From AFIO's **The Intelligencer**
Journal of U.S. Intelligence Studies
Volume 21 • Number 2 • $15 single copy price **Summer 2015**

Association of Former Intelligence Officers
7700 Leesburg Pike Ste 324
Falls Church, Virginia 22043
Web: **www.afio.com**, E-mail: **afio@afio.com**

Assessing Edward Snowden

Whistleblower, Traitor, or Spy?

by Peter C. Oleson

It has been two years since Edward Snowden, a National Security Agency (NSA) contractor, left his position in Hawai'i and flew to Hong Kong on May 18, 2013. Taking with him a massive amount of digital files – somewhere between 1.5 to 1.7 million – that he released via various journalists, Snowden set off an international discourse on electronic surveillance, the need for it, its legality and propriety, and the legality and value of his disclosures.

Is Snowden a whistleblower or something else? It depends on how one defines a "whistleblower." The *Merriam-Webster Dictionary* defines it as "a person who tells police, reporters, etc., about something (such as a crime) that has been kept secret."[1] More enlightening is what Peter B. Jubb, a lecturer in business ethics, has written: "Whistleblowing has been defined often and in differing ways...." "Whistleblowing is characterized as a dissenting act of public accusation against an organization which necessitates being disloyal to that organization." It involves an "ethical dilemma of conflicting loyalties."[2]

But Snowden presents a special case because of his employment as a government contractor and access to classified government information. Under US law, a whistleblower involves both a "protected disclosure" by a "covered employee." Was Snowden a covered employee? The law excludes those working for intelligence organizations, specifically the Central Intelligence Agency (CIA) and NSA, "and any other executive entity that the President determines primarily conducts foreign intelligence or counter-intelligence activities."[3] A protected disclosure is "[A]ny disclosure of information" that a covered employee "reasonably believes" evidences "a violation of any law, rule, or regulation" or evidences "gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety"... on the condition that the disclosure is not prohibited by law nor required to be kept secret by Executive Order.[4] Specific provisions for intelligence community whistleblowers are contained in Presidential Policy Decision-19 (October 2012) and Title VI, Intelligence Authorization Act of 2014 (July 7, 2014). Such whistleblowers are to report their information to appropriate channels that can act to remedy the situation. This includes organizational general counsels, inspectors general, or Congress.[5]

1. *www.merriam-webster.com/dictionary/whistle-blower*
2. Peter B. Jubb. "Whistleblowing: A Restrictive Definition and Interpretation," *Journal of Business Ethics* 21, 77-94, Netherlands: Kluver Academic Publications, 1999.
3. 5 USC § 2302(a)(2)(C).
4. 5 USC § 2302(b)(8)(A). See L. Paige Whitaker "The Whistleblower Protection Act: An Overview," RL33918, Washington, DC: Congressional Research Service, March 12, 2007.
5. Ibid.

So did law or Executive Order prohibit the information Snowden disclosed? As detailed below, much of the information that Snowden provided to others relates to communications intelligence. Title 18 U.S.C. § 798 specifically prohibits the revelation of classified information related to communications intelligence. Section 798 defines classified information as "(1) concerning the nature, preparation, or use of any code, cipher, or cryptographic system of the United States or any foreign government; or (2) concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for cryptographic or communication intelligence purposes; or (3) concerning the communication intelligence activities of the United States or any foreign government; or (4) obtained by the processes of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes."[6]


Laura Poitrus from *Citizenfour* documentary.

Executive Order 13526, Classified National Security Information, spells out how information is to be classified and by whom, how it is to be handled, and how it may be disclosed. Every government employee or contractor who is granted access to classified information signs Standard Form 312, Classified Information Nondisclosure Agreement, which contains in paragraph 3:

> *I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of information or last granting me a security clearance that such disclosure is permitted.*

Presumably, Snowden signed this agreement multiple times during his various employments.

So is he a whistleblower? Yes, for those who wish to disregard or have personal beliefs or motivations to thwart the law. For others, there are questions about Edward Snowden that need answers before a judgment can be made.

What has Snowden exposed? He revealed the existence of widespread electronic surveillance by the NSA and others, including by some of the US's closest allies, of telephonic and Internet data. Snowden revealed details about how the United Kingdom, Canada, Australia, and New Zealand conduct electronic surveillance, often in cooperation with NSA. Signals intelligence cooperation between these "Five Eyes" countries dates from World War II. He also revealed specific programs such as PRISM, which involved Internet companies providing NSA with access to individual accounts; Verizon's delivery of millions of telephone records daily; the ability to analyze anything done on the Internet (Project XKeyscore); the collection of massive amounts of e-mails and Instant Messaging contact lists; a program called "UPSTREAM" that gathers data as it flows past Internet connection points; also the mapping of cell phone locations, and the use of implanted 'cookies';[7] the Federal Bureau of Investigation's involvement in surveillance of US citizens via the Section 215 program;[8] and other data collection efforts.

