TheOnionRouter/TorFAQ, <http://wiki.noreply.org/noreply/TheOnionRouter/TorFAQ#head-2a06030372e30f1308c90b62d6743dc8e408ca58> (last visited Dec. 11, 2006). A good overview of anonymity-protecting networks is also available from John Alan Farmer, *The Specter of Crypto-Anarchy: Regulating Anonymity-Protecting Peer-to-Peer Networks*, 72 FORDHAM L. REV. 725, 745-59 (2003).

run the software in either client or server mode. Those who run the software in server mode become part of the Tor network and facilitate the anonymous communication of other users via a method called “onion routing.” Tor operates by chaining together three Tor proxy services, each with its own encryption key.<sup>38</sup> Tor builds a new chain of servers and encryption keys for each user at frequent intervals. When a user connects to a web site in Tor, that user encrypts the information so that only the final Tor server in the chain has the capability to decrypt and read the message before forwarding it onto its final destination.<sup>39</sup> Because Tor servers are located worldwide, and the software generates a new chain of servers at frequent intervals, compromising a single server would have little effect on the overall privacy and security of the network since that individual server could never know both the content/destination and the sender’s identity at the same time.

In addition to secure access to web sites and other services, Tor has another improvement over other means of accessing the Internet, most of which require that at least one party knows the identity of the other: Tor has a function called “hidden services” that allows an individual to hide a server—such as a web server—inside the Tor network.<sup>40</sup> Any user of Tor may access the content on this server, however, neither party to the communication can know the identity and location of the other. Thus, a true double-blind communication exists. The creator of a hidden service within China could create a hidden web server with content critical of the Chinese government, and the Internet police would have no way to discover the true owner of the web site.<sup>41</sup> While the Chinese Great Firewall could attempt to ban access to IP addresses of individual Tor servers, attempting this with a large Tor user base with transient IP addresses would result in inefficient and incomplete censorship.<sup>42</sup>

The final method of anonymity and privacy on the Internet

---

<sup>38</sup> Tor, Overview, <http://tor.eff.org/overview.html.en> (last visited Dec. 11, 2006).

<sup>39</sup> *Id.*

<sup>40</sup> Tor, Configuring Hidden Services for Tor, <http://tor.eff.org/docs/tor-hidden-service.html.en> (last visited Nov. 21, 2006).

<sup>41</sup> This is true in theory only. A recent bug fix to Tor involved efforts to prevent triangulation on the actual location of the hidden service. Chinese dissidents should be wary of using Tor hidden services to provide absolute anonymity until the possibility of triangulation has been reduced further. *See generally* Roger Dingledine et al., Challenges in Deploying Low-Latency Anonymity (2005) (unpublished manuscript), *available at* <http://tor.eff.org/cvs/tor/doc/design-paper/challenges.pdf>.

<sup>42</sup> The Tor user base has not yet reached this critical mass. This is evident from the fact that web sites like Craigslist.com have banned many—though not all—Tor IP addresses from its online service. Craigslist is still reachable from within Tor, but the user has a less than optimal experience.

discussed in this Note involves a service called Freenet.<sup>43</sup> Unlike Tor, Freenet users do not have the option of running as a client or a server; all Freenet users must join the peer-to-peer Freenet network as a server. Freenet does not allow users to access the Internet outside of Freenet. Instead, the entire network of servers acts as one enormous encrypted double-blind anonymous data store.<sup>44</sup> Each server proxies data for its neighbors within the network, and searches for data may travel through many server “hops” before finding the desired data.<sup>45</sup> As encrypted data moves from server to server, the intermediary servers save a copy of the data; thus every user of Freenet must be willing to store data and serve it to those requesting it. Users never know the identity of the uploader of the content, the identity of the downloader, or even the nature of the content served to others. This anonymity and security is inherent to the Freenet network itself. One web site, [freenet-china.org](http://freenet-china.org), appears to exist as a gateway to Freenet for users in China.<sup>46</sup>

Ordinary proxy servers and Tor’s onion routing allow users to access content on the Internet anonymously. In addition, services such as Freenet and Tor also allow users to serve content anonymously. So long as China’s government continues to suppress information from its citizens, these networks will serve to allow ordinary Chinese citizens to learn about philosophies and news reports that its government would rather suppress, and potentially to create their own anonymous content which criticizes the Chinese government. A “cat and mouse game” currently exists between those who manage the Great Firewall and those who desire to poke holes through it, but technology has not yet advanced enough to automatically detect and block packets from UltraSurf, Freerate, Tor, and Freenet.<sup>47</sup>

These anonymity services have evolved, at least in part, in order to overcome the Chinese government’s suppression of speech. However, the availability of these services within China

---

<sup>43</sup> The Free Network Project, <http://freenet.sourceforge.net> (last visited Oct. 5, 2006).

<sup>44</sup> The Free Network Project, What Is Freenet?, <http://freenetproject.org/whatis.html> (last visited Dec. 12, 2006).

<sup>45</sup> *Id.*; see also The Free Network Project, Freenet Frequently Asked Questions, <http://freenetproject.org/faq.html> (last visited Dec. 12, 2006).

