

UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

CENTER FOR DEMOCRACY & TECHNOLOGY,  
et al.,

Plaintiffs,

v.

No. 03-5051

GERALD PAPPERT,

Defendant.

EXPERT REPORT OF MATT BLAZE

Background

1. I am an Associate Professor in the Department of Computer and Information Science of the University of Pennsylvania in Philadelphia, Pennsylvania. Prior to joining the department full time in January 2004, I was an Adjunct member of the faculty for six years. From 1992 to 2003, I was a Research Scientist at AT&T Labs - Research (formerly known as AT&T Bell Labs) in New Jersey. I received a Ph.D. in computer science in 1992 from Princeton University. A copy of my curriculum vitae is attached as Exhibit A to this testimony.

2. My research focuses on computer and network security, with an emphasis on the applications of cryptography (secret codes) to build secure systems and on the analysis and discovery of vulnerabilities in existing and proposed systems. For example, in 1994, I discovered a basic weakness in the US Government's proposed "Clipper" key escrow encryption system that contributed to that system's withdrawal. Other research has contributed to the standard encryption protocol used for Internet traffic (the "IPSEC" standard), one of the first encrypting "file systems" for automatically protecting stored computer data ("CFS"), methods of analyzing and enforcing trust relationships in complex systems ("Trust Management"), and the discovery last year of a basic weakness in master-keyed mechanical locks. This semester at the University of Pennsylvania I am teaching a PhD-level graduate seminar on security vulnerabilities in computers and networks.

3. I have been asked by the attorneys for the plaintiffs in this lawsuit to provide my expert opinions on (a) the nature of security threats on the Internet, (b) common techniques that are used to respond to such threats, and (c) the ultimate ineffectiveness of

what has been discussed in this case as "IP filtering," "DNS filtering," and "URL filtering" in the face of an effort by web site operators to avoid such possible methods of compliance with orders issued by the Pennsylvania Attorney General to block customers' access to URLs on the Internet.

4. This report and testimony is based on my experience in the field of Internet and network security. In addition, I have reviewed the report prepared by the Defendant's expert, Ben Stern, the direct examination of Mr. Stern, and the direct and cross examination of Mark Krause of WorldCom, Inc. For the convenience of the Court and the parties, I will use in this report the terms "IP filtering," "DNS filtering," and "URL filtering" as Mr. Stern used those terms in his report.

5. In a portion of his direct testimony before the Court, Mr. Stern asserted that child pornography web sites would easily be able to circumvent IP filtering implemented by ISPs to comply with blocking orders from the Pennsylvania Attorney General, but that DNS filtering and URL filtering would be effective methods to block access to child pornography web sites. While I agree that IP filtering is easily circumvented, I believe that Mr. Stern is incorrect in two fundamental ways: (1) to suggest that IP filtering is more vulnerable to evasion than other methods ignores the often trivial ways to evade DNS filtering and URL filtering, and (2) to suggest that any of the three methods would ultimately be effective in blocking access to child pornography web sites ignores the reality that all three methods can and very likely will be evaded by readily available techniques. The basis for my conclusions is discussed in the remainder of this report.

#### The Nature of Security Threats on the Internet

6. The task that the state of Pennsylvania seeks to require Internet Service Providers (ISPs) to carry out -- the blocking of access to specified web sites -- can be analogized to a number of security threats that ISPs routinely must combat. Arguably, the problem of blocking child pornography web sites has similarity to the problem of blocking "Spam" (unsolicited commercial e-mail messages) and "Denial-of-Service" attacks (efforts by malicious actors to shut down or interfere with lawful web sites and other network services). It is thus not surprising that the witness that the WorldCom company chose to make available to the Court was a senior engineer responsible for network security.

7. Three critical points, however, indicate that any effort to block specific child pornography sites is unlikely to succeed over the long run, and indeed may even have less chance of success than efforts to stop Spam or Denial-of-Service attacks.

