Statement for the Record of
The Electronic Privacy Information Center (EPIC)

Marc Rotenberg, EPIC President
Matthew Phillips, EPIC Appellate Advocacy Counsel
Jared Kaprove, EPIC Domestic Surveillance Counsel

Hearing on

"The Google Predicament: Transforming U.S. Cyberspace Policy to Advance Democracy, Security, and Trade"

Before the

Committee on Foreign Affairs,
U.S. House of Representatives

February 10, 2010
2172 Rayburn House Office Building
Washington, DC

Mr. Chairman, Members of the Committee, this statement was prepared for the hearing "The Google Predicament: Transforming U.S. Cyberspace Policy to Advance Democracy, Security, and Trade" to be held on February 10, 2010 before the House Committee on Foreign Affairs. We ask that it be included in the hearing record.

The Electronic Privacy Information Center (EPIC) is a non-partisan public interest research organization established in 1994 to focus public attention on emerging privacy and civil liberties issues. Indeed, EPIC was established, in part, to address concerns about the role of NSA in computer security policy.[1]

EPIC fully supports the Committee's examination of cybersecurity policy. It is important to recognize that as cybersecurity becomes more critical to U.S. firms, it is equally critical that cyberspace policy provide robust privacy protection to the customers of those firms. This statement outlines several steps that the House Committee on Foreign Affairs can take to strengthen the privacy protection of US customers whose data is collected and used by companies around the world.

I. Introduction – There is a Real Threat to User Privacy and Security

On January 12, 2010, Google announced that hackers originating from China had attacked Google's corporate infrastructure.[2] According to Google, evidence suggested "that a primary goal of the attackers was accessing the Gmail accounts of Chinese human rights activists."[3] Secretary of State Hillary Clinton issued a statement immediately following the attack: "We have been briefed by Google on these allegations, which raise very serious concerns and questions. We look to the Chinese government for an explanation. The ability to operate with confidence in cyberspace is critical in a modern society and economy."[4]

Google also stated that "at least twenty other large companies from a wide range of businesses–including the Internet, finance, technology, media and chemical sectors–have been similarly targeted."[5] The sophistication and intent of the attack make clear that cybersecurity vulnerabilities pose a real threat to U.S. firms and their customers. As security expert Bruce Schneier wrote, "some of the hackers are good . . . [they've]

---

[1] *See* EPIC, The Clipper Chip, http://epic.org/crypto/clipper.
[2] David Drummond, *A new approach to China*, The Official Google Blog, Jan. 12, 2010, http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.
[3] *Id.*
[4] Press Release, Secretary of State Hillary Clinton (Jan. 12, 2010), http://www.state.gov/secretary/rm/2010/01/135105.htm.
[5] Drummond, supra note 1.

become more sophisticated in tools and techniques. They're stealthy. They do good network reconnaissance. . . . And they discover their own vulnerabilities."[6]

In response to the attack, Google made infrastructure and architectural changes and decided to stop censoring search results on the Chinese version of Google.[7]

EPIC strongly supports Google's decision to suspend the filtering of search results. For more than a decade, we have warned that filters pose a direct threat intellectual freedom and freedom of expression. As we explained in 1999:

> Originally touted as a technological panacea that would ward off the evils of official censorship, filtering has been shown to pose its own significant threats to free expression in new communications media. Once characterized by their proponents as mere "features" or "tools," filtering and rating systems are now viewed more realistically as fundamental architectural changes that may, in fact, facilitate the suppression of speech far more effectively than national laws alone ever could. [8]

Google's decision to change course on the filter issue in China is the good news.

