Testimony and Statement for the Record of

Marc Rotenberg
President, EPIC
Adjunct Professor, Georgetown University Law Center

Hearing on

"Planning for the Future of Cyber Attack Attribution"

Before the

Committee on Science and Technology
Subcommittee on Technology and Innovation
U.S. House of Representatives

July 15, 2010
2138 Rayburn House Office Building
Washington, DC

Mr. Chairman, Members of the Committee, thank you for the opportunity to appear today to discuss the topic of Cyber Security and Attribution. We appreciate your interest in this topic.[1]

My name is Marc Rotenberg. I am President of the Electronic Privacy Information Center (EPIC), a non-partisan public interest research organization established in 1994 to focus public attention on emerging privacy and civil liberties issues. Since our founding, we have had an ongoing interest in computer security, privacy, and identification. In fact, EPIC began in response to a proposal from the National Security Agency to establish a mandatory key escrow encryption standard that could have easily prevented the emergence of the Internet as a powerful force for economic growth and political change

EPIC was founded in 1994 in part to address concerns about the role of the National Security Agency in computer security policy.[2] Since then EPIC has participated in numerous public debates regarding the protection of privacy rights on the Internet and elsewhere. EPIC is currently engaged in active litigation under the Freedom of Information Act with the NSA and National Security Council regarding National Security Presidential Directive 54, a secret document that governs the NSA's current authority over cyber security policy.[3] EPIC has also been involved recently in seeking information regarding the secret cyber security program known as EINSTEIN 3.0, as well as a new secret program within the NSA called "Perfect Citizen."[4] And I have participated in scientific workshops on such topics as "eDNA," a proposal to tie every user activity to their unique DNA, developed by Admiral John Poindexter, the architect of Total Information Awareness, that was thankfully rejected.[5]

In my statement today, I will point to the risks and limitations of attempting to establish a mandatory Internet ID that may be favored by some as a way to address the risk of cyber attack. Such a proposal has significant implication for human rights and freedom online. It is not even clear that it would be constitutional to mandate such a requirement in the United States.

To be clear, there are real concerns about network security. Network vulnerabilities also have implications for privacy protection. But solutions to one problem invariably create new problems. As we learned in the early days of the Internet, a proposal to make it easier for the government to monitor network traffic will also make communications more vulnerable to criminals and other attackers. Similarly, proposals to mandate online identification will create new risks to privacy and security.

---

[1] EPIC Counsel Jared Kaprove and EPIC IPIOP clerks Matthew Lijoi, Laura Moy, Reuben Rodriguez assisted in the preparation of this statement. The views expressed are my own.

[2] *See* EPIC, *The Clipper Chip*, http://epic.org/crypto/clipper (last visited July 13, 2010).

[3] *EPIC v. NSA*, No. 10-196 (D.D.C. filed Feb. 4, 2010).

[4] *See generally* EPIC, *Cybersecurity and Privacy*, http://epic.org/privacy/cybersecurity/ (last visited July 13, 2010).

[5] John Markoff, *Surveillance Agency Weighed, but Discarded, Plan Reconfiguring the Internet,* N.Y. TIMES, Nov. 22, 2002, available at http://www.nytimes.com/2002/11/22/politics/22TRAC.html. The project description of eDNA stated:

> We envisage that all network and client resources will maintain traces of user eDNA so that the user can be uniquely identified as having visited a Web site, having started a process or having sent a packet. This way, the resources and those who use them form a virtual `crime scene' that contains evidence about the identity of the users, much the same way as a real crime scene contains DNA traces of people.

I. Internet attribution requirements have resulted in censorship and international human rights violations.

It may be that governments establish attribution requirements to address cyber security concerns. But it also clear that governments impose these requirements to track the activities of citizens and to crack down on controversial political views. We know this from our research of identity requirements for Internet use outside of the United States.[6] The risk of mandatory attribution can be seen most clearly today in China. If fact, in just the last day, the Associated Press reported on efforts in China to crack down on anonymity and mandate identification requirements.[7]

Currently, China leads the world in Internet use. Over 360 million people access the internet in China, an increase of 1,500% since the year 2000, accounting for over twenty percent of the world's online population.[8] Despite these numbers, Chinese Internet users must abide some of the strictest identification requirements to get online. By making user Internet activity appear attributable to the individual, China's regulations generate user self-censorship.