For civil libertarians, Snowden's revelations set off a firestorm concerning "illegal" government spying on Americans in violation of the 4th Amendment and a variety of federal laws. An ACLU online petition demonstrates the attitude of some to Snowden's revelations:

> ACLU ACTION
> President Obama:
> Grant Edward Snowden Clemency Now
>
> Edward Snowden is a great American who deserves clemency for his patriotic acts. And we're proud to serve as his legal advisors.
>
> When Snowden blew the whistle on the NSA, he single-handedly reignited a global debate about government surveillance and our most fundamental rights as individuals.
>
> For more than 12 years, the ACLU has been fighting to end government surveillance that invades

6. Peter C. Oleson, *A Compilation of U.S. Espionage Laws and Related Executive Orders*, University of Maryland University College Graduate School, February 2012.

7. A 'cookie' is digital data sent to an Internet user's Web browser that can identify that user and his online actions in the future.

8. Section 215 of the Patriot Act, PL 107-56 (50 USC sec. 1861), amended the Foreign Intelligence Surveillance Act (FISA) of 1978, and was last reauthorized in 2011.

the rights and lives of millions of Americans with virtually no oversight. But several years ago, when our case against mass surveillance finally reached the Supreme Court, it was dismissed for lack of evidence of the secret programs. Snowden provided that evidence, at great personal risk.

Right now, Snowden still lives under threat—exiled in Russia far from his home and his family, and the victim of ongoing public attacks by the NSA and their surveillance allies.

Former U.S. Ambassador to the United Nations John Bolton went so far as to say that Snowden "ought to swing from a tall oak tree" for exposing the NSA's illegal programs.

Despite all this, a top NSA official opened the door to offering Snowden clemency, under certain conditions (though we firmly believe it should be unconditional). So far, President Obama hasn't agreed.

Sign the petition now and let President Obama know that the American people stand with Snowden. If tens of thousands of us join together to deliver our message as one, we have a real chance of bringing him home.[9]

NSA's director at the time, General Keith Alexander, argued that the NSA programs were not only legal but vital to US national security. Regarding the broad surveillance, Alexander argued, "It is the hornet's nest that [enables] the NSA to see threats from Pakistan and Afghanistan and around the world, share those insights with the FBI—who can look inside the United States, based on their authorities—and find out, is there something bad going to happen here?"[10] Many have either not accepted his arguments or remain skeptical of the federal government's intentions.

The Joint Chiefs of Staff chairman, General Martin Dempsey, told the BBC, "The vast majority of [the documents Snowden took] were related to our military capabilities, operations, tactics, techniques and procedures."[11] The scope of his revelations is staggering. It is likely to take years to assess them fully. And his "disclosures will reverberate for decades to come."[12]

What has been Snowden's impact?

He has done great damage to US foreign relations. Brazilian President Dilma Roussef abruptly canceled her state visit to the US in September 2013 and later, at the UN, blasted the US for spying on her and her country. Mexico protested over reported intercepts of President Felipe Calderon. A NATO ally, Turkey, expressed considerable displeasure over Snowden's revelations.

Relations with Germany were disrupted when it became known NSA intercepted Chancellor Angela Merkel's personal cell phone. As a result, German-US intelligence cooperation has been severely restricted. The Germans want all US intelligence officers in-country declared and has stated that its counterintelligence will now target the US, something not done since World War II. Germany expelled the CIA station chief in July 2014, partially because of Snowden's revelations, but also because of the exposure of a German intelligence officer on the CIA payroll.

Information that NSA intercepted European Union and UN officials' communications has resulted in a retaliatory frame of mind for some. Snowden's revelations gave European negotiators an advantage in talks for a massive trade pact with the US that included data privacy rights.[13] In August 2013, President Obama canceled a scheduled meeting with Russian President Vladimir Putin at the G-20 meeting after Putin granted Snowden temporary asylum in Russia. Some observers note that this coincided with the start of the cooling in US-Russian relations. Since then, Russia has occupied the Crimea and sent undercover "volunteers" into eastern Ukraine. On 2 July 2013, Bolivian President Evo Morales' plane departing Russia was forced to land in Vienna due to a rumor that Snowden was onboard. France and Portugal denied overflight permission for

9. *https://www.aclu.org/secure/grant_snowden_immunity*. Emphasis in the original.

10. Alexander at a November 2013 press conference inside NSA. Documents released by Snowden indicate that PRISM is "the number one source of raw intelligence used for NSA analytic reports, and accounts for 91% of the NSA's Internet traffic acquired under FISA §702 authority."

11. BBC, March 6, 2014.

12. Suzanna Andrews, Bryan Burrough, and Sarah Ellison, "The Snowden Saga," *Vanity Fair*, May 2014, 153-203.

13. Ioanna Tourkochoriti (Harvard Law School and National University of Ireland, Galway School of Law), "The Snowden Revelations, the Transatlantic Trade and Investment Partnership and the Divide between US-EU in Data Privacy Protection," *University of Arkansas at Little Rock Law Review*, Vol. 36, 161-176, July 17, 2014. *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2467829* .

Morales' plane forcing it to land in Austria. US-Bolivian relations remain hostile.[14]

Snowden's revelations have impacted others' foreign relations, not just the US. Reports that Australia, one of NSA's partners, eavesdropped on Indonesia caused respective ambassadors to be withdrawn. The United Kingdom has threatened to end intelligence cooperation with Germany if the German Parliament investigates Government Communications Headquarters (GCHQ) activities.[15] Both the United Kingdom and Canada have been criticized for eavesdropping on other nations' delegations to the G-20 meetings in 2009 and 2010. Belgium's telecommunications company and others are suing GCHQ in court.[16]

The damage to US intelligence has been extensive. Snowden leaked the identities of over 1,000 targets of US intelligence and 31,000 files revealing what US policymakers want intelligence to provide (i.e., a list revealing what the US *doesn't* know). His releases contain sufficient detail to identify US and allied intelligence officers. He revealed previously secret details of the US intelligence budget.[17]

Perhaps even more significant is the exposure of specific sources and methods and techniques US intelligence uses. Snowden has exposed how the US tracks terrorists via e-mails, social media, and cell phones. MI-5 Director General Andrew Parker warned that leaks of GCHQ methods have given terrorists "the gift they need to evade us and strike at will." The MI-5 head warned that the Snowden leaks undermined British security as concerns grow over British Islamists fighting in Syria.[18] He also revealed the hacking techniques of NSA's Tailored Access Office, the group that focuses on difficult electronic targets. Islamic State of Iraq and Syria's (ISIS) leader, Abu Bakr al-Baghdadi, has altered his communications to avoid detection.[19] Electronic eavesdropping techniques used against Al-Qaida in Iraq no longer work. National Counterterrorism Center (NCTC) Director Nicholas J. Rasmussen testified to Congress that the US has observed a "decrease in collection."[20] There is a new 7½-minute Al-Qaida video guide on the Internet on how to avoid detection based on Snowden's revelations.[21] Also posted on the Internet are details of the commercially available encryption systems that NSA has been unable to crack, e.g., Combo of TOR, CSpace, and ZRTP (a Voice over Internet Protocol [VoIP]) system resulting in some cases in a "near total loss" of access to targets of interest.[22]

Snowden has revealed that the US had penetrated China's signals intelligence (SIGINT) system and the embassies or missions (17 in total) of Brazil, Bulgaria, Colombia, the EU, France, Georgia, Greece, India, Italy, Japan, Mexico, Slovakia, South Africa, South Korea, Taiwan, Venezuela, and Vietnam. Many are allies. He has also exposed the secret cooperation between Sweden and the NSA.

The damage done by sowing dissent is insidious. In the US, Snowden's revelations have resulted in a fracturing of relationships between government and the telecommunications industry. Apple and Google are encrypting all phone data to ensure privacy, at the expense of law enforcement which, even with a court order in criminal cases, will be unable to gather digital

14. *www.washingtonpost.com/world/bolivian-presidents-plane-forced-to-land-in-austria-in-hunt-for-snowden/2013/07/03/c281c2f4-e3eb-11e2-a11e-c2ea876a8f30_story.html*.

15. GCHQ is the UK's equivalent of NSA. *http://intelnews.org/2015/02/13/01-1642/*.

16. *www.independent.co.uk/news/world/europe/liberties-groups-to-take-gchq-to-court-over-web-privacy-8857321.html* and *http://www.bbc.com/news/technology-28106815*.

17. See *http://en.wikipedia.org/wiki/Edward_Snowden#Revelations* for a fairly comprehensive listing of Snowden's revelations. Also see Barton Gellman and Greg Miller, "'Black Budget' Summary Details US Spy Network's Successes, Failures and Objectives," *Washington Post*, September 5, 2013.

18. SpyPedia, *www.cicentre.com*.

19. "ISIS Keeps Getting Better at Dodging US Spies," *The Daily Beast*, November 14, 2014.