II. The Google-NSA Arrangement Raises Concerns

However, on February 4, 2010, the Washington Post reported that Google and the NSA had entered into a "partnership" to help analyze the attack by permitting them to "share critical information."[9] The NSA and Google have sought to maintain the secrecy of the agreement, as the Post reported that "Google and the NSA declined to comment on the partnership."[10] But, the NSA acknowledged that it has worked with the private sector on cybersecurity in the past: NSA spokeswoman Judi Emmel stated that "as part of its information-assurance mission, NSA works with a broad range of commercial partners

---

[6] Bruce Schneier, *Face-Off: Chinese Cyberattacks: Myth or Menace?*, July 2008, http://www.schneier.com/essay-227.html.
[7] *Id.*
[8] Filters &Freedom: Free Speech Perspectives on Internet Content Controls (EPIC ed.. 1999); *See also* Filters & Freedom 2.0 (EPIC ed, 2001); EPIC, "Faulty Filters: How Content Filters Block Access to Kid-Friendly Information on the Internet" (December 1997), http://epic.org/reports/filter_report.html
[9] Ellen Nakashima, *Google to enlist NSA to help it ward off cyberattacks*, Feb. 4, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR2010020304057.html.
[10] *Id.*

and research associates to ensure the availability of secure tailored solutions for Department of Defense and national security systems customers."[11]

Moreover, sources told the Post that "Google approached the NSA shortly after the attacks," and that "the NSA is reaching out to other government agencies that play key roles in the U.S. effort to defend cyberspace and might be able to help in the Google investigation."[12] According to sources, "the focus of the partnership is "building a better defense of Google's networks, or what its technicians call 'information assurance.'"[13]

The Wall Street Journal has also reported on the relationship between Google and the NSA:

> The NSA's general counsel began drafting what's known as a cooperative research and development agreement the day Google announced the [hacker attack], according to a people familiar with the investigation. The agreement was finalized within 24 hours, but the flow of information was still limited, according to a person familiar with the investigation. It allowed the NSA to examine some of the data related to the intrusion into Google's systems.
>
> Both the FBI and NSA dispatched officials to work directly with Google. Most of the information shared with NSA officials has been about the nature of the data that was stolen from Google, a person familiar with the investigation said.[14]

Similarly, the New York Times reported that "a person with direct knowledge of the agreement" informed them of the agreement, and stated that the agreement "reopens long-standing questions about the role of the agency."[15]

This relationship raises significant concerns. While we recognized that the NSA has substantial expertise in computer security, it is equally true that NSA has substantial expertise -- some would argue greater expertise – in electronic surveillance. NSA's surveillance mission covers many different dimensions, including both direct access to

---

[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] Siobhan Gorman & Jessica E. Vascellaro, *Google Working With NSA to Investigate Cyber Attack*, Wall St. J., Feb. 4, 2010, http://online.wsj.com/article/SB10001424052748704041504575044920905689954.html.
[15] John Markoff, *Google Asks Spy Agency for Help With Inquiry Into Cyberattacks*, N.Y. Times, Feb. 4, 2010, http://www.nytimes.com/2010/02/05/science/05google.html.

intelligence and also the development of techniques and standards that enable surveillance. There is the long history of NSA's involvement on encryption policy that has frequently raised alarms in the computer security community.[16]

Indeed, the entanglement of NSA and private communication providers is not a new phenomenon, and EPIC has sought for more than 15 years to inform the public about the NSA's practices and their effect on individuals' privacy, technical standards, and computer security. EPIC was established, in part, to address concerns about the role of NSA in computer security policy.[17] As far back as 1989, Marc Rotenberg, EPIC's Executive Director, testified to Congress on the specific issue of NSA involvement in encryption policy.[18] EPIC also led the effort to obtain disclosure of documents relating to the NSA's warrantless surveillance program.[19] And EPIC's Advisory Board includes numerous experts on the NSA.[20]

Similarly, in order to discover the details of the Google/NSA relationship, EPIC recently filed a request under the Freedom of Information Act (FOIA) for any records pertaining to the agreement.[21] The public has a significant interest in learning the details of the agreement in order to make informed decisions regarding their online privacy and security. The Congress also has a significant interest in this agreement, particularly considering that Google could have instead turned to the Department of Homeland Security for assistance. Google's decision to partner with the NSA suggests a reluctance to allow formal oversight of this arrangement,

We respectfully request that the Committee ask Google to make public the arrangement it has entered into with the NSA.