The Chinese government identifies users who access to the Internet in three ways: (1) mandatory registration requirements, (2) requirements on Internet Service Providers, and (3) regulation of Internet cafes.[9]

China first began control over individual access to the Internet in 1996, and has since revised its policies several times;[10] many of these revisions entailed requirements that users provide identification when accessing the Internet or using certain Internet services. Chinese citizens wishing to access the Internet are required to obtain a license for Internet access. They must register with the local police by providing their names, the names of their Internet service providers (ISPs), their email addresses, and any newsgroups to which they subscribe.[11] In February of 2010, the Chinese government lifted a ban on registrations of domain names ending

---

[6] *See generally* EPIC, PRIVACY AND HUMAN RIGHTS: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS (2006) [hereinafter "PRIVACY AND HUMAN RIGHTS."]

[7] Anita Chang, *China seeks to reduce Internet users' anonymity,* Associated Press, July 13, 2010, at http://www.google.com/hostednews/ap/article/ALeqM5goTlHz28jUIOSMcwiJD9mX6GVZyQD9GUI6VO0 ("A leading Chinese Internet regulator has vowed to reduce anonymity in China's portion of cyberspace, calling for requirements that people use their real names when buying a mobile phone or going online, according to a human rights group.") *See also,* Rebecca MacKinnon, *RConversation: China's Internet White Paper: networked authoritarianism in action,* June 15, 2010, http://rconversation.blogs.com/rconversation/2010/06/chinas-internet-white-paper-networked-authoritarianism.html.

[8] Internet World Stats, *Internet Users – Top 20 Countries – Internet Use*, http://www.internetworldstats.com/top20.htm (last visited July 13, 2010).

[9] See Trina K. Kissel, *License to Blog: Internet Regulation in the People's Republic of China*, 17 IND. INT'L & COMP. L. REV. 229 (2007).

[10] Kristina M. Reed, Comment, *From the Great Firewall of China to the Berlin Firewall: The Cost of Content Regulation on Internet Commerce*, 13 TRANSNAT'L LAW. 451, 462 (2000). *See also,* PRIVACY AND HUMAN RIGHTS 349-51 (2006) ("China – Monitoring of Cybercafes").

[11] *Id.*

in the ".cn" suffix, but also imposed strict new requirements for their use.[12] Now, individuals individual wishing to set up personal websites using the suffix must verify their identities with regulators and have their photograph taken.[13]

Additionally, some local and provincial Chinese authorities currently require that individuals use their real names when accessing bulletin boards, chat rooms, or IM services.[14] The requirement also extends to university settings, [15] and in July 2005, all administrators and group founders of China's largest instant messaging service, QQ were told that they must use their real names to access the service.[16] A notice from the Shenzhen Public Security Bureau declared: "This year, at various internet chat rooms in our city, there were chat groups, forums, BBS, internet SMS and various internet public information services in which there were illegal assemblies, illegal alliances and obscene behaviors being observed. In order to protect national security and preserve social stability . . . we will be conducting clean-ups on network public information services."[17]

Chinese state-licensed ISPs are required to track and store user activity.[18] ISPs must retain records on user identification, what sites the user visited, the duration of the user's visits, and the user's activity on those sites.[19] Though Chinese laws prohibit disclosure of this information generally, they make exceptions for a number of government purposes, including national security or criminal investigations.[20] Moreover, there are few formal procedures for requesting such data, and most of the time ISPs will disclose to the government an individuals internet usage and identification with just an informal request.[21]

Finally, Internet cafés in China abide by strict regulations that require them to identify their patrons.[22] Many Internet users in China rely on Internet cafés as a primary means of access.[23] All Internet cafés must install filtering software, ban minors from entering, monitor the activity of their patrons, and record patrons' identity and complete session logs for up to sixty