20. National Counterterrorism Center Director Nicholas J. Rasmussen Statement for the Record Before the SSCI, Febraury 12, 2015. *www.dni.gov/index.php/newsroom/testimonies*.

21. *http://rt.com/news/224563-al-qaeda-guide-snowden/*.

22. "Inside the NSA's War on Internet Security, *SpiegelOnline*, December 28, 2014. *www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-securitya-1010361.html*.

evidence. FBI Director James Comey stated:

> *I worry that the post-Snowden wind has blown us to a place beyond reason, a place where skepticism has become unreasoned cynicism and suspicion of the authority we need to be able to enforce the laws of this country, which protect us all.*[23]

Within Europe, Snowden's revelations have turned citizens against their own security services (in Sweden, Norway, and Germany, in particular). An interesting question to ask is: In whose interest is this?

Commercial losses as a result of Snowden's actions will be enormous. Microsoft has already lost overseas customers, including the Brazilian Government. Brazil reportedly has cancelled Boeing's contract for fighters, a loss estimated at $7 billion in initial sales and as much as $20 billion over the lifetime of the fighters. Brazil has turned to Russia for its Pantsir-S1 advanced air defense equipment. IBM is spending over $1 billion for overseas data centers beyond the reach of NSA and US courts. Trade journals report a shunning of American Internet service providers and consulting firms over fear they are cooperating with, or their networks are compromised by, NSA. Bloomberg estimates future losses in cloud computing contracts alone will total $25-35 billion.[24] China has canceled McKinsey's contracts.[25] Forrester Research estimates losses of as much as $180 billion for US companies.[26]

Edward Snowden and Glenn Greenwald in *Citizenfour* documentary.

Perhaps the most significant and long-term damage from Snowden's revelations relates to the future governance of the Internet. Calls for greater national control of the Internet, if realized, may mean that the "Golden Age" of the Internet ended with Snowden. The push to nationalize the Internet inevitably means the fragmentation of the Internet by nations. Facebook founder Mark Zuckerberg commented that this would "balkanize" the Internet, creating "Splinternets."[27] Such an outcome would enhance the control by totalitarian states of dissidents or opponents to the regime.

Regardless of his motivations, clearly Snowden is one of the most damaging betrayers of secrets in US history.

But is he something other than a whistleblower? Is his being a whistleblower simply an excuse or a cover? Jubb observed that there is often a problem differentiating a whistleblower from a "corrupt individual turned informer."[28] These questions, and understanding the timeline of what he did and when, are important in any counterintelligence evaluation.

Edward Lucas, former Moscow bureau chief for *The Economist*, provides a timeline of Snowden's activities.[29] In 2004, Snowden joined the US Army, but was discharged due to injury. According to Snowden, he was in Special Forces; however, there is no public documentation supporting this claim. In 2005, he was hired as a facility guard at the University of Maryland. His computer skills landed him a job with the CIA in 2006. In March 2007, he was deployed overseas to Geneva with CIA's Global Communications Division, the unit that runs and maintains CIA's various communications systems. While stationed in Geneva, Snowden began posting comments on Ars Technica, a technology-focused Internet site with discussion forums. Snowden used the moniker "TheTrueHOOHA." Lucas describes his postings as being Libertarian rantings. According to a *New York Times* article, in 2009, Snowden's CIA supervisor in Geneva gave him a bad personnel report stating that Snowden tried to access unauthorized classified information.[30] Such behavior is a counterintelligence "red flag." In February 2009, Snowden resigned from the CIA. One former KGB officer told Britain's *Daily Mirror* that the SVR probably had been "working" Snowden since his

23. Speech to the International Association of Chiefs of Police, Orlando, FL, Oct. 27, 2014.
24. Chris Strohm, "Tech Companies Reel as NSA's Spying Tarnishes Reputations," *Bloomberg News*, July 29, 2014. *www.bloomberg.com/news/print/2014-07-29/*.
25. "China to Ditch US Consulting Firms over Suspected Espionage," *Financial Times*, May 25, 2014.
26. Steven Levy, "How the NSA almost Killed the Internet," *WIRED*, January 7, 2014.
27. Ibid.
28. Jubb, *Whistleblowing*.
29. Edward Lucas, *The Snowden Operation: Inside the West's Greatest Intelligence Disaster*, 2014. Kindle book.
30. Eric Schmitt, "CIA Warning on Snowden in '09 Said to Slip Through the Cracks," *New York Times*, October 10, 2013. *www.nytimes.com/2013/10/11/us/cia-warning-on-snowden-in-09-said-to-slip-through-the-cracks.html*.

blog postings in 2007. Ex-KGB Major Boris Karpichkov, who defected to the UK in 1998, told the tabloid *Daily Mirror* that the SVR had a recruitment dossier on Snowden, having identified him in Geneva and noted his postings on Ars Technica as a possible defector. While in Hong Kong, Snowden probably was tricked into believing Russia was the best place to go.[31] Karpichkov claims this information came from former colleagues, but this is not verified.