8. First, as Mr. Krause characterized it, the vast majority of network security efforts are akin to an "arms race." As seen in the fights against Spam, Denial-of-Service attacks, and malicious Internet conduct more generally, when ISPs implement a defensive measure, the malicious actors respond and adapt by altering the attack somewhat to avoid the defensive measure, which leads to new defensive measures by the ISPs, which in turn

lead to new attacks (and so forth). Many network and large-scale system security problems are characterized by having no viable “fundamental” solution, and so must rely on defenses that fail to be effective against even very small changes in the attackers’ methods.

9. Second, the blocking of access to child pornography web sites is in some ways even harder to accomplish than most other security requirements because both the web sites and the web sites users are -- from a technical perspective -- using the communications protocols of the Internet exactly as intended. In other words, there is no technical abnormality or defect with the web traffic to be blocked that may allow ISPs to focus in on the traffic to be blocked. Often with Spam and Denial-of-Service attacks, one or more standardized protocols or procedures are violated, or the quantity of traffic is abnormal, and such violation or abnormality can assist the ISP in identifying malicious traffic to be blocked. With access to child pornography web sites, however, there is no inherent technical protocol violation or abnormality that might “tip off” an ISP that the traffic warrants a countermeasure.

10. Third, and most importantly, with efforts to combat Spam and Denial-of-Service attacks, ISPs can implement defensive countermeasures with the full consent and cooperation of the targets (the intended victims) of the communications. In other words, the recipients of these Internet communications do not want to receive them, and the recipients have a strong incentive to cooperate with the ISPs' countermeasures to maximize their effectiveness in thwarting the Spam or Denial-of-Service attack. In stark contrast, in the child pornography context, the ISP is being asked to block the communication between a willing sender and a willing recipient, both of which have an incentive to circumvent or avoid the blocking action imposed by the ISP. The fact that the ISPs are being asked to thwart communications that both the senders and the recipients want to succeed makes this problem much harder than most other network security problems.

11. The approach taken by the Pennsylvania statute -- of requiring ISPs in the middle of the network to block or interfere with communications between two willing Internet users -- is similar to the effort in the 1990s by the Federal government to attempt to access encrypted communications over the Internet (e.g., communications by targets of law enforcement and national security investigations). The government sought to impose technical standards on Internet and other service providers and users that would allow the government to read encrypted communications. Much of my research at that time focused on studying the technological problems inherent in these proposed standards. A fundamental technical difficulty, strikingly similar to the fundamental difficulty here, arose from the fact that third party access to encrypted communication requires interfering with communications between *cooperating* senders and recipients who need not follow the standard system. Ultimately the federal government abandoned its effort to impose encryption standards, at least partly because all the systems proposed did not work against targets who did not follow the standard.

12. Thus, the objective of having access-providing ISPs block access to child pornography web sites is one that is unlikely to be successful over the long run. There are a range of technical countermeasures discussed below that child pornography sites can easily employ, and it is very unlikely that IP filtering, DNS filtering, or URL filtering will be able to withstand modest efforts to circumvent them.

#### Common Techniques Used to Respond to Internet Security Threats

13. IP filtering (more commonly in the industry termed "null routing" or "black-hole routing") is a tool used by ISPs to combat a wide range of misconduct on the Internet, including Spam and Denial-of-Service attacks. Network security personnel routinely block access to specific IP addresses from which malicious traffic is flowing (although unlike what I understand happens with the Pennsylvania blocking orders, null routings of IP addresses for Denial-of-Service prevention are typically temporary in nature). In light of the fact that virtually all ISPs are familiar with and have experience with and facilities for IP address null routing, it is not surprising that IP filtering was the method adopted by most ISPs to comply with blocking orders in this case.

14. DNS filtering, or "DNS spoiling," is not part of an ISP's normal network security arsenal, although some specialized products to fight Spam do rely on DNS-like services that themselves use "spoiling" of a special-purpose version of a DNS database. URL filtering of World Wide Web traffic is not a tool that ISP network security personnel would commonly utilize.

