

From: Teresa B. Veith  
Hamilton, Illinois

October 1, 2013  
Via email  
reviewgroup@dni.gov

To: The DNI Review Group on Intelligence and Communications Technologies

I should like to quote three men from three documents. While I am just quoting a few salient points I would encourage you to read all three in their entirety.

Representative Louie Gohmert from the Congressional Record Volume 159, Number 108 Thursday July 25, 2013 from the middle of page H5079 upto and including most of page H5083: Page H5082:

- You've got to describe with sufficient particularity that people can identify items that you're demanding to be produced.
- You can't just come in and ask for everybody's phone records in the country.
- I go back to 2002, when a CIA attorney at one of our judicial conferences

Start page H5083:

- said, Gee, banks have all of your financial information. Why shouldn't the government? I was aghast and said because the banks can't come to your home, bust down the door, throw you to the ground, put a boot on your back, and put you in handcuffs and drag you off. But the government can and does. So we've got to be very careful to make sure that the government does not overreach what they are allowed to do.
- Then we find out the NSA has gotten orders so they can get every single call that we have made to somebody. There is no specificity in an order like that. This has to stop.
  - I've been surprised.
  - ...I said that's right, that's what the law allows, but they're going so far beyond that.
  - But for those who just want to be Americans and live their private lives and be left alone, the government should not be watching everything they do through their computers, through their debit and credit card purchases and transactions, through every phone call they make.

William E. Binney from the 10 page sworn declaration in Support of Plaintiff's Motion for Partial Summary Judgment Rejecting the Governments Defendant's State Secret Defense in Jewel versus NSA Case 3:08-cv-04373-JSW Document 88 Executed on June 21, 2012 at Washington D.C., Filed 07/02/12 in the United States District Court for the Northern District of California:

Paragraph 5

- The advent of the September 11 attacks brought a complete change in the approach of the NSA toward doing its job. FISA ceased to be an operative concern, and the individual liberties preserved in the U.S. Constitution were no longer a consideration. It was at that time that the NSA began to implement a group on intelligence activities now known as the President's Surveillance Program (PSP).
- ... the PSP involved the collection of domestic electronic communications traffic without any of the privacy protections built into Thin Thread.

Paragraph 6

- I resigned from the NSA in late 2001. I could not stay after the NSA began purposefully violating the Constitution.

Paragraph 13

- The sheer size of that capacity (at the Utah Data Center) indicates that the NSA is not filtering personal electronic communications such as email before storage but is, in fact, storing all that they are collecting. The capacity of the NSA's planned infrastructure far exceeds the capacity necessary for the storage of discreet, targeted communications or even for the storage of the routing information from all electronic communications. The capacity of the NSA's planned

infrastructure is consistent, as a mathematical matter, with seizing both the routing information and the contents of all electronic communications.

Paragraph 15

- Director Mueller responded ... “elements of the Department of Defense,” (namely the NSA) and the FBI had “put in place technological improvements relating to the capabilities of a database to pull together past emails as well as ... and future ones as they come in so that it does not require an individualized search.” (Mueller Senate testimony, March 30, 2011 at minute 43:50). The NSA cannot pull together past emails from the NSA’s database unless the NSA had already collected the emails and stored them in its database.

Senator Ron Wyden from his speech of July 23, 2013; “Wyden on NSA Domestic Surveillance at the Center for American Progress.” 29 pages:

Page 2

- At the time, Senate rules about classified information barred me from giving any specifics of what I’d seen except to describe it as Secret Law – a secret interpretation of the Patriot Act, issued by a secret court, that authorizes secret surveillance programs – programs that I and colleagues think go far beyond the intent of the statute.
- If that is not enough to give you pause, then consider that not only were the existence of and the legal justification for these programs kept completely secret from the American people, senior officials from across the government were making statements to the public about domestic surveillance that were clearly misleading and at times simply false.

Page 3

- They’re going to say, in America, you don’t have to settle for one priority or the other: laws can be written to protect both privacy and security, and laws should never be secret.

Page 4

- The result: the creation of an always expanding, omnipresent surveillance state that – hour by hour – chips needlessly away at the liberties and freedoms our Founders established for us, without the benefit of actually making us any safer.

Page 5

- The combination of increasingly advanced technology with a breakdown in the checks and balance that limit government action could lead us to a surveillance state that cannot be reversed. ... This started not long after 9/11, with a Pentagon program called Total Information Awareness, which was essentially an effort to develop an ultra-large-scale domestic data mining system. Troubled by this effort, and its not exactly modest logo of an all-seeing eye on the universe, I worked with a number of

Page 6

senators to shut it down. Unfortunately, this was hardly the last domestic surveillance overreach. In fact, the NSA’s infamous warrantless wiretapping program was already up and running at that point, though I, and most of members of the Intelligence Committee didn’t learn about it until a few years later. This was part of a pattern of withholding information from Congress that persisted throughout the Bush administration – I joined the Intelligence Committee in 2001, but I learned about the warrantless wiretapping program when you read about it in the New York Times in late 2005.

Page 9

- They (laws) should be public all the time, open to review by adversarial courts, and subject to change by an accountable legislature guided by an informed public.

Page 10

- ... It’s Civics 101. And secret law violates those basic principles. It has no place in America.

Page 11

- They (FISC) chose to issue binding secret rulings that interpreted the law and the Constitution in the startling way that has come to light in the last six weeks. They were to issue the decision that the Patriot Act could be used for dragnet, bulk surveillance of law-abiding Americans.

Page 14

- This means that the government's authority to collect information on law-abiding American citizens is essentially limitless.
- What happens to our government, our civil liberties and our basic democracy if the surveillance state is allowed to grow unchecked?

Page 18

- And let's be clear: the public was not just kept in the dark about the Patriot Act and other secret authorities. The public was actively misled.

Page 20

- The answer is that it is not all right, and it is indicative of a much larger culture of misinformation that goes beyond the congressional hearing room and into the public conversation writ large.

Page 23

- Meanwhile, I have not seen any indication that the bulk phone records program yielded any unique intelligence that was not also available to the government through less intrusive means.

Page 29

- James Madison, the father of our constitution, said that the accumulation of executive, judicial and legislative powers into the hands of any fraction is the very definition of tyranny.

This is no longer about security versus privacy, if it ever was, for if we don't defend both we'll have neither. You are also tasked with regaining the public trust, i.e. assuaging American outrage and fears. Here are a few on mine:

- That our historic system of checks and balances can be completely subverted by stamping TOP SECRET on millions of documents
- That Congressional and FISC oversight can be stymied by a "culture of misinformation"
- That "Foreign Intelligence" includes all domestic digital data
- That anyone believes that "self-reporting" has ever or could ever work
- That since the 1990's, "agents are trained to 'recreate' the investigative trail to effectively cover up where the information originated," ... "Two dozen partner agencies comprise the (DEA's SOD) unit, including the FBI, CIA, NSA, Internal Revenue Service and the Department of Homeland Security." Where is due process? That "(p)arallel construction is a law enforcement technique we use everyday, ... (i)t's decades old, a bedrock concept," illustrates how perverse the Defense of our Constitution and Rule of Law has become at the hands of our Intelligence Community. ["Exclusive: U.S. directs agents to cover up program used to investigate Americans," by John Shiffman and Kristina Cooke, Reuters – Washington Mon. Aug. 5, 2013]
- That Americans even need to discuss Drone Assassinations
- That James Clapper believes that after a pointless "discussion" the secrecy will carry on. I pray he is wrong.

Respectfully,

Teressa B. Veith