Written by **Joe Wolverton, II, J.D.** on May 18, 2012

Is the NSA Using Google to Spy on Account Holders?

Last the week the U.S. Court of Appeals for the District of Columbia Circuit denied a Freedom of Information Act (FOIA) request filed by the Electronic Privacy Information Center (EPIC) aimed at discovering the content of all electronic correspondence between Google and the National Security Agency (NSA).

The source of the controversy was a "highly sophisticated and targeted" cyber attack targeting Gmail accounts of Chinese human rights activists in 2010.

To counter the Chinese government's hacking of its customers' accounts, Google changed Gmail's privacy settings to automatically encrypt all traffic to and from its servers.

In the days following the attacks, Google's chief legal officer, David Drummond, warned that attacks prompted the Internet behemoth to "review the feasibility of our business operations in China." Google, continued Drummond, was "no longer willing to continue censoring our results on Google.cn, and so over the next few weeks we will be discussing with the Chinese government the basis on which we could operate an unfiltered search engine within the law, if at all."

In a blog post, Drummond also wrote that other companies might have been targeted and that he was "working with the relevant U.S. authorities." It's the identity of these American "authorities" and the extent of their involvement in the Google attacks that prompted EPIC's filing of an FOIA petition.

In the petition, EPIC seeks copies of all communications between the NSA and Google regarding the latter's efforts at beefing up its cybersecurity. The NSA challenged EPIC's request by submitting a Glomar Response. In such a maneuver, the entity that is the subject of the FOIA inquiry "neither confirms nor denies" the existence of the material requested.

Named for a ship built by the Central Intelligence Agency (CIA) to covertly recover a sunken Soviet submarine, a Glomar Response typically is given in two scenarios. First, where a refusal to forward the documents would have the effect of admitting that they actually exist, thus compromising national security. Second, law enforcement agencies will give a Glomar Response when producing the requested information would stigmatize a person named in the documents being sought.

In defense of its Glomar parry, the NSA invoked Exemption 3 of FOIA and Section 6 of the National Security Agency Act, which reads in relevant part:

> [N]othing in this Act or any other law…shall be construed to require the disclosure of the organization or any function of the National Security Agency, or any information with respect to the activities thereof, or of the names, titles, salaries, or number of the persons employed by such agency.

In a 12-page decision, Circuit Court Judge Janice Brown, a George W. Bush appointee, accepted the Glomar Response and granted summary judgment for the NSA. The primary question before the three-

judge panel was whether any of the records requested by EPIC would expose "the organization or any function" of the NSA.

Curiously, the judges held (quoting an earlier decision) that "[u]ltimately, an agency's justification for invoking a FOIA exemption is sufficient if it appears 'logical' or 'plausible'" and that "NSA need not make a specific showing of potential harm to national security in order to justify withholding information under Section 6, because 'Congress has already, in enacting the statute, decided that disclosure of NSA activities is potentially harmful.'"

Such broad interpretations of the NSA Act coupled with a crippling deference to Congress guarantee that the NSA will continue to enjoy the protection of judicial cover fire for all their clandestine schemes.

Given this attitude, then, it is not surprising that the Court held that were it to overturn the lower court's ruling and authorize access to the NSA-Google correspondence, EPIC would be privy to information the NSA avers would "pose a threat to U.S. Government information systems." Thus, the Court affirmed, "NSA may take action against the threat"; in this case, that means to refuse to hand over the records requested by EPIC in its FOIA petition.

Later in the opinion, Judge Brown wrote that were she and her colleagues to overturn the District Court's ruling in favor of the NSA, then other private entities "might hesitate or decline to contact the agency, thereby hindering its Information Assurance mission."

In defense of its position, EPIC argues that there is nothing secret about the collaboration between Google and the NSA as it was "widely reported in the national media and acknowledged by the former director of the NSA."

In a footnote, the Court wrote in dictum that "NSA has never officially acknowledged a collaborative relationship with Google, and the national media are not capable of "waiving NSA's statutory authority to protect information related to its functions and activities."

The real question — and undoubtedly the true impetus behind the EPIC FOIA request — was whether the NSA was using Google as an unofficial arm of the spy organization, employing its vast resources and customer accounts to conduct warrantless (thus illegal) monitoring of email messages.

When this issue was addressed in the lower court's decision handed down by U.S. District Judge Richard Leon, the judge held that it didn't matter whether Google was spying for the NSA and even if it was, Americans had no right to know.

Furthermore, when reading between the lines of Judge Leon's decision, when it comes to pulling back the veil of secrecy shrouding the surreptitious activities of the NSA, national security concerns trump the Constitution, the Fourth Amendment, and the right of Americans to know whether their own government is violating their civil rights.

Flush from this favorable decision, the NSA is attempting to keep former employees from recovering computers seized by the government agency in 2007.

Five NSA whistleblowers — Thomas Drake, Bill Binney, J. Kirk Wiebe, Edward Loomis, and Diane Roark — were subjected to persecution and prosecution in response to their attempts to expose government abuse and corruption.

The Government Accountability Project chronicles the maltreatment of the five at the hands of the federal government:

> Binney had a gun pointed to his head as he stepped out of the shower. Drake has the dubious distinction of being the fourth person in U.S. history (and first by the Obama administration) indicted under the Espionage Act for alleged mishandling of classified information.

Rather than just return the equipment, NSA dragged its feet, forcing the five to file a lawsuit to recoup their property.

NSA answered that it couldn't just hand over the computers because agents were busy scouring the hard drives for classified data and that such an effort was an "arduous process."

Furthermore, attorneys for the NSA argued that the seized computers "cannot lawfully be returned." NSA's Deputy Chief of Staff for Signals Intelligence claimed that the information saved on even one of the hard drives could "cause exceptionally grave damage to the national security."

To the contrary, Jesselyn Radack of the nonprofit Government Accountability Project responds that "if the unreturned property contained such damning information, the Justice Department would have used it against Drake at trial, since most of the 'evidence' the government tried to introduce against him was deemed to be unclassified and caused their case to crumble."

Weary of NSA dilatory tactics and laughable excuses, the Court ordered the NSA to answer the lawsuit. With hubris typical of an agency of the federal government, the NSA filed a motion to dismiss, arguing in its brief that all the equipment still held by the NSA is classified.

In an interview conducted by a Huffington Post Politics blogger, Thomas Drake offered the following description of NSA and the cultivation of the soil of secrecy in which it grows and thrives:

> You have to remember, NSA is an institution, and it preserves its integrity before anything else. Rule number one. It's pathological. It's what I call the deep, dark side of this culture, one that has rarely been discussed. Everything is secret.

If NSA is employing Google to spy on Americans (or anyone for that matter), one wonders how dark, how deep, and how wide the conspiracy between the federal government's spy apparatus and giant Internet companies extends.