**United States Sentencing Commission**
**Public Hearing on Proposed Amendments for 2009**
**March 17, 2009**
**Washington, D.C.**

**Prepared testimony of Seth Schoen**
**Staff Technologist, Electronic Frontier Foundation**

Chairman Hinojosa and members of the Commission, thank you for the opportunity to testify today on behalf of the Electronic Frontier Foundation (EFF). It's been some time since our organization has made a foray into sentencing policy matters, and we appreciate the opportunity to appear here.

I'm here to discuss the proposed amendments for 2009 and, in particular, the matter of the treatment of proxy servers and similar technology as "sophisticated means" by the Sentencing Guidelines.

My title at EFF is Staff Technologist, and I've held this position for seven years. I am a computer programmer and I do research on the civil liberties implications of technologies in connection with EFF litigation and try to educate the public about the intersection of technology and individual rights. EFF is a non-profit member-supported organization based in San Francisco with a staff of 29. We've existed since 1990, and we work in the courts and undertake public advocacy to defend free speech, privacy, innovation, and consumer rights in the on-line world.

## The proposed amendment and EFF's view

This year the Commission considered giving the use of a computer proxy as a specific example of technology representing a "sophisticated means" of committing a crime, representing a two-level upward sentencing adjustment under the Guidelines. The Commission has now proposed the following text[1]: "In a scheme involving computers, using any technology or software to conceal the identity or geographic location of the perpetrator ordinarily indicates sophisticated means." As I will explain, EFF opposes this amendment. In particular, these technologies are used routinely by a wide range of people for a variety of purposes, most but not all of which are unconnected to criminality. Technologies like computer proxies that may have the effect of concealing someone's identity or location do not necessarily require technical sophistication or indicate unusual expertise; they do not necessarily contribute to avoiding detecting; and they do not necessarily indicate premeditation or a commitment to a course of criminal conduct, which are all possible rationales for imposing additional incarceration for this behavior. There is no reason to consider the use of proxy technologies to be sophisticated as a general rule. We agree that the use of these technologies might sometimes indicate sophisticated means, but we think this is a case-by-case determination that can most appropriately be made by a court.

1 United States Sentencing Commission, Proposed 2009 amendment to Application Note for Sophisticated Means Enhancement under Subsection (b)(9), January 29, 2009, available at <http://www.ussc.gov/2009guid/20090127_Reader_Friendly_Proposed_Amendments.pdf>.

### What is a proxy?

Although the technologies we're discussing fall into several categories based on their technical characteristics or the purposes for which they're used, most of them could reasonably be referred to as *proxies*[2]. A computer proxy is simply a computer or software that acts *on behalf of* another computer or software. Instead of acting or communicating directly, one computer makes a request to the proxy; the proxy then carries out that request on behalf of the originating computer, and finally communicates back the results of this action. This is similar to the children's game of Telephone, where a message is passed from the beginning to the end through intermediaries and then back again[3]. The most common example is a proxy for web browsing, where an end-user's computer (instead of downloading a web page itself) asks the proxy to do so. The proxy makes the request, downloads the web page, and then sends the contents of the web page back to the requesting computer. One result of this is that the end-user's computer and the web server do communicate directly, because the whole communication is mediated by the proxy. The other party to the communication would see the request as coming from the proxy rather than from the user. As the very least, the proxy creates an extra step in identifying the user. The proxy may or may not be designed to be very good at hiding the user's true identity and location, and the design of the proxy may have nothing to do with the motivation of the person using it.

Conceptually, proxies are a very simple technology, and as I'll discuss, there are many possible reasons to use them.

### My knowledge of proxies

Proxy technologies play important roles in on-line censorship and privacy issues, which are a large part of my job at EFF. Last year I was part of a team that wrote a book called *How to Bypass Internet Censorship*, which I think is the most current hands-on reference in this area[4]. This book is intended to help users in countries where the government uses technical means to censor the Internet and inhibit the free exchange of information and ideas. Almost all of the techniques that we discuss in the book are proxies or similar techniques, and we discuss several kinds of proxies and their characteristics. We also walk people through how find proxies and how to set them up to work with popular Internet software.