By February 2010, Snowden was working for Dell, an NSA contractor, in Japan. Apparently, his online activity had changed by then, as he stopped posting while at Dell. An unanswered question is: Why? One theory is that if he was recruited, Snowden probably would have been told to "cool it."

In September 2010, Snowden made an undeclared visit to India, supposedly to take a computer hacking class.[32] All personnel indoctrinated for access to sensitive intelligence have an obligation to forewarn their security offices of planned foreign travel and report upon return any suspicious contacts with foreigners. An undeclared trip is also a counterintelligence "red flag." India is known as a most permissive environment for spying and often used by the Russians. Snowden has not explained his reasons for the trip.

In December 2010, Snowden decided to become a "leaker," according to Glenn Greenwald, Snowden's favored journalist who appears to control the periodic release of classified documents.[33] However, Snowden probably decided to do so well before. Press reports indicate that government investigators believe he stole documents while at Dell in 2009. Snowden told James Bamford, an author who has written extensively about NSA, that he considered leaking as early as 2008, when he was employed by CIA in Geneva.[34]

Regardless of the date when he decided to leak information, Snowden spent many months collecting information before he reached out to any journalists. His initial attempts to contact journalists failed. In January 2013, he first made contact with Laura Poitras, an American heiress, filmmaker, and Wikileaks activist living in Berlin.[35] Through her, Snowden contacted Glenn Greenwald, a former civil rights lawyer turned activist journalist and, as described by Lucas, a "fierce critic of American corporate and government wrongdoing."[36]

By this date, Snowden was in Hawai'i with Dell, and, in March 2013, changed jobs to work for Booz-Allen Hamilton at NSA's main site in Hawaii. He was there for less than three months. On 18 May 2013, Snowden flew to Hong Kong. Poitras, Greenwald, and veteran journalist Ewen MacAskill of *The Guardian* flew to Hong Kong to interview Snowden. Word leaked out that he was there. In June 2013, Sarah Harrison, Wikileaks founder Julian Assange's assistant, flew to Hong Kong to provide Snowden legal advice, although she had no legal training. (Assange was holed up in the Ecuadoran Embassy in London to avoid extradition to Sweden on rape charges.) With the Hong Kong Government unhappy with Snowden's presence, especially as he revealed details of US spying against China, he fled to the Russian Consulate when the US issued an extradition request on 21 June 2013, and revoked his passport. Snowden was charged with three criminal violations: theft of government property and two offenses under the espionage statutes, specifically giving national defense information to an unauthorized person (18 USC 793(d)) and revealing classified information about "communications intelligence" (18 USC 798(a)3). On June 23, 2013, Snowden flew to Moscow accompanied by Sarah Harrison.[37] By this time, the Russians undoubtedly knew who Snowden was and that he possessed many secrets of great interest.

Snowden spent the next 39 days in the "transit" wing of the Moscow airport hotel. The hotel is run by Russian Border Guards, subordinate to the Federal Security Service (FSB). His Russian lawyer, Anatoly Kucherena, described as a rights activist in the press, is actually a member of the "Public Council," a 15-member advisory board to the FSB and a Putin supporter.[38]

The flood of disclosures began in December 2013. Jacob Appelbaum, a Berlin resident like Poitras—a hacker previously in legal trouble, and Wikileaks

31. Nigel Nelson, "Edward Snowden was targeted by Russian spies 6 years BEFORE he exposed US secrets," *The Daily Mirror*, June 7, 2014. *www.mirror.co.uk/news/ world-news/edward-snowden-targeted-russian-spies-3659815*.

32. Shane Harris, "What Was Edward Snowden Doing in India?" *Foreign Policy*, January 13, 2014. *http://foreignpolicy.com/2014/01/13/what-was-edward-snowden-doing-in-india/*.

33. Glenn Greenwald, *Edward Snowden, the NSA, and the US Surveillance State*, Metropolitan Books, 2014.

34. Andrews et. al., "The Snowden Saga"; James Bamford, "The Most Wanted Man in the World," *WIRED*, September 2014. *http://www.wired.com/2014/08/edward-snowden#ch-7*.