III. The NSA Cybersecurity Authority Should be Made Public

The secrecy surrounding the Google/NSA relationship is exacerbated by the secrecy that the NSA has erected around its basic authority to conduct cybersecurity

---

[16] *See* Whitfield Diffie & Susan Landau, Privacy on the Line: The Politics of Wiretapping and Encryption (1998).
[17] *See* EPIC, The Clipper Chip, http://epic.org/crypto/clipper.
[18] *See* Marc Rotenberg, Testimony on the Computer Security Act, Before the Subcommittee on Legislation and National Security, Committee on Government Operations, U.S. House of Representatives 2-5, May 4, 1989.
[19] *See* EPIC, Freedom of Information Act Work on the National Security Agency's Warrantless Surveillance Program, http://epic.org/privacy/nsa/foia.
[20] *See, e.g.,* James Bamford, The Puzzle Palace (1982).
[21] EPIC, Freedom of Information Act Request, *available at* http://epic.org/privacy/nsa/foia/NSA-Google_FOIA_Request.pdf.

activity. EPIC recently filed a lawsuit to compel NSA to disclose the text of National Security Presidential Directive 54, which sets forth the agency's role in cybersecurity and surveillance.[22] EPIC also sought the full text of the Comprehensive National Cybersecurity Initiative (CNCI) and any privacy policies related to either the Directive or the Initiative.[23]

The documents sought are clearly in possession of the agency. In January 2008, George W. Bush issued the Directive, but it was never released to the public.[24] Under this secret Directive, the Comprehensive National Cybersecurity Initiative (CNCI) was formed to "improve how the federal government protects sensitive information from hackers and nation states trying to break into agency networks."[25] Since the Directive was issued, the NSA has pursued policies set out in the still-secret document.[26] In fact, the Washington Post noted that the NSA, FBI and CIA, were charged with the responsibility of implementing the CNCI.[27] The March 2009 resignation letter of the former head of the DHS National Cybersecurity Center, Rod Beckstrom, confirms that the NSA did in fact gain tremendous influence over DHS cybersecurity operations. In his letter, Mr. Beckstrom asserted that the "NSA effectively controls DHS cyber efforts through . . . technology insertions, and the proposed move of two organizations under DHS (the National Protection and Programs Directorate and the National Cybersecurity Center) to a Fort Meade NSA facility."[28]

---

[22] EPIC, Freedom of Information Act Appeal, FOIA Case 58987, *available at* http://www.epic.org/foia/NSPD54_complaint.pdf.
[23] EPIC Complaint, *available at* http://www.epic.org/foia/FOIAapp112409.pdf.
[24] Jill R. Aitoro, *The Comprehensive National Cybersecurity Initiative*, NEXTGOV, June 1, 2009, http://www.nextgov.com/the_basics/tb_20090601_8569.php.
[25] Letter from Joseph I. Lieberman, Chairman, and Susan M. Collins, Ranking Member, United States Senate Committee on Homeland Security and Governmental Affairs to Michael Chertoff, Secretary, Department of Homeland Security (May 1, 2008), *available at* http://hsgac.senate.gov/public/_files/5108LiebermanCollinslettertoChertoff.pdf.
[26] Jill R. Aitoro, *The Comprehensive National Cybersecurity Initiative*, Nextgov, June 1, 2009, http://www.nextgov.com/the_basics/tb_20090601_8569.php.
[27] Ellen Nakashima, *Bush Order Expands Network Monitoring*, Wash. Post, Jan. 26, 2009, http://www.washingtonpost.com/wpdyn/content/article/2008/01/25/AR2008012503261.html
[28] Letter from Rod Beckstrom, Director, National Cybersecurity Center to Janet Napolitano, Secretary, Department of Homeland Security (March 5, 2009), *available at* http://online.wsj.com/public/resources/documents/BeckstromResignation.pdf.

President Obama's recent focus on Transparency, Participation, and Collaboration between the public and executive agencies further justifies a renewed effort to disclose such information to the public.[29] Despite the agency's possession of the documents and the President's openness initiative, NSA failed to make public the documents. Releasing the documents sought in the request would provide the opportunity for meaningful public participation in the development of new security measures that may have a significant impact on civil liberties, such as privacy. The Senate Committee on Homeland Security and Governmental Affairs recognizes that cybersecurity initiatives must include actions to ". . . reassure [the public] that efforts to secure cyber networks will be appropriately balanced with respect for privacy and civil liberties."[30]

Taken together, these developments underscore the important public interest in making available to the public the Directive that undergirds the government's policy on cyber security. Without the disclosure sought by EPIC, the government cannot meaningfully make assurances about the adequacy of privacy and civil liberties safeguards.

