CINDY COHN (145997)
cindy@eff.org
LEE TIEN (148216)
KURT OPSAHL (191303)
JAMES S. TYRE (083117)
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333
Fax: (415) 436-9993

RICHARD R. WIEBE (121156)
wiebe@pacbell.net
LAW OFFICE OF RICHARD R. WIEBE
One California Street, Suite 900
San Francisco, CA 94111
Telephone: (415) 433-3200
Fax: (415) 433-6382

RACHAEL E. MENY (178514)
rmeny@kvn.com
PAULA L. BLIZZARD (207920)
MICHAEL S. KWUN (198945)
AUDREY WALTON-HADLOCK (250574)
KEKER & VAN NEST, LLP
710 Sansome Street
San Francisco, California 94111-1704
Telephone: (415) 391-5400
Fax: (415) 397-7188

THOMAS E. MOORE III (115107)
tmoore@moorelawteam.com
THE MOORE LAW GROUP
228 Hamilton Avenue, 3rd Floor
Palo Alto, CA 94301
Telephone: (650) 798-5352
Fax: (650) 798-5001

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

CAROLYN JEWEL, TASH HEPTING, GREGORY HICKS, ERIK KNUTZEN and JOICE WALTON, on behalf of themselves and all others similarly situated, Plaintiffs, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	CASE NO. CV-08-04373-JSW **DECLARATION OF WILLIAM E. BINNEY IN SUPPORT OF PLAINTIFFS' MOTION FOR PARTIAL SUMMARY JUDGMENT REJECTING THE GOVERNMENT DEFENDANTS' STATE SECRET DEFENSE** Date: September 28, 2012 Time: 9:00 a.m. Courtroom 11, 19th Floor The Honorable Jeffrey S. White

I, William Binney, declare:

1. I am a former employee of the National Security Agency ("NSA"), the signals intelligence agency within the Department of Defense. Unless otherwise indicated, I have personal knowledge of each and every fact set forth below and can competently testify thereto.

2. A true and correct copy of my resume is attached hereto as Exhibit A.

3. In the late 1990's, the increasing use of the Internet for communications presented

the NSA with a special kind of problem: The NSA could not collect and smartly select from the large volume of data traversing the Internet the nuggets of needed information about "Entities of Interest" or "Communities of Interest," while protecting the privacy of U.S. persons. Human analysts had to manually identify the groups and entities associated with activities that the NSA sought to monitor. That process was so laborious that it significantly hampered the NSA's ability to do large scale data analysis.

4. One of my roles at the NSA was to find a means of automating the work of human analysts. I supervised and participated in the development of a program called "Thin Thread" within the NSA. Thin Thread was designed to identify networks of connections between individuals from their electronic communications over the Internet in an automated fashion in real time. The concept was for devices running Thin Thread to monitor international communications traffic passing over the Internet. Where one side of an international communication was domestic, the NSA had to comply with the requirements of the Foreign Intelligence Surveillance Act ("FISA"). With Thin Thread, the data would be encrypted (and the privacy of U.S. citizens protected) until such time as a warrant could be obtained from the Foreign Intelligence Surveillance Court.

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 the group of intelligence activities now known as the President's Surveillance Program ("PSP"). While I was not personally read into the PSP, various members of my Thin Thread team were given the task of implementing various aspects of the PSP. They confided in me and told me that the PSP involved the collection of domestic electronic communications traffic without any of the privacy protections built into Thin Thread.

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

7. The NSA chose not to implement Thin Thread. To the best of my knowledge, the NSA does not have a means of analyzing Internet data for the purpose of identifying Entities or

Communities of Interest in real time. The NSA has the capability to do individualized searches, similar to Google, for particular electronic communications in real time through such criteria as target addresses, locations, countries and phone numbers, as well as watch-listed names, keywords, and phrases in email. The NSA also has the capability to seize and store most electronic communications passing through its U.S. intercept centers. The wholesale collection of data allows the NSA to identify and analyze Entities or Communities of Interest later in a static database. Based on my proximity to the PSP and my years of experience at the NSA, I can draw informed conclusions from the available facts. Those facts indicate that the NSA is doing both.

8. The NSA could have installed its intercept equipment at the nation's fiber-optic cable landing stations. See Greg's Cable Map, cablemap.info. There are more than two dozen such sites on the U.S. coasts where fiber-optic cables come ashore. If the NSA had taken that route, it would have been able to limit its interception of electronic communications to international/international and international/domestic communications and exclude domestic/domestic communications. Instead the NSA chose to put its intercept equipment at key junction points (for example Folsom Street) and probably throughout the nation, thereby giving itself access to purely domestic communications. The conclusion of J. Scott Marcus in his declaration that the "collection of infrastructure . . . has all the capability necessary to conduct large scale covert gathering of IP-based communications information, *not only for communications to overseas locations, but for purely domestic communications as well,*" is correct.

9. I estimate that the NSA installed no fewer than ten and possibly in excess of twenty intercept centers within the United States. I am familiar with the contents of Mark Klein's declaration. The AT&T center on Folsom Street in San Francisco is one of the NSA intercept centers. Mr. Klein indicated that the NSA's equipment intercepted Internet traffic on AT&T's peering network. It makes sense for the NSA to intercept traffic on AT&T's peering network. The idea would be to avoid having to install interception equipment on each of the thousands of parallel data lines that eventually lead into and out of peering networks. By focusing on peering networks, the NSA intercepts data at the choke point in the system through which all data must pass in order to move from one party's network to another's. This is particularly important because a block data

is often broken up into many smaller packets for transmission. These packets may traverse different routes before reaching the destination computer which gathers them and reassembles the original block.

10. One of the most notable pieces of equipment identified in Mr. Klein's declaration is the NARUS Semantic Traffic Analyzer. According to the NARUS website, each NARUS device collects telecommunications data at the rate of ten gigabits per second and organizes the data into coherent streams based on the protocol associated with a specific type of collected data. A protocol is an agreed-upon way for data to be broken down into packets for transmission over the Internet, for the packets to be routed over the Internet to a designated destination and for the packets to be re-assembled at its destination. Protocols exist at each layer of the OSI (Open Systems Interconnection) 7-layer telecommunications model and are used for a wide variety of data, not just electronic communications. That means that NARUS can reconstruct all information transmitted through the peering network and forward all of the electronic communications to a database for analysis. The NARUS device can also select predetermined data from that path and forward the data to organizations having interest in the data. As I indicated above, the predetermined data would involve target addresses, locations, countries, and phone numbers, as well as watch-listed names, keywords, and phrases.

11. A further notable development has been the NSA's public announcement in October 2009 that it was building a massive, $1.2 billion digital storage facility in Ft. Williams, Utah. According to some reports, the Utah facility will eventually have a data storage capacity measured in yottabytes (10^{24} bytes). Even if the Utah facility were to have no more than the amount of data storage that is presently commercially available, then one would expect the data storage to be in the range of multiples of ten exebytes (10^{18} bytes). See www.cleversafe.com. (According to Cleversafe, its ten exebyte storage solution fills no more than two hundred square feet). In April 2011, the NSA also announced that it would build a new supercomputing center at its Ft. Meade, Maryland headquarters.

12. The amount of data that each NARUS device can process per second is large (10 gigabits is 10 billion bits). To illustrate the sheer size of the data storage capacity of the Utah

facility, one could assume the installation of twenty-five NARUS devices in the U.S. and that all of the NARUS-processed data is sent via fiber-optic cable to Utah. That means that the NARUS processing rate of10 billion bits per second means that one machine can produce approximately 4 x 10^{16} bytes per year. That in turn means that it would take twenty-five devices one year to fill an exebyte or ten years to fill ten exebytes.

13. The sheer size of that capacity 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 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 NSA's planned infrastructure is consistent, as a mathematical matter, with seizing both the routing information and the contents of all electronic communications.

14. Several other circumstances support the conclusion that the NSA is storing all personal electronic communications. One such circumstance is the U.S Senate testimony of the Director of the FBI, Robert Mueller, who has full knowledge of the PSP. Director Mueller's Senate testimony took place on March 30, 2011, shortly after the killings at Fort Hood, Texas. Within days of the Fort Hood incident, the government revealed a series of emails between the perpetrator, Major Nidal Malik Hasan, and a cleric in Yemen with al-Qaeda connections, Anwar al-Awlaki. Because of the emails and other factors, critics complained that the FBI should have been alert to the threat that Major Hasan posed well before the killings.

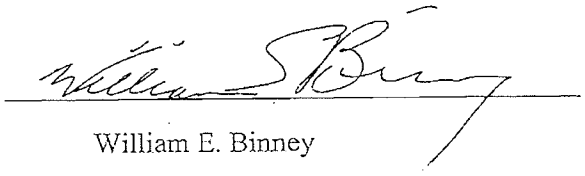
15. At the Senate hearing, Senator Kohl asked Director Mueller what the FBI had done to improve its capabilities for identifying similar threats in the future. Director Mueller responded that the FBI had put in place procedures to coordinate with "elements of the Department of Defense," (namely the NSA) and that 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.

16. A further circumstance is the attempted adoption of a mass data collection program in the United Kingdom. The British analogue to the NSA is an organization dedicated to signals intelligence called the Government Communications Headquarters (GCHQ). The GCHQ's experience is described in the declaration of J. Kirk Wiebe.

17. On May 20, 2012, General Keith Alexander, the current head of the NSA, appeared before Congress and sought to rebut a news article in the March 2012 issue of *Wired* magazine in which I was quoted. I believe that Gen. Alexander was using the word "intercept" in his testimony in a very narrow way. To Gen. Alexander, "intercept" means that a human analyst actually read the electronic communications. That is not the sense of the word "intercept" that was used in the *Wired* article.

18. At some point prior to 2007, I became the target of a federal criminal investigation into the leaks that lead to *The New York Times* article ("Bush Lets U.S. Spy on Callers Without Courts") published on December 16, 2005. I was not the source for the article. As part of that investigation, in July 2007, the FBI raided my home with guns drawn. The raid was apparently prompted by my involvement in reporting government waste to the Inspector General of the Department of Defense. The waste involved in a project called "Trailblazer" cost the taxpayers over four billion dollars. I was formally cleared of criminal wrongdoing in January 2010. I am also a colleague of Thomas Drake, who was eventually indicted for allegedly retaining allegedly classified NSA documents. Those charges were dropped. Those events have nothing whatsoever to do with the truth of the statements set forth above.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct. Executed on June 21, 2012 at Washington D.C.



William E. Binney

EXHIBIT A

William E. Binney

– Mathematician/Analyst –

Skill Areas: Intelligence Analysis; Traffic Analysis; Systems Analysis; Mathematics; Knowledge Management

Description of Most Recent Position

November 2005 – 30 June 2006 Entegra Systems Inc.

For the U.S. Customs and Border Protection, Office of Information Technology, Targeting and Analysis Systems Program Office, Mr. Binney defined statistical modeling techniques and advanced analytic processes, to support the modernization of CBP's Targeting and Analysis systems, tools, and analytical processes to perform predictive analysis of terror-related cargo and passenger transactions. Mr. Binney also supported the evaluation and integration of advanced analytic tools, both COTS tools and tools being develop by research universities and National Labs, under grants from the Department of Homeland Security, Advanced Research Projects Agency (HS/ARPA). Furthermore, Mr. Binney conducted an evaluation of CBP data quality, as well as defining techniques and processes for aggregating Cargo, Passenger, Law Enforcement, and Counter Terrorism-related data from multiple sources into a single, normalized entity-based repository.

Finally, Mr. Binney served as a member of a quick-reaction analytic team, which reviews available intelligence or information, and applies emerging advanced analytic technologies against selected operational data sets, to support executive level decision making and field operations.

Past Positions

From 2002 to 2004, as a member of Entity Mapping LLC., I worked on a contract for a major government organization. The contract effort centered on analysis of data to produce new entities and communities of interest. This effort required development of new data management processes, as well as analytic techniques to first verify the relationships between known entities of interest, then predict the existence of other entities of interest not previously observed. Our efforts also resulted in successfully developing a rules-based exclusionary approach that resulted in automatic discovery of newly observed but unpredicted entities of interest.

Positions held during 32 years career at the National Security Agency

2001 Technical Leader, Intelligence
1999-2001 Representative to the National Technology Alliance Executive Board
1996-2001 Member of the Senior Technical Review Panel
1995-2001 Co-founder/leader of the Automation Research Center (ARC)
2000-2001 Technical Director of the Analytic Services Office
1998-2000 Chair of the Technical Advisory Panel to the Foreign Relations Council
1998-2000 Analysis Skill Field Leader, Operations
1997-2000 Technical Director, World Geopolitical and Military
1996-1997 Technical Director, Russia
1975-1996 Leading analyst for warning, Russia
1970-1975 Analyst on Russia

Military service

1965-1969 Four years in the Army Security Agency (NSA/CSS)

Career Experience:

Over the years, I have applied mathematical discipline to collection, analysis and reporting. In the process, I formulated Set Theory, Number Theory and Probability applications to collection, data analysis and intelligence analysis. Based on this experience, I was able to structure analysis and transform it into a definable discipline making it possible to code and automatically execute these functions without human intervention from the point of collection to the end report. The successful automation of analysis formed the foundation for prototype developments in the ARC. These efforts caught the eye of Congressional Staffers and captured their imaginations. So much so that Congress actively supported and funded ARC development of automated systems. These systems revolutionized the business processes by demonstrating how to handle massive amounts of data effectively and relate results to military and other customers. I have also organized an international coalition of countries to jointly develop technology, share results and gain the benefits of collaborative efforts.

Primarily, I have focused on solving problems from a systems analysis perspective so that gains in any part of the business could be leveraged across the entire business enterprise.

Honors, awards and special achievements:

Directors Productivity Award - 1995
Technical Achievement Award – 1998
Gold Nugget Award - 1988

Numerous Letters of Appreciation
Numerous cash awards

Degrees and Certificates:

B.S. Mathematics, The Pennsylvania State University, 1970
Certified Analysis Professional – 1973