35. Poitras had been tied to previous NSA whistleblower William Binney. As a result, she claimed that she was harassed by the Department of Homeland Security and was apparently on the US "Watch List." Andrews et. al., "The Snowden Saga."

36. Lucas, *The Snowden Operation*.

37. Described as Julian Assange's "closest advisor" (in the press) or "partner" (Wikipedia) or "girlfriend" (*Vanity Fair*).

38. Steven Lee Myers, "Snowden's Lawyer Comes With High Profile and Kremlin Ties," *New York Times*, July 27, 2013.

representative, described by Lucas as a "cyber-libertarian" and "cryptologic expert,"—first revealed publicly Snowden's documents.[39] Since then, there has been a steady stream of revelations, especially from Glenn Greenwald.

It is interesting to note the Wikileaks-Russia connections. Wikileaks is funded by a Putin-friendly oligarch in the background. A Wikileaks representative allegedly provided Belarus its files to crack down on dissidents. Wikileaks founder Julian Assange had a talk show on Russia's RT TV in 2012. A review of Wikileaks' disclosures reveals virtually no criticism of Russia.[40]

Is Snowden a Spy?

It is certainly not proven yet in a court of law; however, he has done things that make him appear to be one. He installed "spiders"[41] into NSA's computer systems to look for keywords and collect them. He accessed, apparently without authorization, more than two dozen specially compartmented files. He borrowed, stole, or forged personal passwords of his cohorts to do this. Most of the documents he has disclosed have nothing to do with surveillance of US persons; rather they reveal programs and capabilities against foreign intelligence targets, such as how NSA targets phone calls and e-mails of the Taliban in Pakistan and e-mails regarding Iranian attempts to avoid sanctions, how NSA hacks Chinese computers, and how NSA responds to foreign cyber espionage against the US. Snowden could not have read even a fraction of the estimated 1.5-1.7 million documents he has disclosed.

Spy or not, clearly Snowden is now a pawn of Russian intelligence and propagandists. Do the Russians have the materials that Snowden took? He arrived in Hong Kong with a suitcase full of computers and thumb drives,[42] but he claims the materials are safe due to encryption.[43] "Snowden told the *New York Times* in October he did not take any secret NSA documents with him to Russia when he fled there in June 2013. 'There's a zero percent chance the Russians or Chinese have received any documents,' Snowden told the *Times*." However, access to encrypted hard drives via "advanced" means, or implanted malware, is easy for a sophisticated intelligence service. If prepared, it only requires physical access for a short period of time to copy a hard drive. Once done, cryptanalytic efforts can be done at leisure. Greenwald claims only he and Poitras have complete sets of Snowden's documents. But who had access to the devices in Hong Kong, the Russian Consulate, or in the United Kingdom, Germany, or Brazil? What means do Greenwald and Poitras have to protect them? If one incident is indicative, one must assume the materials are in Russia's hands. On 18 August 2013, Greenwald's boyfriend/assistant, David Miranda, flying from Poitras in Berlin to Rio de Janeiro, was carrying password-encrypted thumb drives through Heathrow airport and was stopped by British authorities. Miranda was carrying the access passwords on a piece of paper. The password for encrypted cables related to Snowden's files also has been revealed on the Internet.[44] Such carelessness belies the claim that Snowden's materials are "safe."

The Russian intelligence and security services are well practiced in manipulating those who have sought refuge in Russia. Former defectors Kim Philby, Edward Lee Howard, and William Martin and Bernon Mitchell are good examples. All were used for propaganda purposes. His hosts are also using Snowden for the same. Snowden (now a journalist?) was allowed to ask President Putin a question about Russian surveillance in Putin's 17 April 2014 news conference. Putin replied that what Russia does was within the law. The unasked question was: What is Russian law?

Russia has a System of Operative-Investigative Measures (SORM). It is a decades-old system for surveillance of all telecommunications in Russia that is tied to the FSB. This system provides the FSB with full access to metadata *and content*. It includes the Internet, social networks, and credit card transactions. Russians must store their digital information within Russia (not overseas) by law, making it readily available. Russian law is far more comprehensive in allowing government surveillance than comparable US laws. Domestic and international Russian surveillance capabilities are extensive; it also maintains an

39. Nathaniel Rich, "The American Wikileaks Hacker," *Rolling Stone*, December 1, 2010. *www.rollingstone.com/culture/news/meet-the-american-hacker-behind-wikileaks-20101201*.

40. Joshua Foust, "Has Wikileaks Been Infiltrated by Russian Spies?" War Is Boring Blog, August 29, 2013. *https://medium.com/war-is-boring/has-wikileaks-been-infiltrated-by-russian-spies-b876a8bc035a*

41. A "spider" is a program that searches for and collects Web pages automatically. Used by search engines, such as Google and Yahoo, they are also known as "webcrawlers."