---

[12] Reporters Without Borders, *Internet Enemies: China*, at 3, Dec. 3, 2010, *available at* http://en.rsf.org/IMG/article_PDF/china-china-12-03-2010,36677.pdf.
[13] David Pierson, *China Steps Up Policing of New Websites*, L.A. TIMES, Feb. 25, 2010.
[14] Radio Free Asia, *China Tightens Grip on Cyberspace*, Aug. 17, 2005, http://www.rfa.org/english/news/in_depth/2005/08/17/internet_china/.
[15] *Id.*
[16] Nanfang Weekend, *Fourteen Departments United to "Purify" the Internet*, Aug. 18, 2005, translated in EastSouthWestNorth, Purifying the Chinese Internet, http://www.zonaeuropa.com/20050821_1.htm (last visited July 9, 2010). QQ has 100 million active users, including 8 million users who are founders or administrators.
[17] *Id.*
[18] *See* Open Net Initiative, Internet Filtering in China (2009), http://opennet.net/sites/opennet.net/files/ONI_China_2009.pdf at 15.
[19] *Id.*
[20] *Id.* at 14.
[21] *Id.* at 14–15.
[22] *See id.* at 15. *See also,* Jill R. Newbold, Note, *Aiding the Enemy: Imposing Liability on U.S. Corporations for Selling China Internet Tools to Restrict Human Rights*, 2003 U. ILL. J.L. TECH. & POL'Y 503, 504 (2003).
[23] *See generally,* Audra Ang, *China Wants Web News 'Civilized'*, DESERET MORNING NEWS, Sept. 26, 2005, at A4, *available at* 2005 WLNR 15133888.

days.[24] In many cities, Internet cafés are also connected by live video feeds to the local police department.[25]

The identification requirements China placed on Internet access cause users to police their own Internet usage. China's Internet users (justifiably) believe that all of Internet activity is attributable to the individual. Transgressing Chinese Internet policy is often met with harsh penalties.[26] Therefore, without anonymity, many Internet users in China steer well clear of any potentially controversial activity that might violate China's vague Internet prohibitions.

China is well known for directly filtering internet content within its borders;[27] however, the practice of attributing Internet activity to the specific user through identification requirements is even more effective in regulating Internet content than direct filtering.[28] China's identification laws are designed to make the user believe "that every bit of [her] activity is tracked."[29] Furthermore, China's enforcement of its Internet laws gives users reason to be concerned that if they violate the laws, they will be caught and the punishment will be severe.[30] Almost every internet-related imprisonment resulted from an accusation of subversion, a guilty verdict, and a two to twelve year prison sentence.[31] In this way, "[t]he manhunts for individual internet users, which often mobilize dozens of agents from the public security and state security ministries, serve as warnings for the recalcitrants and dissidents who continue to surf the internet."[32]

Given that individual users, content providers, and ISPs can all be held liable for illegal content,[33] each of these entities acts as a self-censor, avoiding, monitoring, or deleting content that might be illegal. Removing Internet anonymity and requiring identification to access the Internet means that China's "best censorship is self-censorship."[34]

In addition to China, several other countries have used Internet identification requirements to limit or control their citizens' speech. In Burma, internet cafés are required to take screenshots of their patrons' screens every five minutes, and must be able to provide every

---

[24] Open Net Initiative, *supra* note 18 at 15.
[25] *Id.*
[26] *E.g.*, Kristen Farrell, *The Big Mamas are Watching: China's Censorship of the Internet and the Strain on Freedom of Expression*, 15 MICH. ST. J. INT'L L. 577, 578–85 (2007) (describing three examples of arrests and imprisonment for internet speech).
[27] *See, e.g.,* Open Net Initiative, *supra* note 18.
[28] *See generally,* Congressional-Executive Commission on China, 2005 Annual Report, at III(e), http://www.cecc.gov/pages/annualRpt/annualRpt05/2005_3e_expression.php (last visited July 9, 2010).
[29] Tim Johnson, *In China, Sophisticated Filters Keep the Internet Near Sterile*, MCCLATCHY, July 13, 2005, http://www.mcclatchydc.com/2005/07/13/12100/in-china-sophisticated-filters.html.
[30] Congressional-Executive Commission on China, 2005 Annual Report, at III(e), *supra* note 28. *See also* Farrell, *supra* note 26; Kissel, *supra* note 9 at 243–46.
[31] *See* Bobson Wong, *The Tug-of-War for Control of China's Internet*, http://www.hrichina.org/fs/downloadables/pdf/downloadable-resources/a3_Tugofwar.2004.pdf?revision_id=8986 (last visited July 9, 2010) (describing Chinese citizens who were imprisoned for posting information on the internet).
[32] Reporters Without Borders, *Living Dangerously on the Net: Censorship and Surveillance of internet Forums*, May 12, 2003, http://www.rsf.org/article.php3?id_article=6793.
[33] *See* Open Net Initiative, *supra* note 18 at 15.
[34] Matthew Forney, *China's Web Watchers*, TIME, Oct. 3, 2005, *available at* http://www.time.com/time/magazine/article/0,9171,501051010-1112920,00.html.