We respectfully request that the Committee express its support for the release of NSPD-54, which is the secret cybersecurity authority for the NSA to conduct surveillance.

IV. Encryption of Google Traffic is Critical for User Privacy

In a related cybersecurity matter, on January 13, 2010 Google set as a default the encryption of all traffic to and from its Gmail email servers.[31] In the announcement, Google stated that it had not previously made encryption the default because it "can make your mail slower since encrypted data doesn't travel across the web as quickly as unencrypted data."[32]

---

[29] Memoranda from Barack Obama, President of the United States, on Transparency and Open Government (January 21, 2009), *available at* http://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment.

[30] Letter from Lieberman & Collins, s*upra* note 5.

[31] Sam Schillace, *Default https access for Gmail*, The Official Gmail Blog, Jan. 13, 2010, http://gmailblog.blogspot.com/2010/01/default-https-access-for-gmail.html; *see* Ryan Singel, *Google Turns on Gmail Encryption to Protect Wi-Fi Users*, Wired, Jan. 13, 2010, http://www.wired.com/threatlevel/2010/01/google-turns-on-gmail-encryption-to-protect-wi-fi-users.

[32] *Id.*; *see also* Alma Whitten, *HTTPS security for web applications*, Google Online Security Blog, June 16, 2009, http://googleonlinesecurity.blogspot.com/2009/06/https-

Complete traffic encryption was available to users beginning in 2008, but was not enabled by default.[33] Due in part to the lack of encryption in Google's cloud computing services, EPIC filed a Complaint before the Federal Trade Commission on March 17, 2009, petitioning the Commission to investigate the adequacy of Google's privacy and security safeguards.[34] The Commission is reviewing EPIC's Complaint.[35] Similarly, 39 security and privacy experts wrote to Google, observing that Google users faced "a very real risk of data theft and snooping, even by unsophisticated attackers."[36]

As of 2009, Gmail had roughly 146 million monthly users.[37] Despite the cybersecurity risk to the millions of Gmail users, Google did not enable complete encryption until after the hacker attack originating from China.[38] The Washington Post reported that "Google approached the NSA shortly after the attacks."[39] The timing of Google's decision to enable traffic encryption suggests a connection between that decision and Google's relationship with the NSA regarding the hacker attacks. NSA has a long and controversial history of involvement with encryption policy.[40]

EPIC respectfully urges the Committee to investigate the connection and NSA's role, if any, in Google's decision to start encrypting Gmail, as well as whether NSA will have any ongoing role in Google's security practices.

---

security-for-web-applications.html (discussing Google's failure to encrypt all email traffic).

[33] *Id.*

[34] EPIC, *In re: Google, Inc. and Cloud Computing Services*, March 17, 2009, *available at* http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf.

[35] Letter from Eileen Harrington, Acting Director, Bureau of Consumer Protection, to Marc Rotenberg, John Verdi, and Anirban Sen (Mar. 18, 2009), http://epic.org/privacy/cloudcomputing/google/031809_ftc_ltr.pdf.

[36] Letter from 37 experts to Eric Schmidt, CEO of Google (June 16, 2009), http://www.wired.com/images_blogs/threatlevel/2009/06/google-letter-final2.pdf.

[37] Michael Arrington, *Bing Comes To Hotmail*, TechCrunch, July 9, 2009, http://www.techcrunch.com/2009/07/09/bing-comes-to-hotmail.

[38] *See* Sam Schillace, *Default https access for Gmail*, The Official Gmail Blog, Jan. 13, 2010, http://gmailblog.blogspot.com/2010/01/default-https-access-for-gmail.html.

[39] Ellen Nakashima, *Google to enlist NSA to help it ward off cyberattacks*, Wash. Post, Feb. 4, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR2010020304057.html.

[40] *See* Diffie & Landau, *supra* note 16.