<sup>46</sup> While Freenet links on the [freenet-china.org](http://freenet-china.org) web site resemble ordinary “www” links, the Freenet links will not work unless the Freenet software is installed and running. Because [freenet-china.org](http://freenet-china.org) is an ordinary web site, it is possible that China has censored the URL, though nothing prevents other individuals from creating mirror sites. Mirror sites are duplicate copies of web sites located on different servers, often leading the user back to the original web site. See SearchStorage.com, What Is a Mirror?, [http://searchstorage.techtarget.com/sDefinition/0,290660,sid5\\_gci212579,00.html](http://searchstorage.techtarget.com/sDefinition/0,290660,sid5_gci212579,00.html) (last visited Dec. 11, 2006).

<sup>47</sup> See Anderson, *supra* note 9; Fowler, *supra* note 25.

highlights the ability of Internet users anywhere—even users living under repressive regimes—to route around censorship via anonymity services. In China, where surveillance under the Golden Shield has made it clear that the government does not value privacy of communication, the ability of individuals to communicate their ideas anonymously has become a battle between the government and its citizens. The censors attempt to block access to outside IP addresses which provide anonymity, but with each iteration, developers of anti-censorship anonymity software make their software more robust. Because Tor and Freenet provide better anonymity as their respective user bases increase, a large enough user base<sup>48</sup> with transient IP addresses outside of China would be difficult, if not impossible, for the Chinese government to block.<sup>49</sup> Thus, the experience of Chinese Internet users with avoiding censorship and surveillance provides valuable lessons for other governments that wish to control free expression, dissemination of information, and online content.

### III. FREE SPEECH AND ANONYMITY IN THE UNITED STATES

Every country—even the most democratic among them—places some limits on freedom of expression. American free speech doctrine does not provide absolute protection to speakers, but rather condones controls on speech in certain contexts in both civil and criminal law. The United States Supreme Court has upheld restrictions on obscenity, child pornography, and speech that advocates unlawful conduct.<sup>50</sup> Libel laws and intellectual property laws allow individuals to use the legal system to restrain the speech of others. Prior to the growth of the Internet, a robust conversation about the limits of freedom of expression already existed in the United States. While speakers in the United States

---

<sup>48</sup> Alessandro Acquisti, Roger Dingledine, & Paul Syverson, *On the Economics of Anonymity*, FREEHAVEN.NET 2 (Jan. 2003), <http://freehaven.net/doc/fc03/econymics.pdf> (last visited Dec. 11, 2006) (explaining that “users are better off on crowded systems because of the noise other users provide.”).

<sup>49</sup> Because people in China do not enjoy a right to anonymity of communication, it is certainly possible that the government will eventually implement a surveillance system that discovers and blocks packets carrying Tor and Freenet data. However, even if this were to become technically possible, the software developers might still find methods to route around the censorship mechanism, such as by hiding the data in ordinary-looking web traffic.

<sup>50</sup> *Paris Adult Theatre I v. Slaton*, 413 U.S. 49, 57 (1973) (“[W]e hold that there are legitimate state interests at stake in stemming the tide of commercialized obscenity, even assuming it is feasible to enforce effective safeguards against exposure to juveniles and to passersby.”); *New York v. Ferber*, 458 U.S. 747 (1982) (upholding a law against child pornography); *Virginia v. Black*, 538 U.S. 343, 358-60 (2003) (describing categories of situations where government may regulate speech). See also Jonathan Zittrain, *A History of Online Gatekeeping*, 19 HARV. J.L. & TECH. 253 (2006) (describing the gatekeeping function and liability of private actors in keeping “bad” content off the Internet).

possess greater rights than do speakers in China to freely express their views, even Americans must occasionally watch what they say.

Unlike China, however, anonymous speech does have a reasonable degree of protection in the United States. The United States Supreme Court has proclaimed that “an author’s decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment.”<sup>51</sup> Also, unlike China, which requires Internet users and ISPs to register with the government, the United States government may not require individuals to inform the government about their desire to speak. One recent Supreme Court decision explained:

It is offensive—not only to the values protected by the First Amendment, but to the very notion of a free society—that in the context of everyday public discourse a citizen must first inform the government of her desire to speak to her neighbors and then obtain a permit to do so.<sup>52</sup>

Thus, in the United States, a dichotomy exists between the government’s limited right to place restrictions on speech and the general doctrine that speakers need not identify themselves to the government. Most American doctrines on the legality of speech restrictions evolved in an age before the Internet allowed any individuals to create their own worldwide soapboxes with little effort. As the American legal system has attempted to adapt its free speech doctrine to the Internet age, little attention has been paid to the possibility that broad speech restrictions—even those that are arguably necessary for the protection of American society—might have the perverse result of encouraging illegal activity by pushing that activity into the anonymous corners of the Internet where law enforcement cannot easily discover the speakers’ identities and legal process cannot locate the physical location of offending content.

Societies which respect the rule of law must draw lines to distinguish between uses of the Internet that benefit society and uses that should be stopped because they threaten the fabric of society. The difficulty with drawing such lines results from the multiple shades of gray in between, and the potential for chilling effects on speech should those lines not be drawn carefully enough. The Supreme Court has acknowledged the potential for chilling effects in laws which regulate speech on the Internet, most

---

<sup>51</sup> *McIntyre v. Ohio Elections Comm’n*, 514 U.S. 334, 342 (1995).

<sup>52</sup> *Watchtower Bible & Tract Soc’y of N.Y., Inc. v. Vill. of Stratton*, 536 U.S. 150, 165-66 (2002). Farmer, *supra* note 37, at 764-71, gives a comprehensive discussion of the right to anonymous speech.

recently in *Ashcroft v. ACLU*, where the Court struck down a federal law that prohibited speech deemed “harmful to minors” in the absence of an age verification system.<sup>53</sup> *Ashcroft*, however, was a close five to four decision. That fact, combined with recent examples of attempts to regulate speech on the Internet within the United States, suggests that efforts will continue to regulate speech.

One recent example of an attempt to regulate speech on the Internet was a law proposed by Peter Biondi, a New Jersey Assemblyman. Biondi’s proposed law would have required “an Internet service provider [to] establish, maintain and enforce a policy to require any information content provider who posts written messages on a public forum web site either to be identified by a legal name and address, or to register a legal name and address.”<sup>54</sup> Biondi introduced the legislation in response to obnoxious pseudonymous comments about politicians posted on a local Internet discussion site.<sup>55</sup> While Biondi’s law and the reasoning behind it would likely sit well with China’s Internet censors, the law’s requirement for users to register prior to criticizing their government flies in the face of well-respected Supreme Court precedent on speech critical of government and anonymous speech.<sup>56</sup>

Another example is a recent proposal by Attorney General Alberto Gonzales that would require ISPs to retain records of particular user activities for a minimum amount of time for the purpose of assisting with law enforcement investigations.<sup>57</sup> Gonzales made this proposal in light of growing recognition of the problem of child pornography and child abuse over the Internet. Gonzales gave few details about what type of records the proposed law would require ISPs to maintain, but the context strongly indicates that the law would require retention of more than basic

---

<sup>53</sup> *Ashcroft v. ACLU*, 542 U.S. 656 (2004).

<sup>54</sup> An Act Concerning the Posting of Certain Internet Messages and Supplementing Chapter 38A of Title 2A of the New Jersey Statutes, Assem. 1327, 212th Leg. (N.J. 2006).

<sup>55</sup> Declan McCullagh, *Perspective: The Problem of Thin-Skinned Politicos*, C|NET NEWS.COM, Mar. 6, 2006, [http://news.com.com/The+problem+of+thin-skinned+politicos/2010-1028\\_3-6046090.html](http://news.com.com/The+problem+of+thin-skinned+politicos/2010-1028_3-6046090.html).

<sup>56</sup> *See, e.g., Watchtower Bible*, 536 U.S. at 165-66 (upholding the right to engage in door-to-door advocacy without first registering with the government); *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964) (carefully circumscribing the definition of libel with regard to defamation of public officials).

<sup>57</sup> Anne Broache, *U.S. Attorney General Calls for ‘Reasonable’ Data Retention*, C|NET NEWS.COM, Apr. 20, 2006, [http://news.com.com/U.S.+attorney+general+calls+for+reasonable+data+retention/2100-1030\\_3-6063185.html?tag=nl](http://news.com.com/U.S.+attorney+general+calls+for+reasonable+data+retention/2100-1030_3-6063185.html?tag=nl); *see also* Declan McCullagh, *FBI Director Wants ISPs to Track Users*, C|NET NEWS.COM, Oct. 17, 2006, [http://news.com.com/FBI+director+wants+ISPs+to+track+users/2100-7348\\_3-6126877.html](http://news.com.com/FBI+director+wants+ISPs+to+track+users/2100-7348_3-6126877.html) (quoting FBI Director Robert Mueller as wanting ISPs to keep better records of user activities).

IP address information, and could reach as far as e-mail and web sites visited. Although the goal of preventing child pornography and child abuse is laudable, the means implied by Gonzales could result in a monitoring system that would rival China's Golden Shield in its ability to determine what information Internet users communicate to each other.<sup>58</sup>

What Biondi and Gonzales, amongst others, have failed to realize is that utilities like Tor and Freenet already exist, potentially rendering the proposed surveillance programs obsolete upon their inception. Gonzales specifically linked his proposal to the prevention of child abuse; the proposal intends to give law enforcement additional tools to locate child pornography on the Internet and identify those responsible for creating and circulating the material. However, unlike the average American Internet user, those responsible for child pornography are quite aware of the criminal nature of their acts and the potential for law enforcement intervention.<sup>59</sup> Sophisticated criminals frequently realize the inherent lack of privacy and security in ordinary web surfing and e-mail, and many already take steps to prevent discovery of their content and their identities.<sup>60</sup> Law enforcement has come to recognize "the growing use of sophisticated security measures and of peer-to-peer networking, where participants can share files with one another on their computers rather than downloading them off a Web site," and that child pornographers often use "encryption and data destruction software to protect the files."<sup>61</sup> In another recent case, British authorities arrested a man with the online nickname "Terrorist" who taught extremist Islamist groups "how to hack Web sites and how to use the

---

<sup>58</sup> Gonzales gave few details regarding the means behind his proposal; however, for the proposal to have actual teeth, it would probably need to monitor much more than basic IP address information of the connecting computer. Because of the lack of details, this Note will not engage in a constitutional analysis of Gonzales' proposal.

A comparison could be made, however, between the Court's striking down a requirement to register with government prior to speech in *Watchtower Bible* and any requirement that ISPs keep records of users' identities and their online speech. As at least one court has explained, even laudable police goals may have an impermissibly overbroad implementation. *Ctr. for Democracy & Tech. v. Pappert*, 337 F. Supp. 2d 606 (D. Pa. 2004).

<sup>59</sup> Gretchen Ruethling, *27 Charged in International Online Child Pornography Ring*, N.Y. TIMES, Mar. 16, 2006, at A18.

<sup>60</sup> *Id.*

<sup>61</sup> *Id.* The law enforcement officers who interviewed Christopher Soghoian, *infra* note 71, about his fake airline boarding pass generator supposedly told him that "parts of the US government . . . strongly disapprove of Tor . . . [and] thought that research universities such as IU, MIT, Georgia Tech, Harvard and others have no business supporting such projects." Christopher Soghoian, *Good News and Bad News*, <http://slightparanoia.blogspot.com/2006/11/good-news-and-bad-news.html> (Nov. 28, 2006). *But see* Onion Routing, <http://www.onion-router.net> (last visited Dec. 25, 2006) (describing the benefits and development of anonymous services such as Tor, and which claims to be "An Official U.S. Navy Web Site").

Internet securely, for example by surfing anonymously.”<sup>62</sup> Because many of those engaging in criminal activity already take steps to hide their identities and the content of their communications, broad Internet surveillance proposals may not effectively address the problem.

#### IV. REGULATION OF SPEECH VIA PUBLIC AND PRIVATE LAW

Although child pornographers and terrorists present the most troublesome examples of illegal content on the Internet, many other less despicable examples of content on the Internet have also resulted in civil litigation or criminal charges against the speakers. Many of these cases fall in a much larger gray area of appropriate speech, and government prohibition of content on the Internet could have the result of either a chilling effect on further speech or driving the questionable speech underground to places on the Internet where the law has difficulty reaching.

Governments are not the only actors that wish to remove certain information found on the Internet. Intellectual property laws provide private actors with the power to use the court system to enforce their rights against those who violate them. Since the original Napster music sharing system was shut down by court order in 2001,<sup>63</sup> file sharing has continued through other utilities. Napster was susceptible to court order by music companies and musicians because the software relied upon a central server, easily subject to legal process. As a result, software developers created more robust peer-to-peer systems, like Gnutella, which had no required centralized server, but instead relied on individual users to each become servers in a type of spider-web-like network.<sup>64</sup> In response, the musicians and media company plaintiffs started suing individual users and developers of the software itself.<sup>65</sup> These lawsuits, which have had mixed success in removing pirated content from the Internet, require accurate identification of those sharing and pirating content.<sup>66</sup>

---

<sup>62</sup> Mark Hosenball, *Hacking for Terror?*, MSNBC.COM, Mar. 15, 2006, <http://www.msnbc.msn.com/id/11847159/site/newsweek>.

<sup>63</sup> *A&M Records, Inc. v. Napster, Inc.*, 2001 U.S. Dist. LEXIS 2186 (D. Cal. Mar. 5, 2001), *aff'd*, 284 F.3d 1091 (9th Cir. 2002).

<sup>64</sup> Jerome Kuptz, *Independence Array*, WIRED MAG., Oct. 2000, *available at* <http://www.wired.com/wired/archive/8.10/architecture.html> (last visited Dec. 11, 2006).

<sup>65</sup> *MGM Studios Inc. v. Grokster, Ltd.*, 125 S. Ct. 2764 (2005), *remanded, summary judgment granted by* 2006 U.S. Dist. LEXIS 73714 (C.D. Cal. Sept. 27, 2006). Grokster lost the case because the Court found that the software deliberately induced theft of intellectual property. Because current anonymizing software has found use among Chinese dissidents and law enforcement, and is advertised for such purposes, anonymizing software has many distinct purposes beyond theft, and *Grokster's* holding may not apply.

<sup>66</sup> See Justin Hughes, *On the Logic of Suing One's Customers and the Dilemma of Infringement-*

In today's legal environment, few serious legal claims suggest that fair use allows sharing massive quantities of music and movies on the Internet. However, expensive litigation over fair use does prevent at least some dissemination of ostensibly legal content in the United States. If one uses Google to search for the term "xenu," the bottom of the search results page will reveal that "[i]n response to a complaint we received under the US Digital Millennium Copyright Act, we have removed 1 result(s) from this page." Google provides a link to a takedown request received from the Church of Scientology instructing Google to delist a set of web pages that the Church claimed violated their copyrights.<sup>67</sup> If viewers saw some of the web pages at issue, however, they would realize that the creator of these web pages intended them as a criticism of Scientology by comparing photographs and quotations from Scientologists to photographs and quotations from Adolf Hitler.<sup>68</sup> In this context, an obvious argument exists for fair use. Nevertheless, because the European owner of the web site did not want to subject himself to American legal process, he chose not to fight the delisting.<sup>69</sup>

Beyond copyright, American legal process has also been used to shut down web sites deemed to be threatening. When an anti-abortion group created a web site called "The Nuremberg Files," with information about abortion doctors, Planned Parenthood sued the group on the theory that the web site constituted a "true threat" against the lives of doctors featured on the site.<sup>70</sup> The site posted "wanted" posters of abortion doctors. If a doctor featured on the site was wounded, his name was grayed out. If a doctor was killed, then his name appeared on the site with a strike-through. The court explained its reasoning for holding that the First Amendment did not apply with a chilling description of how the

---

*Based Business Models*, 22 CARDOZO ARTS & ENT. L.J. 725 (2005) (analyzing the success of lawsuits in removing infringing content from the Internet); Jim Fitzgerald, *Piracy Suit Being Dropped Against NY Mom*, ASSOCIATED PRESS, Dec. 19, 2006 (RIAA sued a mother and her two children for file sharing, but dropped the portion of the suit against the mother after "[t]he judge called her an 'Internet-illiterate parent, who does not know Kazaa from kazoo.'"); Benny Evangelista, *RIAA Drops Claim that Grandmother Stole Online Music*, SAN FRANCISCO CHRON., Sept. 25, 2003, at B1 (RIAA dropped file sharing claim against individual who claimed that she did not own a computer capable of running file sharing software).

<sup>67</sup> Following the link leads to *Google Asked to Delist Scientology Critics (#1)*, CHILLING EFFECTS, Mar. 8, 2002, <http://www.chillingeffects.org/dmca512/notice.cgi?NoticeID=232>.

<sup>68</sup> Operation Clambake Presents: Made for Propaganda, Operation Clambake, <http://www.xenu.net/archive/photoalbum/propaganda/prop6.html> (last visited Nov. 21, 2006). It is difficult to determine with certainty that this is the web page removed from Google's results. However this is among the web sites listed in the takedown request.

<sup>69</sup> Molly Wood, *Net Effect: Church, DMCA, and Too Many Missing Links*, C|NET REVIEWS, Sept. 27, 2002, [http://reviews.cnet.com/4520-3513\\_7-5021276-1.html](http://reviews.cnet.com/4520-3513_7-5021276-1.html).

<sup>70</sup> *Planned Parenthood of the Columbia/Willamette, Inc. v. Am. Coalition of Life Activists*, 290 F.3d 1058 (9th Cir. 2002).

site operated: “After a ‘WANTED’ poster on Dr. David Gunn appeared, he was shot and killed. After a ‘WANTED’ poster on Dr. George Patterson appeared, he was shot and killed. After a ‘WANTED’ poster on Dr. John Britton appeared, he was shot and killed.”<sup>71</sup>

#### V. THE DANGERS OF SPEECH OVERREGULATION IN A WORLD WITH ANONYMOUS COMMUNICATION

These examples show that a wide variety of content and speech on the Internet is subject to legal process in the United States. Some of that content, such as child pornography, clearly displays a crime in progress. Other subject matter, such as “The Nuremberg Files,” crosses the line from advocacy of a political point of view into advocacy of murder. Still other content spans the range of intellectual property law and its fair use exception. Because software that allows double-blind communication over the Internet cannot differentiate between “good” uses and “bad” uses, the software could just as easily allow the creation of an anonymous web site for the distribution of child pornography or the planning of a terrorist attack as it could for a Chinese dissident organization or a critic of Scientology. The same technology that protects a Chinese dissident from a knock on the door in the middle of the night could also provide cover for the planning of a terrorist attack.

The question thus becomes one of how government and law enforcement should respond to the possibility that illegal activity could move from the easily monitored open Internet to

---

<sup>71</sup> *Id.* at 1085. Although the court succeeded in preventing the defendants from operating the web site in the United States, a Dutch web site decided to mirror the contents. See *Alleged Abortions and Their Accomplices*, <http://www.xs4all.nl/~oracle/nuremberg/aborts.html> (last visited Nov. 21, 2006). Karin Spink, the individual responsible for this mirror of The Nuremberg Files, claims that he vehemently disagrees with the murder of abortion doctors, but that he has made this content available online in the interest of free speech.