user's ID number, telephone number, and address if the police request them.[35] In Egypt, Internet cafés must be licensed by the government, although what the requirements and stipulations of obtaining a license are unclear.[36] Additionally, although no formal policy demands it, Internet café owners are often coerced through licensing raids into recording customer IDs and maintaining them on file. The records are not sent to a central database.[37] In Iran, ISPs are liable for their users' activity, and are also responsible for recording all user information and IP addresses.[38] All Internet traffic is also routed through the Telecommunications Company of Iran, so it can easily be monitored.[39] In Syria, although other ISPs are available, users wishing to use the government-owned Syria Telecommunication Establishment (STE) must apply with their government issued identity card and supply their username and password.[40] Internet cafés are also heavily monitored, with café managers required to take customers' personal information (up to and including mother's and father's names) and to keep a record of what sites their customers visit. Additionally, café managers must report any overtly illegal activity.[41] Just like in China, all these identification and tracking requirements must lead to self-censorship of politically sensitive speech.

II. In the United States, a government-mandated Internet identification requirement would likely violate the First Amendment.

Anonymity is an important protection to shield the speakers of unpopular or controversial opinions. It is settled law that the First Amendment incorporates a right to speak anonymously.[42] A government mandated identity requirement would pose a significant threat to the ability of users to engage in political speech online. In order to place such a burden on the ability of individuals to express political speech, the government must show that the proposed burden is the least restrictive means of advancing an overriding state interest. Under this standard, a program to deter and investigate cyber attacks in which all users are required to identify themselves before accessing the Internet is unlikely to be constitutional in practice.

A. The First Amendment protects the right to speak anonymously online.

Anonymous and pseudonymous speech has a long history in the United States. Before the American Revolution, much political writing was distributed in the form of anonymous pamphlets and later, during the debate surrounding adoption of the Constitution, the Founders published essays under names such as "Publius," "Cato," and "Brutus."[43] In light of this history, the Supreme Court has recognized a First Amendment right to anonymous political speech.[44] As

---

[35] Reporters Without Borders, *Internet Enemies – Burma*, at 3, http://en.rsf.org/internet-enemie-burma,36676.html.
[36] *See* Eric Goldstein, et al., *False Freedom: Online Censorship in the Middle East and North Africa*, Human Rights Watch Vol. 17, No. 10(E) at 33 (2005) (hereinafter *False Freedom*).
[37] *Id.*
[38] *See False Freedom*, *supra* note 36 at 47.
[39] Open Net Initiative, *Internet Filtering in Iran, 2009*, http://opennet.net/sites/opennet.net/files/ONI_Iran_2009.pdf at 3.
[40] *False Freedom*, *supra* note 36 at 75.
[41] Reporters Without Borders, *Internet Enemies – Syria*, at 3, http://en.rsf.org/IMG/article_PDF/syria-syria-12-03-2010,36689.pdf.
[42] *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334 (1994).
[43] *See McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 368 (1994)(Thomas, J. concurring).
[44] *Id.* at 342.

the Supreme Court said in the *McIntyre* case, while this right to remain anonymous "may be abused when it shields fraudulent conduct . . . our society accords greater weight to the value of free speech than to the dangers of its misuse."[45] Courts have also recognized that in the area of speech, the interest in anonymity outweighs other competing interests, such as the interests in preventing fraud, false advertising, and libel.[46]