42. Andrews et. al., "The Snowden Saga."

43. Reuters, "US Lawmaker Investigates Whether Russia Behind Snowden's Leaks," January 19, 2014. *www.nytimes.com/reuters/2014/01/19/us/politics/19reuters-usa-security-snowden.html*.

44. *www.telegraph.co.uk/news/uknews/crime/10276460/David-Miranda-was-carrying-password-for-secret-files-on-piece-of-paper.html*

extensive SIGINT system, including in Cuba.

Snowden has also had extraordinary access to international communications for selected conferences with sympathetic audiences around the world.

Why did Snowden do this? Understanding his psyche is difficult from afar. James Bamford, in his September 2014 *WIRED* article, calls Snowden a "sincere idealist." Brown University Professor Rose McDermott has written that it is hard not to categorize Snowden as having a prototypical narcissistic personality disorder. He appears to have excessive vanity and seeks attention. He has claimed positions greater than what he had in reality. When his story falls off of the front page, he does something new to get back to center stage.[45] According to *Vanity Fair*'s profile of Snowden, his friends described him as naïve.[46]

[Snowden's] provision of massive amounts of classified information about US intelligence and military capabilities to the country's enemies is undeniably a traitorous act. The argument that providing classified information to journalists is different than providing it to an enemy nation is spurious, especially when publication of that information makes it readily available to any enemy.

From his comments, it is clear that Snowden rejects being held accountable for his actions. In *CitizenFour*, Wikileaks filmmaker Laura Poitras' sympathetic documentary, Snowden states he wants to stand trial. But in a 17 June 2013 online chat on *The Guardian*'s website, Snowden rejected that he would receive a fair trial in the US:

> *The US Government, just as they did with other whistleblowers, immediately and predictably destroyed any possibility of a fair trial at home, openly declaring me guilty of treason and that the disclosure of secret, criminal, and even unconstitutional acts is an unforgivable crime. That's not justice, and it would be foolish to volunteer yourself to it if you can do more good outside of prison than in it.*

Snowden insists on procedures that conflict with the established rules of procedure in US courts.

Snowden also has claimed to have not revealed any information on US intelligence operations against "*legitimate* military targets," but rather only NSA efforts against "civilian infrastructure." He claims his revelations have done no harm to the US, but how does he know that? asks David M. Barrett, a Villanova University political science professor.[47] Snowden has set himself up as the judge for what is right and wrong, and what is in the national interest and what is not.

Some Conclusions and Questions

From various news reports, it is evident that there have been numerous government screw-ups related to the Edward Snowden case. His background investigation was faulty. US Investigations Services, LLC (USIS), the contractor that conducted his background investigation, reportedly only interviewed his mother and girlfriend. The US Government investigated USIS for fraudulently and improperly conducting investigations to maximize billings. Its contract was cancelled.[48] Would a proper background investigation have revealed characteristics that might have excluded Snowden from receiving a sensitive compartmented clearance?

There is a US Government system for exchanging security-related personnel information between agencies. A person terminated from one agency under suspicion should not be granted a clearance by another agency. Why was an adverse CIA personnel report not available to NSA adjudicators prior to granting Snowden access to sensitive intelligence?

Snowden "borrowed" passwords from several of his cohorts at work. This is always a prohibited activity. Why were his requests to borrow passwords not reported by others? Perhaps the answer is that Americans have always disbelieved that one of their own would spy against the country. "This disbelief spawned a 'national capacity for naiveté,' as former CIA counterintelligence chief Paul Redmond dubbed it, "which surfaced as early as the American Revolution."[49] Apparently it continues today.

45. Rose McDermott comments in Loch Johnson (Editor), "An INS Special Forum: Implications of the Snowden Leaks," *Intelligence and National Security*, August 28, 2014, 803-4. *www.tandfonline.com/loi/fint20*.

46. Andrews et. al., "The Snowden Saga."

47. David M. Barrett comments in Loch Johnson (Editor), "An INS Special Forum: Implications of the Snowden Leaks," *Intelligence and National Security*, August 28, 2014, 797. *www.tandfonline.com/loi/fint20*.

48. Sakthi Prasad, "US brings fraud charges against firm that vetted Snowden," *Reuters*, January 23, 2014. *www.reuters.com/article/2014/01/23/us-usa-usis-idUSBREA0M0BD20140123*.

