

1 Those signals might entail: (i) the electronic communications between persons such as radio
2 transmissions, telephone signals and email, (ii) the non-communications electronic emissions from
3 equipment like radar; or (iii) a combination of the two. As an analyst at the NSA, part of my job
4 was to sift through various intelligence sources for the purpose of identifying Profiles of Interest,
5 Persons of Interest, Entities of Interest or Communities of Interest. An Entity of Interest is a group,
6 organization or association that is subject to further inquiry. A Community of Interest is a looser
7 association of people that might share a common object, such as an attack on the nation, and would
8 similarly be subject to further inquiry. A Profile of Interest would encompass shared attributes
9 within an Entity of Interest or Community of Interest that helps to identify the members of the
10 group or members or another group engaged in a similar activity.

11 4. A common misconception is that an analyst must review the content of
12 communications between people in order to establish a link between them. In fact, an NSA analyst
13 would regard a person's association and the persistence of that association with other persons as
14 being of greater relevance to a determination of whether the person is a member of a Community
15 of Interest than the actual words used in a series of communications.

16 5. The use of associations may be illustrated with the networks of connections between
17 and among the planners and perpetrators of the attacks on September 11. Two of the September 11
18 hijackers, al-Mihdhar and al-Hazmi were known to have terrorist connections because it was
19 known that they had attended an al-Qaeda summit in Kuala Lumpur. Upon their arrival in
20 California in 2000, each man communicated with the principal hijacker, Mohamed Atta. Atta, in
21 turn, communicated with various other persons involved in the planning and implementation of the
22 September 11 attacks. Using a Profile of Interest that assumed that electronic communications
23 between two terrorists indicated a potential terrorist, an analyst would identify Atta as a potential
24 terrorist. Persons who communicated with Atta and one further known terrorist would in turn be
25 identified as a potential terrorist, and so on. Eventually, one could identify the entire network of
26 plotters from California to Germany, including the principal planner, Khalid Sheik Mohammed. A
27 true and correct copy of the linkages among the communications is attached hereto as Exhibit B.

28 6. Building these associations among persons using manual analysis is a slow,

1 laborious process. In the late 1990's, I learned that Mr. Binney had created a program called Thin
2 Thread, which was designed to identify networks of connections between individuals from their
3 electronic communications over the Internet in an automated fashion in real time. Thin Thread
4 could have identified the small number of members of the September 11 plot (nineteen plus a few
5 overseas) in a relatively short period of time.

6 7. I agree with Mr. Drake's assessment that everything changed at the NSA after the
7 attacks on September 11. The prior approach focused on complying with the Foreign Intelligence
8 Surveillance Act ("FISA"). The post-September 11 approach was that NSA could circumvent
9 federal statutes and the Constitution as long as there was some visceral connection to looking for
10 terrorists.

11 8. To the best of my knowledge, the NSA does not have a means of analyzing all of its
12 Internet data for the purpose of identifying Entities or Communities of Interest in real time. The
13 NSA has the capability to do individualized searches, similar to Google, for particular electronic
14 communications in real time through such criteria as target addresses, locations, countries and
15 phone numbers, as well as watch-listed names, keywords, and phrases in email. The NSA has the
16 ability to do individualized or small scale searches for particular electronic communications in real
17 time. It also has, or is in the process of obtaining, the capability to seize and store most electronic
18 communications passing through its U.S. intercept centers. The wholesale collection of data allows
19 the NSA to identify and analyze Entities or Communities of Interest later in a static database.
20 Based on my proximity to the PSP and my years of experience at the NSA, I can draw informed
21 conclusions from the available facts. Those facts indicate that the NSA is doing both.

22 9. I agree with the analysis and conclusions set forth in Mr. Binney's declaration,
23 particularly about the capabilities of the NARUS device. Like Mr. Binney, I have concluded that,
24 because the NSA did not have Thin Thread or, for that matter, a functional Trailblazer, the NSA
25 has chosen to seize and save all electronic communications.

26 10. The intelligence programs put into place under the newly-coined name, President's
27 Surveillance Program ("PSP") was not limited to seizing electronic communications from late 2001
28 forward. In order to gain historical data on the associations between persons, I understand that the

1 NSA gained access to the historical telephone records of the major telecommunications companies,
2 including especially AT&T. As I explained above, it is the existence, timing, and frequency of
3 communications between persons that are informative and not the just the content.

4 11. On occasion, the government reveals small pieces of the data that it has collected.
5 For example, a Department of Justice whistleblower, Jesselyn Radack (who also happens to be one
6 of my lawyers), moved from the Department of Justice to a private law firm. The private firm fired
7 her, and, during the course of the dispute, her former firm supplied her lawyer with a list of calls
8 not only made from Ms. Radack to a reporter, Michael Isikoff, but also to calls that Mr. Isikoff had
9 made to lawyers in the Department of Justice in which Ms. Radack was not on the line. A true and
10 correct copy of the list is attached hereto as Exhibit C. That list could only have been supplied by
11 Mr. Isikoff's telecommunications carrier.

