

NSA Deception Operation? Questions Surround Leaked PRISM Document's Authenticity

Was Edward Snowden spotted before he decided to leak documents, and set up by the NSA?

By [Steve Kinney](#)

Global Research, June 12, 2013

Region: [USA](#)

Theme: [Intelligence](#)

"I can't in good conscience allow the US government to destroy privacy, Internet freedom and basic liberties for people around the world with this massive surveillance machine they're secretly building." – Edward Snowden

Intelligence services have been feeding false information to known enemy informants in their own ranks for a long time, and they are very good at it.

Today, the potential whistleblower is one of the most dangerous informants an intelligence service can confront.

Was Edward Snowden spotted before he decided to leak documents, and set up by the NSA?

Substantial evidence supports the possibility that he was. Numerous questions cast doubt on the authenticity of the Power Point slide show describing PRISM, but the UK Guardian has not seen fit to release it to the public. Perhaps Glenn Greenwald should anonymously leak this file: In the words of Snowden himself, "The public needs to decide."

Was Edward Snowden under surveillance at intelligence contractor Booz Allen in advance of releasing the PRISM document?

In the wake of the Wikileaks scandals, the U.S. intelligence community has answered "Who shall watch the watchmen?" by introducing active surveillance and detailed profiling of their own analysts and contractors, looking for potential whistleblowers.[1] By his own account, Snowden often discussed perceived Agency wrongdoing with his co-workers, which suggests that he should have been profiled and flagged as a potential leaker by the NSA's internal surveillance process.

Interviewed by Glenn Greenwald, Snowden described his workplace behavior in the time leading up to his decision to leak documents:

"When you see everything, you see them on a more frequent basis and you recognize that some of these things are actually abuses, and when you talk about them in a place like this, where this is the normal state of business, people tend not to take them very seriously and move on from them. But over time that awareness of wrongdoing sort of builds up and you feel compelled to talk about it, and the more you talk about it, the more you're ignored, the more you're told it's not a problem, until eventually you realize that these things need to be determined by the public, not by somebody who is simply hired by

the government.”[2]

Questioning The Document

Classified DoD briefing files are created to meet formal style specifications and are subject to stringent internal reviews. After the publication of pages from the PRISM presentation, independent analysts were quick to notice and report substantial deficiencies in the document.[3] Others have expressed serious doubts about the PRISM slide show’s pedigree, including the NSA’s former top attorney:

“Stewart Baker, the NSA’s general counsel in the 1990s and now an attorney at Steptoe and Johnson, said he was not familiar with PRISM or similar government activity, but the leaked Powerpoint presentation sounds “flaky,” as do the initial reports.

“The Powerpoint is suffused with a kind of hype that makes it sound more like a marketing pitch than a briefing — we don’t know what its provenance is and we don’t know the full context,” Baker said. He added, referring to the Post’s coverage: “It looks rushed and it looks wrong.” – Declan McCullagh, Wired, June 7, 2013[4]

The logos of major U.S. IT and communication service providers are splashed across the top of PRISM power point slides like sponsor patches on a NASCAR driver’s jacket. Vendor logos often do appear next to product illustrations in DoD briefing documents, and are sometimes used to indicate a vendor’s position in process or procurement flow charts. But the “ad banner” format present in the leaked PRISM slides is very unusual and apparently unique to the PRISM document. All of the vendors named have vehemently denied knowledge of the PRISM program described in the slides.[5] Some of these denials, such as those by Twitter and Google, are from companies which have previously fought court battles against arbitrary disclosure of their users’ data to Federal agencies.[6]

A second PRISM?

Unclassified documents available on the Internet identify a completely different PRISM program, a powerful integrated network communications tool for Department of Homeland Security counter-terrorism crisis management. This PRISM integrates incident reporting, GPS tracking of emergency service and law enforcement vehicles, “outbound 911” public alert networks, CBN and other technical sensor data, etc. A detailed, unclassified 2004 description of the “DHS PRISM” is available at Cryptome.[7] A 2007 report from the RAND Corporation defines PRISM as a “Planning Tool for Resource Integration, Synchronization, and Management”[8]. It seems unlikely that two network-centric programs as large and different as the DHS and NSA PRISMs, both operating inside the United States, would bear the same name. Only Monty Python calls everyone Bruce “to avoid confusion.”