#### The Ultimate Ineffectiveness of Attempts to Block Access to Web Sites

15. Mr. Stern testified that child pornography web sites could fairly easily evade IP filtering by adopting a technique by which a web sites IP address is changed very frequently. Mr. Stern further suggested that DNS filtering and URL filtering would in contrast be effective tools to block child pornography web sites.

16. I completely agree with Mr. Stern that it would be a trivial matter to evade IP filtering, using any of a variety of techniques. I also agree with the implication of Mr. Stern's testimony -- that the operators of child pornography sites would very likely take action to evade the blockings imposed by ISPs. I strongly disagree, however, with his suggestion that the situation would be any different for DNS filtering or URL filtering.

17. Ultimately, assuming that the operators of child pornography sites would take evasive actions as Mr. Stern suggests (an assumption of Mr. Stern's that I agree is quite plausible), all three blocking methods can be trivially evaded. A sampling -- by no means exhaustive -- of the methods for evasion that a web site operator could employ is set out below.

18. An operator of child pornography web sites could employ the following methods to evade IP filtering:

- frequently changing a web site's IP address;
- dynamically changing links to differing IP addresses in advertising banners;
- dynamically changing links to differing IP addresses in sexually-oriented search engines;
- operating one or more proxy servers for the use of customers;
- circulating simple instructions to customers about the use of any of the thousands of unrelated proxy servers available on the Internet (including proxy servers financed by the U.S. Government for the purpose of helping to evade censorship by the governments of China, Iran, and other repressive regimes); and
- providing to customers a small utility that directs a web browser to a dynamically changeable address.

19. An operator of child pornography web sites could employ the following methods to evade DNS filtering:

- using IP addresses in URLs;
- frequently changing a web site's URL address, and using a wide variety of methods to quickly circulate the new URL, including (a) spam; (b) dynamically changing links to differing URLs in advertising banners; (c) dynamically changing links to differing URLs in sexually-oriented search engines; (d) placement of new URLs in well-known places in newsgroups or web pages of links; and (e) seeding of new URLs returned by seeded searches in Google or any other major search engine;
- operating one or more proxy servers for the use of customers;
- circulating simple instructions to customers about the use of any of the thousands of unrelated proxy servers available on the Internet; and
- providing to customers a small utility that directs a web browser to a dynamically changeable address.

20. An operator of child pornography web sites could employ the following methods to evade URL filtering:

- using a non-standard port number;
- using "https" encryption for the front page of the web site, and then redirecting to a dynamically changing URL for all subsequent pages;
- using the FTP protocol to transmit and display web pages;
- frequently changing a web site's URL address, and using a wide variety of methods to quickly circulate the new URL, including (a) spam; (b) dynamically changing links to differing URLs in advertising banners; (c) dynamically changing links to differing URLs in sexually-oriented search engines; (d) placement of new URLs in well-known places in

- newsgroups or web pages of links; and (e) seeding of new URLs returned by seeded searches in Google or any other major search engine;
- operating one or more proxy servers for the use of customers;
- circulating simple instructions to customers about the use of any of the thousands of unrelated proxy servers available on the Internet; and
- providing to customers a small utility that directs a web browser to a dynamically changeable address.

21. In analyzing the scenarios raised by the Pennsylvania web blocking law, one can either assume that child pornography sites will not take evasive actions to avoid ISPs' blocks, or one can assume that such sites will take evasive actions. Those two alternate assumptions will yield the following results:

(a) if one assumes that child pornography sites will not take evasive action, then for the reasons that Mr. Krause explained (and because it is the most familiar and least costly available option), ISPs will most commonly choose to comply with a blocking order using IP address blocking; or

(b) if one assumes that child pornography sites will take evasive action (which, based on my experience with network security issues, is the assumption I would make), then none of the blocking methods will be effective at preventing child pornography web sites from reaching willing and interested users.

I declare under penalty of perjury that the foregoing is true and correct.

---

Matt Blaze

Executed on February 13, 2004