EFF has also previously funded the development of Tor, which is likely the most popular anonymizing proxy network in the world, with over 100,000 regular users[5]. At that time we worked closely with the Tor developers on technical issues. Tor is no longer receiving funding from EFF, but we continue to work closely with the developers; for example, our lawyers continue to advise them.

---

2 In *How to Bypass Internet Censorshop*, we distinguished several sorts of proxy-like services, including *web proxies*, *application proxies*, and *virtual private networks* (VPNs). These distinctions are not very relevant for the purposes of this testimony because they deal primarily with technical details of how the services are implemented and accessed.

3 Computers do, however, repeat messages somewhat more faithfully than schoolchildren's whispers.

4 See *How to Bypass Internet Censorship* (FLOSS Manuals, 2008), available at <http://en.flossmanuals.net/CircumventionTools>. A printed copy may be purchased from <http://www.lulu.com/content/4904448>.

5 Tor development is coordinated by the Tor Project, Inc., a 501(c)(3) not-for-profit organization. See <http://www.torproject.org/>. The number of Tor users has been estimated by the Tor Project as “hundreds of thousands”, but can be difficult to measure precisely because users are anonymous and do not register themselves.

### Proxies in practice

The use of proxies and similar technologies is extremely widespread in practice; they form an important and basic part of computing infrastructure. One of the most familiar examples is the use of virtual private networks (VPNs), most often used by businesses to provide secure remote access to a network from anywhere in the world. A virtual private network typically hides the identity and location of a user because the user's communications, like web browsing or e-mail, would appear to originate from within a network location that is totally independent of the user's current physical location.

Another common example is an anonymizing proxy service such as Anonymizer.com, which could be provided on a commercial or volunteer basis. Such a service is most often used for protecting an Internet user's privacy[6].

The range of applications of proxies and the like is extremely broad. Here is a more comprehensive, though not exhaustive, list of ways these technologies are used every day:

- **Proxies can connect one network to another**, especially if the two networks use different technology. A familiar example today is connecting the Internet to various cell phone networks, which are generally not based on the same underlying technology as the Internet. Proxies can be used to provide Internet access to phones, or to send SMS text messages between phones and instant messaging software on PCs. One result of this is that on some networks, many different cell phone users could appear to the rest of the Internet to be using the same Internet address because all of their communications are going through the same proxy. For proxies of this sort, the use of the proxy is mandatory but invisible, and requires no special action on the part of the cell phone customer.
- **A corporate proxy** is sometimes used in conjunction with a firewall to separate internal from external network communications, for a variety of potential business reasons. It might be used to keep internal communications confidential, to reduce the demand on a business's Internet links, or to enhance the businesses ability to monitor its employee's communications, for business policy or regulatory compliance reasons. In this case the proxy is operated by the company, and all employees would use it. Again, all employees (at least at one location, and, in some designs, potentially also employees at different locations) would appear to be coming from the same single proxy address.
- I have already briefly discussed the case of **corporate VPNs**, which are used to give employees who are at home or on the road secure access to the corporate network, and which (if the users browse the web or use other Internet services while connected) would cause it to appear that they are coming from inside the corporate network, though they might be physically anywhere in the world.
- **Caching proxies** are very widespread, though they are most extensively used outside of the United States, where Internet access may be slower or more expensive. For example, they've been extremely important in Australia, a highly developed country whose Internet links to the outside world are limited by its geographic isolation. A caching proxy makes web requests on

6 These services are often marketed as means of protecting consumer privacy by reducing the extent to which advertisers and large web sites can build up elaborate profiles of individual Internet users' behavior. But, as I discuss below, they are also especially useful for protecting communications from interception in an untrusted network environment.

behalf of users and then saves the results temporarily so that the same popular document does not need to be downloaded multiple times over the Internet when multiple users are interested in it. For instance, if thousands of users in Australia wanted to read the *New York Times* one morning, a caching proxy could make a single request to the *Times* and download one copy (on behalf of whoever happened to be the first user to try to read the newspaper), and then the proxy would make that same copy available to each subsequent user. It's a much more efficient use of Australia's Internet connection to download popular items into Australia only once and then have a copy available in Australia, although the *Times* then loses information about how popular the newspaper is in Australia. It would see only one request (from the proxy) and not know how many readers it represented or who or where they were[7]. Caching proxies are also used by some businesses and universities in the United States when they want to economize and make more efficient use of their networks. Sometimes the proxy operator will give the user instructions on how to use the proxy; sometimes the network is designed to automatically route users' access through the proxy without any action on their part.

- **Library proxies** are operated by many universities' and other institutions' research libraries to manage access to subscriptions to academic journals and other periodicals provided on-line. When a library purchases access to a journal, the journal operator may agree that access will be provided only to users who are coming from within the library's or university's network. However, the library has affiliated users who will want to access these resources from off-campus, so it may provide a proxy that allows registered users to visit journal and periodical web sites or access subscription-based databases[8]. When this proxy is used, it will appear to the web sites that the users are coming from on-campus even though they are physically remote, so access will be granted. (Publishers generally agree to this practice as long as the library agrees to restrict proxy access to those users with a bona fide relationship to the university; however, when a proxy is used, the publishers can no longer determine who is accessing a site or where the user is physically located.) A 2000 survey found that 71 of 74 responding libraries were using a proxy for some purpose, most often for off-site access to subscription resources or databases[9].
- **Proxies to perform monitoring or censorship** of users' communications are common in schools and businesses, and are sometimes deployed by Internet service providers or governments on the level of an entire country, like Saudi Arabia, to restrict Internet access in that country. In this case the proxy might keep records of what users view, and it might also refuse to download particular sites or particular parts of sites that the proxy operator has on a blacklist. The Internet provider might automatically and invisibly route all communications through such a proxy, or it might block direct access to the web and then give users directions for how to get limited web access by configuring their computers to use the proxy[10].

---

7 Extremely popular web sites, or sites experiencing a sudden spike in popularity, may welcome the use of caches because it reduces the load on the sites' own Internet connections. Some popular or suddenly-popular sites actively encourage the use of caching proxies such as the public proxy network Coral CDN, because these reduce the sites' network capacity demands by saving copies of popular documents elsewhere. The use of Coral would, however, reduce the sites operators' ability to learn who is viewing their sites or from where. See <http://www.coralcdn.org/>.

8 For typical examples of library proxies used for this purpose, see <http://www.lib.berkeley.edu/Help/proxy.html> (University of California, Berkeley), <http://www.library.upenn.edu/proxy/> (University of Pennsylvania), and <http://pulproxy.princeton.edu/> (Princeton University). Library proxy services continue to be common options at major research universities.

9 See Peter Murray, "Library Proxy Use Survey Results", December 11, 2000, available at <http://www.pandc.org/proxy/survey/report.html>.

10 See generally Ronald J. Deibert et al., *Access Denied: The Policy and Practice of Global Internet Filtering* (Cambridge,

- The use of **proxies to evade monitoring or censorship** is the primary topic of the book I coauthored last year. When Internet access is censored, if the censor failed to block access to proxy sites in the outside world, these can be used to make indirect requests that would be prohibited if they were made directly. Thus, accessing the Internet through a proxy can get around the blocking. There are even several examples where the U.S. government, through entities like the International Broadcasting Bureau, has funded the operation of these proxies to try to undermine foreign censorship schemes[11]. Such proxies are widely used every day to defeat the restrictions of censorship systems like the so-called "Great Firewall of China".
- Sometimes **proxies and VPNs can protect privacy** by preventing other people on one's local network from seeing what one is doing. For example, any user on a wifi network in a café or at a conference could easily record *all* the communications of any other user. This is illegal, but it is very easy to do with commonly available software and is extremely difficult to detect. So a user on a wifi network can use a proxy or VPN that encrypts communications and protects them from eavesdroppers. This is a good security precaution whenever one is using a wifi network. I've used it at conferences and meetings when there were dozens or thousands of strangers present who might have a reason to want to spy on my communications. These services might be provided on a commercial basis. In this case, concealing a user's physical location is not an intended purpose of the use of the proxy or VPN, but it is a likely effect – because the user's communications will seem to come from a single consistent proxy location regardless of where the user is physically getting network access.

We can make a few observations about these rather varied reasons to use proxies. First, many of them operate without the user's knowledge – the user may be forced to use a proxy by an Internet provider (or even a cell phone network operator), and not even know the proxy is there. Second, proxies do create another step in tracing a user because the user's communications are routed through the proxy and the user's original address or location is hidden behind the proxy. Whether this makes it ultimately easier or ultimately harder to identify the user varies, however: some proxies make it easier to identify users (because they keep detailed logs of users' identities and activities), while other proxies make it more difficult (because they keep no logs or because they encrypt their communications). The net effect depends on the design of the proxy. Third, many Internet users will, for one reason or another, use a proxy routinely, on an ongoing basis; their computers may be set up to use proxies automatically whenever they go on-line.

Finally, the anonymizing effect of a particular proxy may or may not be the reason that an individual chooses to use it. There are many legitimate reasons to use proxies. Of course, proxies provide potential benefit to criminals because they may be useful for concealing criminal behavior or making it less straightforward to track down a criminal. But this is only one of many uses of proxies. And uses of proxies are so ubiquitous that, when criminals do use proxies, they may not be doing so deliberately to hide their identity or location.

---

MA: MIT Press, 2008), portions available at <http://opennet.net/accessdenied>.

11 See, e.g., Kevin Poulsen, "U.S. Sponsors Anti-Censorship Web Service", *SecurityFocus*, August 26, 2003, available at <http://www.securityfocus.com/news/6807> (describing IBB contract with Anonymizer.com to provide proxy services to users in Iran); Peggy Lim and Anne Krishnan, "N.C. Outfit Pierces China's Firewalls: Web Users See Past Censors", *News and Observer*, February 26, 2006 , available at <http://www.newsobserver.com/689/story/411976.html> (describing Voice of America funding for DynaWeb and UltraReach to provide proxy services to users in China).

**Are proxies sophisticated?**

Now I'd like to consider the question of whether proxies are "sophisticated" and whether the use of some technology is "sophisticated means" under the Sentencing Guidelines. I think the most important point to make is that *a user need not be sophisticated in order to make use of a sophisticated technology*. People without any particular technical expertise often make use of technologies that are extremely complex from an engineering point of view. A car is sophisticated, representing a vast engineering effort, but it can be driven by a 16-year-old with a little bit of practice. Microsoft Word is sophisticated, again representing many years of programmer effort, but all kinds of computer users make use of it; they don't have to know much more than how to type. So I think there is an importance distinction between the effort that went into inventing the underlying technology and the sophistication of an individual making use of that technology. In modern life people rely on amazing inventions every day. Proxy users may simply be connecting to the Internet from work, from Australia, or through a web-based commercial proxy service no more difficult to use than visiting the Commission's website[12].

Apart from the sophistication of the user, I think that proxies are quite often *not* technologically sophisticated. The proxy concept has existed for decades and is a basic, routine part of network infrastructure. The idea of repeating a request on behalf of someone else is not a difficult idea to understand, and, as it turns out, is not a difficult idea to implement. While preparing for this testimony, I decided to try creating a proxy from scratch. This took me five minutes and about 15 lines of computer code. The resulting proxy that I wrote is not very good (it doesn't handle errors sensibly, for example), but it did work: a web browser can be made to send requests through it. My proxy can receive a request, perform that request, and send the result back to the user, and it can be used for web browsing. I don't think it is a particularly complex technical artifact.