Would the NSA lie to us?

The National Security Administration is one of the country’s most officially secretive agencies. In the Washington press corps, its popular nicknames have included “No Such Agency” and the “Never Say Anything” agency.

It is against long standing Agency policy to comment directly on any classified matter, and

its Directors have consistently refused to confirm or deny any Agency activity when questioned by the press. But when the UK Guardian broke the story of the PRISM leak, the Director of National Intelligence promptly confirmed the document as authentic, calling the leak “reprehensible”:

“The unauthorized disclosure of information about this important and entirely legal program is reprehensible and risks important protections for the security of Americans.” – James R. Clapper, Director of National Intelligence[9]

This very unusual confirmation raises more questions about the PRISM document than it answers.

Is it possible that the PRISM leak was set up by the NSA as a deception operation in support of the Obama Administration’s ongoing wars against whistleblowers and the 4th Amendment? Documents from Federal intelligence contractor HBGary, published in 2011 by anonymous hackers, include a Power Point presentation proposing methods for attacking Wikileaks, and this document names Glenn Greenwald, who broke the PRISM story, as a specific target:

“The presentation, which has been seen by The Independent, recommends a multi-pronged assault on WikiLeaks including deliberately submitting false documents to the website to undermine its credibility, pioneering cyber attacks to expose who the leakers to WikiLeaks are and going after sympathetic journalists.

“One of those mentioned is Glenn Greenwald, a pro-WikiLeaks reporter in the US. Writing on Salon.com. Greenwald stated that his initial reaction was “to scoff at its absurdity.” – Jerome Taylor, The Independent[10]

The UK Guardian released the PRISM story on the opening day of PFC Bradley Manning’s court martial. The leaked PRISM document will certainly influence public debate on both whistleblower protections and State surveillance – and influence is one of our intelligence community’s regular daily chores. Some commentators have been very quick to present forceful talking points in favor of free and unrestrained State surveillance[11], and there is growing consensus that reports depicting PRISM as a mass domestic surveillance dragnet were a false alarm. The Washington Post, which broke the story at the same time as the UK Guardian, has walked back its position on the civil rights implications of the PRISM materials.[12] Meanwhile, it seems that everyone has forgotten about Romas/COIN.

Universal Surveillance: Romas/COIN, Odyssey and beyond

The same security breach at HBGary that revealed formal proposals to plant false leaks and target reporter Glenn Greenwald personally, also disclosed the existence of a real surveillance program with dramatically more dangerous civil liberty implications than PRISM: Romas/COIN, and its planned successor, Odyssey. Barrett Brown summarizes what is known about this program in an article on the Project PM website:

“A successful bid for the relevant contract was seen to require the combined capabilities of perhaps a dozen firms – capabilities whereby millions of conversations can be monitored and automatically analyzed, whereby a wide range of personal data can be obtained and stored in secret, and whereby

some unknown degree of information can be released to a given population through a variety of means and without any hint that the actual source is U.S. military intelligence. All this is merely in addition to whichever additional capabilities are not evident from the limited description available, with the program as a whole presumably being operated in conjunction with other surveillance and propaganda assets controlled by the U.S. and its partners.”[13]

According to its internal e-mail from 2010 and 2011, HBGary was a prime contractor coordinating bids from Google, Apple, AT&T and others to build an expanded, upgraded version of the Romas/COIN information warfare system. Minor publicity attending the naming of these high profile vendors in the HBGary documents may have inspired the NASCAR-style sponsor logos decorating the dubious PRISM slides.

When HBGary’s e-mails were disclosed, the Odyssey bid was on hold with HBGary and its partners waiting for a revision in program requirements from the DoD. Two years have passed since HBGary was preparing to bid against Northrop Grumman for the prime contractor position on the Odyssey program. Odyssey should now be completed or nearing completion.