In the current age, the Supreme Court has recognized the important role the Internet plays as a means of communication.[47] People use the Internet for a wide range of political and social purposes.[48] Through the use of the Internet, "any person with a phone line can become a town crier with a voice that resonates further than it could from any soapbox."[49] Anonymity is an important part of Internet communication. "The 'ability to speak one's mind' on the Internet 'without the burden of the other party knowing all the facts about one's identity can foster open communication and robust debate."[50] Knowing they might face retaliation, ostracism, or embarrassment, users were forced to identify themselves before engaging in speech on the Internet might be deterred from expressing unpopular ideas or seeking sensitive information.[51] As a result of the Internet's importance as a communication tool, courts have extended the protections of the First Amendment, and specifically the right to anonymity, to online speech.[52]

B. Courts have found broad identification requirements on Internet use to violate the Constitution.

A broad requirement for all users to identify themselves before being able to access the internet would almost certainly be considered overbroad, insufficiently narrowly tailored to achieve its purpose, and unconstitutional. In *ACLU v. Miller*, the Northern District of Georgia considered a state law that criminalized knowingly transmitting data while falsely identifying oneself.[53] The state asserted that the statute's purpose was fraud prevention. The court agreed that this was a compelling interest, but held that the statute was not sufficiently narrowly tailored to achieve its purpose because the statute would apply whenever anyone falsely identified themselves, even when there was no intent to defraud or deceive. Furthermore, the court noted that "the act prohibits such protected speech as the use of false identification to avoid social

---

[45] *See id.* at 357 (citing *Abrams v. United States*, 250 U.S. 616, 630–31 (Holmes, J., dissenting)).
[46] See, e.g., *Talley v. California*, 362 U.S. 60, 65 (1960).
[47] *See Reno v. Am. Civil Liberties Union*, 521 U.S. 844, 870 (1997) (finding that Supreme Court precedent "provide[s] no basis for qualifying the level of First Amendment scrutiny that should be applied to [the Internet]").
[48] See DAVID KIRKPATRICK, THE FACEBOOK EFFECT: THE INSIDE STORY OF THE COMPANY THAT IS CONNECTING THE WORLD 1-8 (describing the use of Facebook to promote an anti-FARC group in Columbia).
[49] *Id*.
[50] *Doe v. 2theMart.com*, 140 F. Supp. 2d 1088, 1092 (W.D. Wash. 2001) (citing *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573, 578 (N.D. Cal. 1999)).
[51] *See McIntyre*, 514 U.S. at 334; *Am. Civil Liberties Union v. Miller*, 977 F. Supp. at 1230.
[52] *See e.g.*, *Sinclair v. TubeSockTedD,* 596 F. Supp. 2d 128, 132 (D.D.C. 2009) ("Generally speaking, the First Amendment protects the right to speak anonymously. Such rights to speak anonymously apply, moreover, to speech on the Interent." (citations omitted)); *Doe v. 2TheMart.com*, 140 F. Supp. 2d at 1093 (holding "the right to speak anonymously extends to speech via the Internet"); *Am. Civil Liberties Union v. Johnson*, 4 F. Supp. 2d 1029, (D.N.M. 1998) (holding that a state statute requiring website operators restrict access to indecent materials through use of a credit card, debit account, or adult access code violates the First Amendment "because it prevents people from communicating and accessing information anonymously").
[53] 977 F. Supp. 1228, 1230 (N.D. Ga. 1997)

ostracism, to prevent discrimination and harassment, and to protected privacy . . . ."[54] As a result, the court held that the statute was overbroad and unconstitutional.

Whereas *Miller* merely prevented people from falsely identifying themselves, in *Doe v. Shurtleff* the state of Utah sought to require a convicted sex offender affirmatively submit his "internet identifiers" to the state for inclusion in its sex offender registry. This would include all of the offender's email addresses, chat user names, instant messaging names, social networking pages, and passwords. Once the information was submitted, there were no restrictions on how the Department of Corrections could use or disseminate it. There were no statutory limits which prevented the Department of Corrections from "using the information to reveal the identity of a registrant who had spoken online in a non-criminal manner, or to release the information to others who wish to do so." Although he was a convicted sex offender, Doe retained his First Amendment right to speak anonymously online and the statute implicated criminal and protected speech alike.[55] Thus, the court held that the statute was not sufficiently narrowly tailored to achieve its purpose of protecting children from Internet predators and investigating online crime.[56]

These two cases show that where the government attempts to install a mandatory identification requirement without limits as to how the information can be used, the courts are likely to strike the requirement down as overbroad and unconstitutional.

C. Courts have only found Internet identification requirements to be constitutional in extremely limited circumstances involving convicted sex offenders.

The only courts that have found Internet identification requirements not to violate the Constitution have been considering extremely limited situations involving the tracking of convicted sex offenders on specific websites. The best example of this is the sequel to the *Shurtleff* decision. After the original decision, the Utah legislature went back and amended the statute requiring the sex offender to submit his Internet identifiers to include new limits on how the information could be used and disseminated. The Department of Corrections would only be able to use the information "to assist investigating sex-related crimes."[57] In accordance with Utah's Governmental Records and Management Act, they would also be able to disclose the information to the subject of the record, to anyone authorized by the subject, or when the information is subject to a court order or legislative subpoena. With these new restrictions in place, the court held that the identification requirements "no longer intruded into Doe's ability to engage in anonymous core political speech."[58] Because the information could no longer be used to monitor Doe's speech, the chilling effect on his speech was diminished and the registry was in compliance with the First Amendment.[59]

---

[54] *Id.* at 1233.
[55] *Id.* at 21.
[56] *Doe v. Shurtleff*, No. 1:08-CV-64 TC, 2008 U.S. Dist. LEXIS 73787, at *23 (D. Utah Sept. 25, 2008).
[57] *Doe v. Shurtleff*, No. 1:08-CV-64 TC, 2009 U.S. Dist. LEXIS 73955, at *5 (D. Utah Aug. 20, 2009)[hereinafter "Shurtleff II"].
[58] *See id.* at *9–10.
[59] *Id.*

In a similar case, *White v. Baker*,[60] the court struck down a requirement for sex offenders to submit all of their Internet identifiers as overbroad, however, it provided suggestions for how such a statute would pass constitutional muster. The court held that the Georgia statute at issue went wrong by requiring *all* of the offender's Internet identifiers. First, the court noted that "a regulatory scheme designed to further the state's legitimate interest in protecting children from communication enticing them into illegal sexual activity should consider how and where on the internet such communication occurs."[61] A requirement to turn over *all* Internet identifiers would include an offender's identification on blogs or on shopping websites where communication with children would be unlikely or impossible.[62] Furthermore, there were few limits as to how the information, once submitted, could be used or disseminated.[63] The statute allowed the information to be used for undefined "law enforcement purposes" and even to be disclosed to the public. This opened up the possibility that the offender's speech could be monitored by government or private citizens, disclosing protected speech that the offender chose to engage in anonymously.[64] Concluding the opinion, the court noted that, because the state had a compelling interest, it had the ability to enact regulation, provided it was sufficiently narrowly targeted at the kind of interactive communications that entice children into illegal sexual conduct and the disclosure provisions of the statute were narrowed.[65]

Investigating cyber attacks is a broad use compared to investigating sex crimes and one could easily imagine it turning into monitoring of political speech on anonymous message boards or similar communications platforms. This would be an especially prevalent concern if the government required individuals to submit all of their Internet identifiers, as in *White*. Finally, there would be the ever-present specter of a data breach in the government's database, thereby risking the exposure of the identities and activities of all Americans on the Internet. Given the difficulties in narrowly tailoring the law to meet some ill-defined interest in cyber attacks, a mandatory identification scheme for Internet use may be possible, but it would probably be unconstitutional in practice.