The futility of removing certain types of objectionable content from the Internet has also arisen in the context of airport security. Christopher Soghoian, a computer security researcher, designed a web site with software that created fake airline boarding passes. Shortly after Soghoian’s web site became public, the FBI raided his home and demanded the take-down of the boarding pass generator. Although the fake boarding passes could not be used to board an airplane, they would allow individuals to bypass the airline check-in process in order to gain access to the supposedly secure gate areas of an airport. Soghoian claims that he wrote the software to highlight an obvious and well-known weakness in airport security. Joris Evers, *DIY Boarding Pass Site Gets Shut Down*, C|NET NEWS.COM, Oct. 30, 2006, [http://news.com.com/DIY+boarding+pass+site+gets+shut+down/2100-7348\\_3-6130875.html](http://news.com.com/DIY+boarding+pass+site+gets+shut+down/2100-7348_3-6130875.html). Shortly after Soghoian was forced to take down his web site, another individual created a web site with a boarding pass generator, asking that others “[p]lease mirror this content if you are able to.” Document Generator, <http://j0hn4d4m5.bravehost.com> (last visited Dec. 12, 2006).

anonymous double-blind networks. The answer to this question lies within the fact that these anonymous networks provide the best protection against surveillance only when a large critical mass of users makes use of the software. If only a small number of individuals use anonymizing software, then those monitoring the surveillance equipment attached to the network would have reason to wonder what those specific individuals have to hide. However, as the user base grows, each additional server running distributed anonymity software adds another layer of complexity to the network, and surveillance software can only see that communication has occurred between different nodes; the surveillance equipment cannot determine the originator, content, or destination of the communication. As Tor's web site explains: "Having servers in many different places on the Internet is what makes Tor users secure. [By running a Tor server] [y]ou may also get stronger anonymity yourself, since remote sites can't know whether connections originated at your computer or were relayed from others."<sup>72</sup> As more individual users become anonymous in their communications, those communications will result in additional anonymity to all other users of the network. Such an outcome would greatly hinder the power of law enforcement to monitor the Internet, regardless of whether law enforcement works to silence critics of a totalitarian regime or towards the goal of protecting abused children.

Thus, governments that wish to maintain a useful surveillance scheme on the Internet for use by law enforcement should seek to discourage use of distributed anonymous networks. In the United States, for example, assuming that speaking anonymously on the Internet is protected by the First Amendment,<sup>73</sup> the government cannot impose an outright ban on the use of the software. Instead, governments in general should realize that Pandora's box was opened long ago, and that countries cannot accept the benefits of the Internet without accepting the increasingly freer distribution of information that has occurred with the Internet age. Because of the ease with which any individual on the Internet may become a publisher of information—whether on the open web or on an anonymous network—governments which actively

---

<sup>72</sup> Tor, Configuring a Tor Server, <http://tor.eff.org/docs/tor-doc-server.html.en> (last visited Nov. 21, 2006).

<sup>73</sup> It is beyond the scope of this Note to delve into this issue. In the United States, cases such as *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995), and *Watchtower Bible & Tract Society of New York, Inc. v. Village of Stratton*, 536 U.S. 150 (2002), strongly suggest that the United States government cannot completely prohibit anonymous communication on the Internet or require registration with the government prior to using the Internet for speech. See also Farmer, *supra* note 37, at 764-71.

attempt to suppress large amounts of content could see that content move away from the open web and open peer-to-peer networks, and onto double-blind anonymous networks. Therefore, it is in the best interests of governments to keep speech suppression to a minimum.

The case of Chinese government surveillance and suppression of speech presents the most obvious example of a situation where government over-regulation resulted in the movement of information underground, where neither illegitimate censors nor legitimate law enforcement may reach.<sup>74</sup> While this has not yet occurred in the United States, it is not hard to imagine what would occur if a software developer built software that allowed double-blind anonymous file transfers. Given the popularity of the original Napster music file sharing software and the continuing popularity of other file sharing software, music traders could easily move away from open peer-to-peer software and to anonymous networks where their true identity would remain masked from legal process. Government policy should be drawn to discourage those who desire free pirated music from using anonymous networks. Otherwise, those who share copyrighted material could provide cover for those with much worse motives.

This is not to suggest that governments should allow all speech to exist on the Internet or that musicians should not get paid for their work. Communication that presents an actual danger should remain regulated. Rather, this Note proposes that governments should carefully circumscribe the categories of regulated communication so that very few individuals actually feel any need to circumvent government surveillance via anonymity. Given that speech is “good,” “bad,” and various shades of gray in between, the current regime of suppressing some questionable speech could push much of the “gray” speech that may in fact be perfectly legal, such as the use of Scientology materials to compare

---

<sup>74</sup> Oddly enough, the United States government has given financial support to some of the anonymizing software utilities designed by Falun Gong supporters that allow Chinese Internet users to read information that their government does not want them to see and post online criticism that their government does not want them to say. The Chinese government views Falun Gong as a serious threat to social and government stability within China. See *supra* note 7. Thus, the United States participates in preventing Chinese censors from eliminating information that they see as harmful from the Internet by granting a potentially unbreakable veil of anonymity to those who participate in the distribution of that information. To put this in perspective, imagine the outcry were the Chinese government to support anonymizing software that allowed Al Qaeda members to communicate securely. The purpose of this comparison is not in any way to suggest moral equivalency between Al Qaeda and Falun Gong, but rather to point out the differences that exist between governments' views of “good” and “bad” communication. *But see* Soghoian, *supra* note 61 (individuals representing the U.S. government were concerned about research into anonymous networks like Tor).