V. The US Should Support the Council of Europe Privacy Convention

EPIC also urges the Committee to indicate its support for the Council of Europe Convention on Privacy. The convention, which has been adopted by both members and non-members of the Council of Europe, aims to ensure that the rights of the individual would be protected even as governments and private organizations took advantage of new systems of automation. More than forty countries have ratified the Convention, which was opened for signature on January 28, 1981.

Twenty-nine experts in privacy and technology have sent a letter to U.S. Secretary of State Hillary Clinton to urge that the United States begin the process of ratification of the Council of Europe Convention on Privacy. The letter states that "Just as communications networks can be used for good and ill, so too can computer technology."

That outlook is reflected in Secretary Clinton's recent remarks on Internet Freedom, in which she stated that "Just as steel can be used to build hospitals or machine guns, or nuclear power can either energize a city or destroy it, modern information networks and the technologies they support can be harnessed for good or for ill." Secretary Clinton also stressed the importance of freedom of expression and privacy protection as fundamental rights in the digital age and noted the ongoing importance of the Universal Declaration of Human Rights.

The letter also calls attention to the Madrid Declaration, in which civil society groups have urged countries that have not yet ratified the Council of Europe Convention to do so as soon as possible. The signatories state, "privacy is a fundamental human right. In the 21st century, it may become one of the most critical human rights of all." EPIC respectfully requests that the Committee indicate its support for both of these important international conventions.

Bank Data Sharing Agreement Implicates Privacy Interests

Finally, EPIC would like to direct the Committee's attention to the steps taken by the European Parliament to protect the privacy of European Union citizens. The United States and the European Union had entered into a temporary agreement to allow the U.S. access to European banking data.[41] According to Secretary of State Hillary Clinton and

[41] *See* Letter from Hillary Rodman Clinton, Secretary of State, and Timothy F. Geithner, Secretary of the Treasury, to Jerzy Buzek, President of the European Parliament (Feb. 5, 2010).

Secretary of the Treasury Timothy F. Geithner, the agreement is important to "common efforts" between the European Parliament and the United States to prevent terrorism.[42]

However, on February 5, the European Parliament civil liberties committee voted not to make the agreement permanent because it failed to provide sufficient privacy safeguards.[43] The President of the European Parliament, Jerzy Buzek, stated that "the European Parliament attaches high priority to ensuring that civil liberties and data protection are fully and properly safeguarded in the important fight against terrorism," and urged the Council of the European Union "fully to reflect the concerns of, and recommendations made by, the European Parliament."[44] Similarly, the incoming Justice Commissioner of the European Commission, Viviane Reding, expressed skepticism regarding the agreement: "I remain to be convinced that all these SWIFT transfers are necessary, proportionate and effective to fight terrorism."[45]

The Committee on Foreign Affairs should take into consideration the concerns expressed by the European Parliament and ensure that any agreement between the United States and the European Union provides robust privacy safeguards.

VI. Conclusion

Hostile governments and computer criminals pose a real threat to U.S. firms operating online. As cyber security becomes more critical to U.S. firms, the U.S. must also ensure the privacy and security of the *customers* of U.S. firms. A security policy that lacks a strong commitment to privacy protection will create new problems

EPIC respectfully requests the Committee to take the steps outlined in this statement, including investigating the nature of the Google/NSA relationship; urging the NSA to disclose the text of NSPD 54, as required under the FOIA; investigating the NSA's role in Google's decision to encrypt traffic; indicating its support for the Council of Europe privacy convention and the Madrid Declaration; and ensuring the bank data privacy of U.S. and European consumers.

Thank you for your consideration of these views.

---

[42] *Id*.
[43] BBC News, *Euro MPs shun bank data deal with US*, Feb. 5, 2010, http://news.bbc.co.uk/2/hi/europe/8500132.stm.
[44] Letter from Jerzy Buzek, President, European Parliament, to José Luis Zapatero, President-in-Office, Council of the European Union (Feb. 8, 2010).
[45] Peppi Kiviniemi, *EU Reding: Skeptical About Necessity Of SWIFT Agreement*, Wall St. J., Jan. 28, 2010, http://online.wsj.com/article/BT-CO-20100128-715306.html.