III. Most research makes clear that attribution techniques have significant limitations.

So far, I have described how countries will deploy Internet attribution techniques for purposes unrelated to cyber security. I have also suggested that it would be unconstitutional for the United States government to impose an identity requirement for Internet users in the United States. Still, there is a clear need in the instance of a cyber attack or other types of malicious Internet use to determine the source of an attack. As one commentator has said, "[w]ithout the fear of being caught, convicted and punished, individuals and organizations will continue to use

[60] No. 1:09-cv-151-WSD, 2010 U.S. Dist. LEXIS 25679 (N.D. Ga. Mar. 3, 2010).
[61] *Id.* at 48–49.
[62] *Id.* at 49–50.
[63] *Id.* at 50–54.
[64] *Id.* at 52.
[65] *Id.* at 55.

the Internet to conduct malicious activities."[66] But the problem is not easily solved. As Internet security expert Bruce Schneier has bluntly stated:

> Any design of the Internet must allow for anonymity. Universal identification is impossible. Even attribution -- knowing who is responsible for particular Internet packets -- is impossible. Attempting to build such a system is futile, and will only give criminals and hackers new ways to hide. . . .
>
> Attempts to banish anonymity from the Internet won't affect those savvy enough to bypass it, would cost billions, and would have only a negligible effect on security. What such attempts would do is affect the average user's access to free speech, including those who use the Internet's anonymity to survive: dissidents in Iran, China, and elsewhere.[67]

As I said earlier, improved attribution techniques may chill speech, including dissenting speech in repressive political and organizational regimes. This has been acknowledged by many of the current participants in the cyber security debate. One group stated that the absence of attribution, or "non-attribution," can be "vital to protecting radical ideas and minority views in oppressive regimes,"[68] and cautioned that the "[m]echanisms developed to facilitate attribution must enforce non-attribution for the purposes of sharing opinions and ideas."[69] Another group pointed out that attribution exposes political dissidents and whistleblowers to potential reprisals.[70] The Department of Homeland Security has itself made clear the need to balance attribution against the need for anonymity and free speech.[71]

Second, no matter how good attribution technologies are, attribution will probably still fail to identify the most sophisticated attackers. In the words of one expert group, "[w]hile anonymizers can be defeated in theory, there are numerous practical difficulties to achieving attribution when a sophisticated user desires anonymity."[72] Another commentator notes that "[s]mart hackers . . . route attacks through countries with which the target's government has poor diplomatic relations or no law enforcement cooperation, and exploit unwitting, third-party networks."[73] Because sophisticated attackers often obscure their trail by routing activities through multiple countries, complete attribution capability would require the implementation of coordinated policies on a near-impossible global scale.

---

[66] Jeffrey Hunker, Robert Hutchinson & Jonathan Margulies, *Attribution of Cyber Attacks on Process Control Systems*, *in* CRITICAL INFRASTRUCTURE PROTECTION II 87, 88 (Mauricio Papa & Sujeet Shenoi eds., 2008). [Hereinafter "CRITICAL INFRASTRUCTURE PROTECTION II."]

[67] Bruce Schneir, *Schneir on Security: Anonymity and the Internet,* Feb. 3, 2010, available at http://www.schneier.com/blog/archives/2010/02/anonymity_and_t_3.html

[68] CRITICAL INFRASTRUCTURE PROTECTION II.

[69] *Id.*

[70] MATT BISHOP, CARRIE GATES & JEFFREY HUNKER, THE SISTERHOOD OF THE TRAVELING PACKETS 4 (2009), *available at* http://www.nspw.org/papers/2009/nspw2009-gates.pdf.

[71] U.S. DEP'T OF HOMELAND SEC., A ROADMAP FOR CYBERSECURITY RESEARCH 69 (2009), *available at* http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf.

[72] Hunker, Hutchinson & Margulies, *supra* note 66, at 91.

[73] Kenneth Geers, *The Challenge of Cyber Attack Deterrence*, 26 COMP. L. SEC. REV. 298, 301 (2010).

Finally, improved attribution techniques will probably not be effective against non-state enemies, such as the al-Qaeda terrorist network. As an initial matter, non-state actors are unlikely to have access to the resources necessary to launch successful cyber attacks. As Mr. Knake has said "al-Qaeda lacks the capability and motivation to exploit . . . vulnerabilities" in our country's critical infrastructure.[74]

On the other hand, some scholars believe that terrorist groups may well have access to the sort of sophisticated computer technologies needed to conduct cybercrime.[75] Even if terrorists could get their hands on the tools needed to launch a successful cyber attack against the United States, improved attribution techniques probably wouldn't help us deter them because one of the biggest problems with non-state terrorists is that they aren't deterred by the threat of retaliation.