On the other hand, there are proxy systems whose design is quite complex. The Tor proxy network, which EFF used to fund and still advises, is a good example; the inventors of Tor are real experts. Graduate students and academics are doing PhD-level research – with presentations at academic conferences every year – trying to evaluate how effectively Tor can or can't hide a user's identity[13]. This is still a subject of very active research and the people doing that research (and the programmers who work on Tor) are quite advanced. But at the same time, they've made a very substantial effort to try to ensure that the *use* of Tor is within reach of anybody – that it can be installed on a computer, and set up on a computer, and used on a regular basis – by just about anyone[14]. These efforts are apparently successful; Tor reportedly has over 100,000 regular users, and most of them are not computer experts; they may not know how Tor works and wouldn't be able to reproduce it for themselves. The book I coauthored also discusses Tor and other technologies like it; the book was aimed at people who are not experts, and we tried to show them that they could get started using even something like Tor with a few simple steps, and that this could be done in a matter of minutes. *Tor is a sophisticated technology, yet its users are not sophisticated users.*

---

12 Web-based proxies created with freely-available tools like James Marshall's CGIProxy (available from <http://www.jmarshall.com/tools/cgiproxy/>) typically require only that a user go to the proxy home page and then type in the address of a site to visit. A user need not install or configure any software or change any web browser settings.

13 See Free Haven Project, "The Free Haven Anonymity Bibliography", available at <http://www.freehaven.net/anonbib/full/date.html> (listing and summarizing academic research that tries to assess the security of proxy systems like Tor and other privacy-protecting technology under various conditions).

14 See <http://www.torproject.org/easy-download.html.en> (providing "installation bundles" that automate the installation of Tor on Microsoft Windows and MacOS X systems).

Looking at Internet history as well as current trends supports the conclusion that proxies and similar technologies are not necessarily "sophisticated means". First, because proxies are so useful, support for using a proxy has been built into every web browser for over a decade. It's simple to set up a proxy in a web browser, and the web browser documentation and other sources (like our book) explain this process in a step-by-step way. Second, developers of proxy networks and proxy tools have themselves tried to make it easy and straightforward for users to use these systems, whether they're non-commercial systems like Tor or commercial systems like Anonymizer and other offerings in the proxy and commercial VPN industries. Many proxy developers are trying to provide mass-market services and they seem to have acquired rather large, diverse, and unsophisticated user bases.

It also appears that millions of Internet users around the globe are at least intermittent proxy users because they want to access information that's been blocked by their governments. Reports from China indicate that all sorts of people make use of proxies. And there are also organizations that are trying to make this process ever easier and more routine. So however sophisticated the proxy technology may be, the sophistication involved in using it will decrease, just as has happened with other technologies. If it was ever reasonable to assume that proxy users were thereby demonstrating special technical acumen, it isn't reasonable today, and it will be even less reasonable in the future.

**Conclusion**

Proxies are a part of our network infrastructure, and there are many reasons to use them. Millions of Internet users do so regularly. It is not reasonable to assume as a general matter that proxy use (even when it has the effect of creating uncertainty about a user's identity or location) is a sophisticated means of committing a crime. The use of proxies is often not intentional or knowing; it may be basically or originally for an entirely non-criminal purpose; and it may not interfere with the identification of users (even though it may add an extra step to the process). Courts might, of course, conclude as fact-finders that a perpetrator intentionally used a proxy to hide his identity and location and that the steps taken to use that technology constituted "sophisticated means" in a particular case, but it would assume too much to establish this as a general rule. The Commission should not adopt an amendment that would encourage sentencing courts to do so.

Thank you once again for the opportunity to participate in this hearing, and I welcome any questions you may have.