February 4, 2010

BY CERTIFIED MAIL

National Security Agency
Attn: FOIA/PA Office (DJP4)
9800 Savage Road, Suite 6248
Ft. George G. Meade, MD 200755-6248

RE: Freedom of Information Act Request and Request for Expedited Processing

Dear FOIA/PA Officer:

This letter constitutes a request under the Freedom of Information Act ("FOIA"), 5 U.S.C § 552, and is submitted on behalf of the Electronic Privacy Information Center ("EPIC"). EPIC seeks records in the possession of the National Security Agency ("NSA") regarding the agency's arrangements with Google on cyber security, as well as records regarding the agency's role in setting security standards for Gmail and other web-based applications.

Background

On January 12, 2010, Google announced that hackers originating from China had attacked Google's corporate infrastructure.[1] According to Google, evidence suggested "that a primary goal of the attackers was accessing the Gmail accounts of Chinese human rights activists."[2] In response, Google made infrastructure and architectural changes and decided to stop censoring search results on the Chinese version of Google.[3]

On February 4, 2010, the press reported that Google and the NSA had entered into a "partnership" to help analyze the attack by permitting them to "share critical information."[4] The Washington Post reported that "Google and the NSA declined to comment on the partnership."[5] However, the NSA acknowledged that it has worked with the private sector on cyber security 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 and research associates to ensure the availability of secure tailored solutions for Department of Defense and national security systems customers."[6]

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

[1] 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.
[2] *Id.*
[3] *Id.*
[4] 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?hpid=topnews.
[5] *Id.*
[6] *Id.*

the U.S. effort to defend cyberspace and might be able to help in the Google investigation."[7] According to sources, "the focus of the partnership is "building a better defense of Google's networks, or what its technicians call 'information assurance.'"[8]

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.[9]

In a related cyber security matter, on January 13, 2010 Google set as a default the encryption of all traffic to and from its Gmail email servers.[10] 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."[11]

Complete traffic encryption was available to users beginning in 2008, but was not enabled by default.[12] 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.[13] The Commission is reviewing EPIC's Complaint.[14] Similarly, 37 security and privacy experts wrote

---

[7] *Id.*
[8] *Id.*
[9] 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?mod=WSJ_latestheadlines.
[10] 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.
[11] *Id.*; *see also* Alma Whitten, *HTTPS security for web applications*, Google Online Security Blog, June 16, 2009, http://googleonlinesecurity.blogspot.com/2009/06/https-security-for-web-applications.html (discussing Google's failure to encrypt all email traffic).
[12] *Id.*
[13] EPIC, *In re: Google, Inc. and Cloud Computing Services*, March 17, 2009, *available at* http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf.
[14] 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.

to Google, observing that the lack of encryption exposed Google users to "a very real risk of data theft and snooping, even by unsophisticated attackers."[15]

As of 2009, Gmail had roughly 146 million monthly users.[16] Despite the cyber security risk to the millions of Gmail users, Google did not enable complete encryption until after the hacker attack originating from China.[17] The Washington Post reported that "Google approached the NSA shortly after the attacks."[18] 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.

Documents Requested

EPIC requests copies of the following agency records:

1. All records concerning an agreement or similar basis for collaboration, final or draft, between the NSA and Google regarding cyber security;

2. All records of communication between NSA and Google concerning Gmail, including but not limited to Google's decision to fail to routinely encrypt Gmail messages prior to January 13, 2010; and

3. All records of communications regarding NSA's role in Google's decision regarding the failure to routinely deploy encryption for cloud-based computing service, such as Google Docs.

Request for Expedited Processing

This request warrants expedited processing because it is made by "a person primarily engaged in disseminating information . . ." and it pertains to a matter about which there is an "urgency to inform the public about an actual or alleged federal government activity." 5 U.S.C. § 552(a)(6)(E)(v)(II).

EPIC is "primarily engaged in disseminating information." *American Civil Liberties Union v. Department of Justice*, 321 F. Supp. 2d 24, 29 n.5 (D.D.C. 2004).

Moreover, there is particular urgency for the public to obtain information about the relationship between the NSA and Google. As of 2009, Gmail had roughly 146 million monthly users, all of whom would be affected by any relationship between the NSA and Google. In less

[15] 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.
[16] Michael Arrington, *Bing Comes To Hotmail*, TechCrunch, July 9, 2009, http://www.techcrunch.com/2009/07/09/bing-comes-to-hotmail.
[17] *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.
[18] 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?hpid=topnews.

than one day, the relationship has received widespread coverage in the media.[19] In order for the public to make meaningful decisions regarding their personal data and email, it must be aware of the details of that relationship. Neither Google nor the NSA has provided information regarding their relationship. The public should be informed.

Request for "News Media" Status

EPIC is a non-profit, educational organization that routinely and systematically disseminates information to the public. EPIC is a representative of the news media. *Epic v. Dep't of Defense*, 241, F.Supp. 2d 5 (D.D.C. 2003).

Based on our status as a "news media" requester, we are entitled to receive the requested records with only duplication fees assessed. Further, because disclosure of this information will "contribute significantly to public understanding of the operations or activities of the government," as described above, any duplication fees should be waived.

Thank you for your consideration of this request. As provided in 5 U.S.C. § 552(a)(6)(E)(ii)(I). I will anticipate your determination on our request for expedited processing within ten (10) calendar days.

Sincerely,

_____
Matthew Phillips
Appellate Advocacy Counsel, EPIC

[19] *See, e.g.*, *Id.*; 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?mod=WSJ_latestheadlines; David Alexander, *Google, NSA may team up over cyberattacks: report*, Reuters, Feb. 4, 2010, http://www.reuters.com/article/idUSTRE6130M120100204.