The National Research Council ("NRC") recently undertook an extensive review of cyber security and considered the problem of attribution in several instances.[76] The NRC identified three reasons that deterrence by retaliation may be particularly ineffective against non-state actors:

> First, a non-state group may be particularly difficult to identify. . . . Second, a non-state group is likely to have few if any information technology assets that can be targeted. Third, some groups . . . regard counterattacks as a challenge to be welcomed rather than something to be feared.[77]

The NRC concluded:

> The bottom line is that it is too strong a statement to say that plausible attribution of an adversary's cyberattack is impossible, but it is also too strong to say that definitive and certain attribution of an adversary's cyberattack will always be possible.[78]

Based on our review of the costs and benefits of attribution techniques, there are a few key points to consider:

- The attribution of cyberattacks would greatly assist in facilitating counterattacks.
- The law of war requires an attacked body to attribute the initial attack before a counterattack will be permitted.

---

[74] Robert K. Knake, Expert Brief: Cyberterrorism Hype v. Fact, http://www.cfr.org/publication/21434/cyberterrorism_hype_v_fact.html (last accessed July 13, 2010).
[75] *See*, *e.g.*, CLAY WILSON, CONG. RESEARCH SERV., BOTNETS, CYBERCRIME, AND CYBERTERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS 16 (2008), *available at* http://www.fas.org/sgp/crs/terror/RL32114.pdf; Geers, *supra* note 73, at 302.
[76] NAT'L RESEARCH COUNCIL COMM. ON OFFENSIVE INFO. WARFARE, TECHNOLOGY, POLICY, LAW AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES (William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., 2009).
[77] *Id.* at 313.
[78] *Id.* at 41.

- Improved attribution methods would probably increase the ability to deter attacks; however, deterrence would only be effective against individuals or groups who fear retaliation.
- Attribution of activities carried out over the Internet is extremely difficult, and in many cases impossible, to achieve.
- Improvements to attribution methods will most likely fail to prevent technically sophisticated attackers from hiding their identity.
- Because Internet activity may be routed through multiple countries, including those with limited network security resources, complete attribution capability will require the implementation of coordinated policies on a near-impossible global scale.
- Improved techniques for achieving attribution of Internet activities will chill dissenting speech in repressive political and organizational regimes.
- Critical infrastructure administrators ought to be more concerned about vulnerability to internal attacks than about vulnerability to attacks from the outside.

Conclusion

Steve Bellovin, another security expert, noted recently that one of risks of the new White House plan for cyber security is that it places too much emphasis on attribution.[79] As Dr. Bellovin explains:

> The fundamental premise of the proposed strategy is that our serious Internet security problems are due to lack of sufficient authentication. That is demonstrably false. The biggest problem was and is buggy code. All the authentication in the world won't stop a bad guy who goes around the authentication system, either by finding bugs exploitable before authentication is performed, finding bugs in the authentication system itself, or by hijacking your system and abusing the authenticated connection set up by the legitimate user.[80]

While I believe the White House, the Cyber Security Advisor, and the various participants in the drafting process have made an important effort to address privacy and security interests, I share Professor Bellovin's concern that too much emphasis has been placed on promoting identification.

I also believe that online identification, promoted by government, will be used for purposes unrelated to cyber security and could ultimately chill political speech and limit the growth of the Internet. Greater public participation in the development of this policy as well as a formal rulemaking on the White House proposal could help address these concerns.

Thank you for the opportunity to testify today. I will be pleased to answer your questions.

---

[79] The White House, *National Strategies for Trusted Identities in Cyberspace: Creating Options for Enhanced Online Security and Privacy (Draft),* June 25, 2010, http://www.dhs.gov/xlibrary/assets/ns_tic.pdf

[80] Steve Bellovin, SMBlog: *Comments on the National Strategy for Trusted Identities in Cyberspace*, July 11, 2010, http://www.cs.columbia.edu/~smb/blog/2010-07/2010-07-11.html