49. Michael Sulick, *Spying in America: Espionage from the Revolutionary War to the Dawn of the Cold War*, Washington, DC: Georgetown University Press, 2012), p. 2, citing former CIA chief of counterintelligence, Paul Redmond, "America Pays the Price for Openness," *Wall Street Journal*, June 2000, *www.apfn.net/message-*

Various critics perceive the avenues in the Intelligence Community available to whistleblowers as inadequate, despite the law and Presidential Directive 19. If those who perceive wrongdoing or waste cannot report such easily and without fear of retribution, leaks to journalists, who actively seek such information, will remain a major problem.

The scope and scale of NSA's surveillance exposed by Snowden was not appreciated by many in Congress and, certainly, not by the American public. Despite the amnesia of some lawmakers, Snowden's revelations came as an unwelcome surprise to many. The government's tendency toward extreme secrecy simply added fuel to the fire, especially from strict civil libertarians whose distrust of government is foremost in their thoughts and who suspected a cover-up.

Technological innovations have also changed public perceptions of what protections US persons should have under the Fourth Amendment of the Constitution. The legal debate over communications content versus metadata decided by the Supreme Court in Smith v. Maryland in 1979 preceded the invention of the "smart" phone, which can contain so much personal data and tracking information from Global Positioning System (GPS) microchips. Today, what constitutes a "search" and what legal procedures are relevant? The legal landscape seems to be shifting.

Regarding Snowden's actions, one has to ask several questions. How did he travel as he did (India, Hong Kong) without help? Why did he go to China and then Russia? Why did he not go to Iceland (the home of Wikileaks) or Sweden or elsewhere where there are very permissive legal environments and where it would be unlikely he would be extradited to the US for a "political" crime; many countries regard spying as a political crime and are disinclined to extradite an accused spy unless it has suffered damage to its own interests.

The Economist's Lucas, noting that Snowden has not criticized Russian or Chinese mass surveillance, concludes that his Russian supported activity "looks ... like ... a global anti-American campaign." David Ignatius, the national security reporter for *The Washington Post*, notes that the NSA programs were legal. That makes it hard to say Snowden was a whistleblower of illegal activities.[50] Glenn Hastedt, James Madison University political science and justice studies professor concludes, "[f]rom a legal perspective Snowden is not a whistleblower."[51]

Regardless of legalities, for those who wish to dismiss the specifics of the law, Snowden will remain a whistleblower. His provision of massive amounts of classified information about US intelligence and military capabilities to the country's enemies is undeniably a traitorous act. The argument that providing classified information to journalists is different than providing it to an enemy nation is spurious, especially when publication of that information makes it readily available to any enemy. Is Snowden a spy? Certainly, he is a defector, living in Russia. His stay recently was extended for three years. He is supported by the Russian intelligence services. At worst, he has been (and still is) a controlled agent of Moscow, a saboteur trying to cripple NSA and US intelligence.

So, in summary, is Edward Snowden a whistleblower? – yes and no. A traitor? – yes. A spy? – perhaps. At best, he is a "useful idiot." This is a term often ascribed to Lenin to describe a Westerner who helped the Soviet Union through his or her naïveté.

Finally, what about Snowden's future? As Russia wants to know how the US encrypts its most sensitive communications and what Snowden knows about other sensitive matters, it will support him. He will also be used as a propaganda tool. Some have opined that his useful life for the Russians is approximately three years. But then what? Nigel Nelson of the *Daily Mirror* wrote that Snowden was probably tricked about death threats if he returns to the US.[52] Is he safe in Russia? Some think not, especially after his usefulness expires and if he becomes a liability to Moscow.[53]

Peter Oleson is a former associate professor in the graduate school of the University of Maryland University College. Previously, he was an assistant director of the Defense Intelligence Agency and senior intelligence policy advisor to the undersecretary of defense for policy. He was president of a consulting firm specializing in technology and program management for intelligence systems. He is a member of the board of AFIO.

board/7-09-03/discussion.cgi.46.html.

50. David Ignatius, comments to an AFIO symposium, 3 May 2014.

51. Glenn Hastedt comments in Loch Johnson (Editor), "An INS Special Forum: Implications of the Snowden Leaks," *Intelligence and National Security*, 28 August 2014, 798. *www.tandfonline.com/loi/fint20*.

52. Nigel Nelson, "Edward Snowden was targeted."

53. The long-standing Russian tendency to deal fatally with "problems" could be a problem for Snowden. Boris Nemtsov, a Putin opponent, was shot dead near the Kremlin in March 2014. A Russian agent murdered Alexander Litvinenko, an outspoken KGB defector, in London in 2006 by polonium. Russian journalist Anna Politkovskaya, a critic of the Kremlin, was also murdered in 2006. Edward Lee Howard, a CIA defector to Moscow, died mysteriously in Moscow in 2002.