Scientology with Adolf Hitler, onto anonymous networks. Further, because those committing serious crimes on the Internet frequently already use security and anonymity software to hide their communications, the main chilling effect will be on “gray” speech rather than communication that is truly dangerous. Because anonymous networks benefit from an increased number of users, the act of pushing “gray” speech into the anonymous zone would have the very perverse effect of assisting the “bad” speakers in the anonymity of their communication.

A recent *New York Times* article highlighted a real-world example of a law intended to prevent illegal activity that in fact made illegal activity harder to detect.<sup>75</sup> The city of Dubuque, Iowa drafted an ordinance which prohibited convicted sex offenders from living in ninety percent of the city. Many residents supported the ordinance on the theory that it would keep sex offenders away from their families. Prior to the ordinance, ninety percent of the sex offenders in Dubuque registered with police. After the ordinance passed, many sex offenders became homeless, and only half complied with the registration requirement. Because the ordinance effectively prevented these people from living in plain sight, many of them dropped out of sight and away from government surveillance that actually served a protective function.<sup>76</sup>

The lesson to be learned from Dubuque’s experience is that the goal of a law should not be to push the symbolic representation of illegal activity to the fringes, where it becomes difficult to detect and monitor, but rather to prevent the illegal activity itself. Crime is easier to detect when it is allowed to exist in plain sight; enforcement should prevent actual criminal activity and not just cause criminal speech to be swept into an anonymous speech zone. By carefully considering the potential effect of every attempt to silence communication on the Internet, government and law enforcement may realize that perhaps some gray and bad communication should be allowed to exist in a place where surveillance can occur.<sup>77</sup>

---

<sup>75</sup> Monica Davey, *Iowa’s Residency Rules Drive Sex Offenders Underground*, N.Y. TIMES, Mar. 15, 2006, at A1.

<sup>76</sup> *Id.*; see also Peter Whoriskey, *Some Curbs on Sex Offenders Called Ineffective, Inhumane*, WASH. POST, Nov. 22, 2006, at A1 (“Most predators are mobile, after all, and by upending their lives, the law may make them more likely to commit other offenses, critics say. . . . In Iowa, which in 2002 became one of the first states to impose residency restrictions, police and prosecutors have united in opposition to the law, saying that it drives offenders underground and that there is ‘no demonstrated protective effect,’ according to a statement by the Iowa County Attorneys Association, which represents prosecutors.”).

<sup>77</sup> It is beyond the scope of this Note to suggest precisely which of the examples used should be allowed to exist in plain sight. While this Note does argue that government should take a lighter hand in regulating speech on the Internet, the author also does not

## VI. CRITIQUES &amp; CONCLUSION

Some commentators have suggested that anonymity for its own sake is a worthy goal and that law enforcement should adapt to the Internet age by better gumshoe work.<sup>78</sup> There is some truth to the idea that law enforcement could make some adaptations to work in an anonymous environment. Perfect anonymity requires perfection in maintaining anonymity. A single slip-up—i.e., an accidental communication over a non-anonymous network—would break that anonymity and expose the speaker. People frequently lack the perfection necessary to maintain anonymity all the time, as evidenced by those who use an anonymous network to access Internet e-mail accounts on Yahoo and Google. Over the course of a long period of time, a user could easily make the mistake of accessing the e-mail account from a non-anonymous computer; a single mistake like this would reveal the true identity of the account's owner. Additionally, much of the activity that law enforcement seeks to prevent has real-world consequences apart from the communications over the Internet. For these consequences to occur, the perpetrators must break anonymity at some point to complete the crime. In doing so, the perpetrators lose the benefits of anonymity.<sup>79</sup>

While this theory does have some merit, the argument places freedom of speech—including communication that results in

---

believe in anarchy. Allowing the unrestrained piracy of intellectual property would work against economic incentives to creation of content and allowing anti-abortionists to incite murder could have deadly results. However, in a world where such activity could either occur in plain sight or on an anonymous network, governments must make some difficult policy choices.

One such policy choice is the right of journalists to protect their sources. After a court decision allowing the government to subpoena phone records of newspaper reporters who obtained secret information about an upcoming raid on terrorist organizations, one judge dissented, explaining:

The Court's decision also confirms the ability of journalists to protect the identities of their sources in the hands of third-party communications-service providers—in this case, one or more telephone companies. Without such protection, prosecutors, limited only by their own self-restraint, could obtain records that identify journalists' confidential sources in gross and virtually at will. Reporters might find themselves, as a matter of practical necessity, contacting sources the way I understand drug dealers reach theirs—by use of clandestine cell phones and meetings in darkened doorways. Ordinary use of the telephone could become a threat to journalist and source alike. It is difficult to see in whose best interests such a regime would operate.

N.Y. Times Co. v. Gonzales, 459 F.3d 160, 175 (2d Cir. 2006) (Sack, J., dissenting).

<sup>78</sup> One such commentator is Fred von Lohmann. Mr. von Lohmann is a senior staff attorney at the Electronic Frontier Foundation, who has written extensively on law and technology. Electronic Frontier Foundation, Fred von Lohmann, [http://www.eff.org/about/staff/?f=fred\\_von\\_lohmann.html](http://www.eff.org/about/staff/?f=fred_von_lohmann.html) (last visited Nov. 21, 2006). The suggestion about anonymity ascribed to him resulted from a conversation between Mr. von Lohmann and the author.

<sup>79</sup> One example of this is the recent British arrest of a jihadist after that individual attempted to use stolen credit cards. Hosenball, *supra* note 62.

harm—above all other concerns in a civil society. As is evident from current political events in unstable countries, societies in turmoil do not place as high a value on freedom of expression as compared to the need to fulfill physical needs and maintain order and stability within society. China, currently in the midst of a transition from a communist to a capitalist society, has begun to realize that opening the door a crack to free expression has not resulted in societal turmoil, but rather has brought economic benefits. However, even in the United States, with its robust doctrine of free expression, a large percentage of society might be unwilling to live with the Freenet credo that “[t]he true test of someone who claims to believe in Freedom of Speech is whether they tolerate speech which they disagree with, or even find disgusting”<sup>80</sup> as applied to communication that involves the creation of child pornography, assisting with terrorism, or incitement to murder abortion doctors. It’s a nice theory, but the theory must give way to the reality that there are some forms of speech that the overwhelming majority of Americans want to prevent. Rather than draw attention to the protection that anonymity provides to these types of speech, a better strategy involves encouraging government to eliminate the need for anonymity in the first place in order to make it easier for light to shine on those truly deserving of punishment.

A greater concern about encouraging governments to step back from heavy censorship of the Internet is the possibility that user apathy and unfriendly user interfaces may result in few users threatening to switch to anonymous services as governments place more restrictions on speech. One security expert has said that “[m]ost people don’t care about security and privacy until they’ve lost it.”<sup>81</sup> Even Bill Xia, who builds one of the security tools used by Chinese citizens to circumvent the Great Firewall, admits that many people are just interested in using the Internet for entertainment, fashion, and gossip, rather than free speech.<sup>82</sup> In

---

<sup>80</sup> The Free Network Project, Freenet Frequently Asked Questions, <http://freenetproject.org/faq.html> (last visited Dec. 12, 2006); see also Farmer, *supra* note 37, at 781-84 (discussing “regulation by code” from within the anonymous network rather than by government regulation from without).

<sup>81</sup> Tom Spring, *Who’s Reading Your Instant Messages?*, PCWORLD.COM, May 24, 2001, <http://pcworld.about.com/news/May242001id50984.htm>.

<sup>82</sup> Fowler, *supra* note 25. See also Bennett Haselton, *Behind the Magic of Anti-Censorship Software*, SLASHDOT, Dec. 20, 2006, <http://yro.slashdot.org/article.pl?sid=06/12/20/1336245> (“I fear . . . that the greatest weapon in [the arsenal of government censors] is not IP blocking, or keyword filtering, or even the threat of arrest. It’s just apathy.”). But see Howard W. French, *In Chinese Boomtown, Middle Class Pushes Back*, N.Y. TIMES, Dec. 18, 2006, at A1 (describing the situation in Shenzhen, China, where a growing middle class is gradually becoming more politically interested and active).

addition, the user interfaces for tools such as Freenet are sorely lacking and require technical expertise well beyond that available to an average user. For example, Freenet is so slow that it makes real-time communication almost impossible. This does not bode well for wide adoption of the software by those who have only a passing interest in anonymity.

However, user interfaces for other software like Tor have begun improving to the point where ordinary users might feel comfortable using it for regular web browsing. In addition, the Tor network has seemed to greatly increase its speed and reliability over the past two years, making it a more viable option for those who desire to “try” anonymity so long as it does not greatly impact their general Internet user experience. As the software becomes easier to use, more individuals may adopt it on a trial basis as needed to provide anonymity. This appears to have occurred in China, because hits to various types of anonymous servers have increased after major political events in China.<sup>83</sup> Although the average American user may not yet see the need for anonymous communication, recent news reports about illegal government surveillance of phone calls, Alberto Gonzales’ recommendations that ISPs preserve large amounts of data about users, and growing awareness of privacy and security violations by both governments and corporations may eventually result in a growing critical mass of users who would be willing to try anonymity software. It is this critical mass that governments should seek to prevent by ceasing the very behaviors which might move consumers in that direction.

*Eric J. Stieglitz\**

---

<sup>83</sup> French, *supra* note 82. One Beijing-based media analyst explained that the Internet in China is “driven mainly by games and chat, rather than harder political issues, but at the same time the Internet is starting to have an effect inside China, with a number of articles starting to appear on web sites about corruption and other issues, that have forced action.” Griffiths, *supra* note 18.

\* Articles Editor, *Cardozo Law Review* 2006-2007. J.D. Candidate, 2007, Benjamin N. Cardozo School of Law. Thanks to Mom, Dad, Dani, and Chavi for their love and support over all these years. Thanks to Brian E. Foont and Lois Raff for commenting on earlier versions of this Note. Thanks to Professor Susan Crawford for organizing the seminar that resulted in the original draft of this Note. ©2007 Eric J. Stieglitz.