Is it possible that the PRISM leak was intended to mislead the American people into dramatically under-estimating the real domestic surveillance capabilities of our National Security Agency? You might well think so, but this reporter could not possibly comment.

Notes

- 1) Eric Schmitt, White House Orders New Computer Security Rules, New York Times, October 6, 2011
<https://www.nytimes.com/2011/10/07/us/politics/white-house-orders-new-computer-security-rules.html>
- 2) Glenn Greenwald interviews Edward Snowden, Guardian US, Sunday 9 June 2013
<http://www.guardian.co.uk/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video>
- 3) Are the NSA’s PRISM slides photoshopped?, Top Level Telecommunications, June 7, 2013
<http://electrospace.blogspot.nl/2013/06/are-nas-prism-slides-photoshopped.html>
- 4) Declan McCullagh, “No evidence of NSA’s ‘direct access’ to tech companies”, Wired, June 7, 2013
at
http://news.cnet.com/8301-13578_3-57588337-38/no-evidence-of-nas-direct-access-to-tech-companies/
- 5) Joanna Stern, NSA PRISM: Dissecting the Tech Companies’ Adamant Denials of Involvement in Government Spying Program, ABC News, June 7, 2013
<http://abcnews.go.com/Technology/nsa-prism-dissecting-technology-companies-adamant-denial-involvement/story?id=19350095>
- 6) Declan McCullagh, Justice Department tries to force Google to hand over user data, CNET News, May 31, 2013
http://news.cnet.com/8301-13578_3-57587005-38/justice-department-tries-to-force-google-to-hand-over-user-data/

Declan McCullagh, DOJ sends order to Twitter for WikiLeaks-related account info, CNET News, January 7, 2011

http://news.cnet.com/8301-31921_3-20027893-281.html

7) MAJ Gregg Powell and COL Charles Dunn III, Homeland Security: Requirements for Installation Security Decision Support Systems, Battle Command Battle Lab (Gordon), March 21, 2004

<http://cryptome.org/2013/06/dhs-prism.pdf>

8) Carl Rhodes, Jeff Hagen, Mark Westergren, A Strategies-to-Tasks Framework for Planning and Executing Intelligence, Surveillance, and Reconnaissance (ISR) Operations, RAND Corporation, 2007

http://www.rand.org/pubs/technical_reports/TR434.html

9) James R. Clapper, Director of National Intelligence, DNI Statement on Activities Authorized Under Section 702 of FISA, June 06, 2013

<http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/869-dni-statement-on-activities-authorized-under-section-702-of-fisa>

10) Jerome Taylor, The US bank and the secret plan to destroy WikiLeaks, The Independent February 13, 2011

<http://www.independent.co.uk/news/world/americas/the-us-bank-and-the-secret-plan-to-destroy-wiki-leaks-2215059.html>

11) Tim Worstall, NSA's PRISM Sounds Like A Darn Good Idea To Me: This Is What Governments Are For, Forbes, June 7, 2011

<http://www.forbes.com/sites/timworstall/2013/06/07/nsas-prism-sounds-like-a-darn-good-idea-to-me-this-is-what-governments-are-for/>

12) Peter Weber, Is the NSA PRISM leak much less than it seems?, Yahoo! News, Jun 10, 2013

<http://news.yahoo.com/nsa-prism-leak-much-less-seems-141000562.html?.tsrc=rtlde/>

13) Barrett Brown, Romas/COIN, Project PM, <http://wiki.echelon2.org/wiki/Romas/COIN>,

See also Barrett Brown, A sinister cyber-surveillance scheme exposed, UK Guardian, June 22, 2011

<http://www.guardian.co.uk/commentisfree/cifamerica/2011/jun/22/hacking-anonymous>

Steve Kinney is an independent researcher and writer on computer and network security topics, with a long standing interest in the civil and human rights implications of Internet censorship and surveillance by State and corporate actors.

The original source of this article is Global Research

Copyright © [Steve Kinney](#), Global Research, 2013

[Comment on Global Research Articles on our Facebook page](#)

[Become a Member of Global Research](#)

Articles by: [Steve Kinney](#)

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca