Questioning Ed Snowden's Cure-All

Forgetting Cypherpunk History

By Bill Blunden

Ed Snowden recently gave fellow NSA whistleblower James Bamford an "extended cut" interview in Moscow[1]. While Snowden offered up a few morsels of headline-worthy information, like how he purposefully left forensic artifacts for investigators or details on the NSA's automated cyber-attack system called MonsterMind, Bamford's piece ends with Snowden describing what he views as the answer to the NSA's global surveillance program:

> *"We have the means and we have the technology to end mass surveillance without any legislative action at all, without any policy changes… By basically adopting changes like making encryption a universal standard—where all communications are encrypted by default—we can end mass surveillance not just in the United States but around the world."*

So, that's it, huh? All we need is strong crypto? Download the latest app and guaranteed civil liberties are but a click away…

Pleasant fiction, caws your humble narrator.

Snowden's train of thought echoes that of many cypherpunks back in the 1980s, doesn't it? There were true believers in this milieu who thought that strong encryption alone would be sufficient to thwart Big Brother. This idea is founded on the stance that political considerations can be entirely eschewed in favor of strictly technical or market-oriented solutions. One might even posit that there are intimations of Libertarian ideology (i.e. corporate feudalism[2]) at work, which might not be surprising considering the Ed Snowden was a supporter of Ron Paul[3].

Such a mindset no doubt serves the interests of an entrepreneur like Pierre Omidyar, a billionaire who plans to generate income by peddling security products. Products that will address the very scandals that his new media venture unearths[4]. Isn't that convenient? To be able to present a problem with one hand and then proffer a solution with the other? Problem-Reaction-Solution; also known as the *Hegelian dialectic*. By the way this tactic has also been employed, to the hilt, by a Pentagon carpetbagger named Keith Alexander[5].

Yet Snowden's own documents clearly illustrate that strong encryption doesn't translate into cyber security[6]. If the minions of the Deep State want your data they'll get it. Anyone who refuses to play ball ends up like the CEO of Lavabit[7] (if they're lucky[8]). It doesn't matter how "secure" vendors claim their technology is. Government spies, with the full cooperation of large multinational corporations (it's a matter of *shared class interest*, you see[9]), have demonstrated

a notable talent for leveraging hidden back doors and conducting *computer network exploitation* (CNE)[10]. This conclusion is further buttressed by "accidental" back doors like the Heartbleed vulnerability, which sent shockwaves across the Internet[11]. John Young, of Cryome.org, describes the current state of affairs:

> *"So it has come to pass, there is no refuge from politics, and the once reviled tin - hats of conspiracy theories are replacing anomymous masks, especially by the best and brightest cryptographers who have been hoodwinked far more than dreamed of in earliest days of cypherpunks."*

As Hungarian scholar Karl Polyanyi explained, the concept of unfettered free markets is a quaint myth. Markets are defined by governments and the ground rules that they establish. The same could be said for cyber-security, which suffers as a matter of official policy. Spies have been given [secret] license to undermine software in the pursuit of the Eye of Providence[12]. Likewise hi-tech vendors release bug-ridden code because they can get away with making society accept the cost. In the eyes of a hi-tech CEO the incidents which result from their faulty products are a *negative externality*.

This underscores a point that both Ed Snowden and Glenn Greenwald have failed to acknowledge[13]. There are laws that allow these violations to transpire. Furthermore the government which formulated these laws has been captured by plutocratic factions[14]. The intelligence services, in particular the CIA, exist to serve these elite interests[15]. To seek refuge in strong encryption is to escape into denial. Bolstering security and protecting our civil liberties will require the public to mobilize and build the political impetus to take on the Deep State.

Bill Blunden is an independent investigator whose current areas of inquiry include information security, anti-forensics, and institutional analysis. He is the author of several books, including *The Rootkit Arsenal* and *Behold a Pale Farce: Cyberwar, Threat Inflation, and the Malware-Industrial Complex*. Bill is the lead investigator at Below Gotham Labs.

End Notes

[1] Jame Bamford, "The Most Wanted Man In The World," *Wired*, August 13, 2014, http://www.wired.com/2014/08/edward-snowden/

[2] Mike Konczal, "We Already Tried Libertarianism - It Was Called Feudalism," *The Next New Deal*, June 11, 2013, http://www.nextnewdeal.net/rortybomb/we-already-tried-libertarianism-it-was-called-feudalism

[3] Barton Gellman and Jerry Markon, "Edward Snowden says motive behind leaks was to expose 'surveillance state'," *Washington Post*, June 10, 2013, http://www.washingtonpost.com/politics/edward-snowden-says-motive-behind-leaks-was-to-expose-surveillance-state/2013/06/09/aa3f0804-d13b-11e2-a73e-826d299ff459_story.html

[4] Glenn Greenwald, "Email exchange with reader over First Look and NSA reporting," *UT Documents*, January 6, 2014, http://utdocuments.blogspot.com/2014/01/email-exchange-with-reader-over-first.html

[5] George Smith, "Keith Alexander really IS a pariah," *Escape from Whitemanistan*, August 2, 2014, http://dickdestiny.com/blog1/?p=18406

[6] Bill Blunden, "Mass Subversion Is a Reality," *Counterpunch*, July 24, 2014, http://www.counterpunch.org/2014/07/24/mass-subversion-is-a-reality/

[7] Spencer Ackerman, "Lavabit email service abruptly shut down citing government interference," *Guardian*, August 9, 2013, http://www.theguardian.com/technology/2013/aug/08/lavabit-email-shut-down-edward-snowden

[8] Gary Lee, "Area Writer Investigating Inslaw Case Found Dead," *Washington Post*, August 13, 1991, http://www.highbeam.com/doc/1P2-1079614.html

[9] Bill Blunden, "The NSA's Corporate Collaborators," *Counterpunch*, May 9-11, 2014, http://www.counterpunch.org/2014/05/09/the-nsas-corporate-collaborators/

[10] Bill Blunden, "The NSA Wants You to Trust Tor, Should You?" *Counterpunch*, July 18-20, 2014, http://www.counterpunch.org/2014/07/18/the-nsa-wants-you-to-trust-tor-should-you/

[11] Sean Gallagher, "Heartbleed vulnerability may have been exploited months before patch," *Ars Technica*, April 9, 0214, http://arstechnica.com/security/2014/04/heartbleed-vulnerability-may-have-been-exploited-months-before-patch/

[12] Antony Loewenstein, "The ultimate goal of the NSA is total population control," *Guardian*, July 10, 2014, http://www.theguardian.com/commentisfree/2014/jul/11/the-ultimate-goal-of-the-nsa-is-total-population-control

[13] Bill Blunden, "An Open Letter to Glenn Greenwald," *Counterpunch*, June 19, 2014, http://www.counterpunch.org/2014/06/19/an-open-letter-to-glenn-greenwald/

[14] Larry Bartels, "Rich People Rule!" *Washington Post*, April 8, 2014, http://www.washingtonpost.com/blogs/monkey-cage/wp/2014/04/08/rich-people-rule/

[15] "Philip Agee and Edward Snowden: A comparison," *Rancid Honeytrap*, August 13, 2014, http://ohtarzie.wordpress.com/2014/08/13/philip-agee-and-edward-snowden-a-comparision/