12 12. On a further occasion, the government revealed a series of emails between the
13 perpetrator of the killings at Fort Hood, Major Nidal Malik Hasan, and a cleric in Yemen with al-
14 Qaeda connections, Anwar al-Awlaki. (al-Awlaki was later killed in an attack by a U.S. drone in
15 Yemen). Because of the emails and other factors, critics complained that the FBI should have been
16 alert to the threat that Major Hasan posed well before the killings. The Director of the FBI, Robert
17 Mueller, who has full knowledge of the PSP, answered questions about the emails at a Senate
18 hearing. As Mr. Binney explains in his declaration, Director Mueller's reply indicated the
19 existence of an NSA database of emails.

20 13. The attempted adoption of a mass data collection program in the United Kingdom
21 provides a further indication of the NSA's program. The British analogue to the NSA is an
22 organization dedicated to signals intelligence called the Government Communications
23 Headquarters (GCHQ). The GCHQ is the NSA's oldest and closest collaborator in intelligence
24 matters, and the GCHQ and NSA often work together in matters of common interest. In 2008, the
25 GCHQ sought government funds for a substantial expansion of its buildings and infrastructure (not
26 unlike the NSA's expansion in Utah and Ft. Meade). The GCHQ's plans included the creation of
27 an enormous central database to store the details of every phone call, email, and Internet search
28 made in the UK. The project was named Mastering the Internet or "MTI." GCHQ inadvertently

1 disclosed the MTI project through a job placement advertisement in the computer trade press. A
2 public outcry ensued, and the Home Secretary was compelled to announce publicly that GCHQ
3 would abandon its plans for the construction of a central database.

4 14. My assessment is that the GCHQ's experience in the U.K. confirms that a central
5 database is within the contemplation of the signals intelligence community and suggests that the
6 GCHQ's MTI project is an attempt to follow the NSA's lead.

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

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

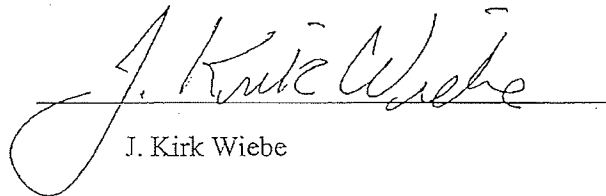
19
20 
21 J. Kirk Wiebe

EXHIBIT A

J. Kirk Wiebe

– *Intelligence Professional/Business Process Engineer* –

Skill Areas: Change Management (supervisory); Knowledge Management; Teaching; Intelligence Analysis; Workflow Analysis; Business Process Reengineering; Information Management.

Degrees, Certifications, and Licenses

- ◆ Bachelor of Arts Degree, Indiana University – 1969
- ◆ Master of Arts Degree for Teachers, Indiana University – 1974
- ◆ NSA Speech and Graphic Language Analysis Professional Certification – June 1976

Description of Most Recent Position

November 2005 – 15 June 2006 - Entegra Systems Inc.

Mr. Wiebe applied advanced analytic techniques to support analysis efforts associated with the modernization of U.S. Customs and Border Protection Targeting and Analysis systems. Mr. Wiebe conducted an evaluation of CBP data quality, identified existing gaps in the modernization effort from an enterprise perspective, and recommended steps for aggregating and analyzing Cargo, Passenger, Law Enforcement, and Counter Terrorism-related data from multiple sources. In addition, Mr. Wiebe and a colleague made an important intelligence discovery that ultimately led to the arrest of individuals involved in the illegal export of components used to detonate IEDs (improvised explosive devices) used against U.S. and coalition forces in Iraq and Afghanistan.

Past Positions and Major Accomplishments

1) Knowledge-Discovery and Analysis for Major Government Agency, Herndon, VA

July 2003 through August 2004 – Mr. Wiebe assisted in leading an effort to reengineer an existing Information Technology-based analysis business process for a major government agency. Mr. Wiebe employed specialized analytic methods to discover previously unknown entities of interest to the customer and associated knowledge, and he identified unique entity profiles based on observed behavior patterns that had not been previously recognized or defined.

2) Entity Mapping/Relational Intelligence Demonstration, Boeing Corporation, Herndon VA

July 2002 – November 2002 – Mr. Wiebe participated as a member of Entity Mapping, LLC on an IR&D contract with Boeing to demonstrate advanced analytic concepts. As a member of the lead development team, he provided a briefing on underlying processes and results to senior Boeing managers and technicians.

3) SIGINT Automation Research Center/National Security Agency

July 2000 through October 31, 2001 (date of retirement) – Mr. Wiebe collaborated with teams of innovative analysts, computer scientists and programmers to improve the intelligence analysis business processes in support of rapidly evolving corporate NSA business objectives and goals.

4) New Analysis Techniques Center for Operations/National Security Agency

April 1999 through July 2000 – Mr. Wiebe led a team to stand up a major new analysis organization in operations. He recruited essential manpower to provide budgetary and other staff support to management of the new organization, obtained logistics support, and liaised with IT services to provide necessary computers and software for the organization's leadership and staff organizations.

5) Information Technology Services Organization/National Security Agency

November 1997 through March 1999 – Mr. Wiebe served as the enterprise's IT services representative to two important strategic planning activities aimed at transforming analysis and intelligence production capabilities in the operations organization. He provided expertise and led key efforts to define the roles of Knowledge Management and Business Process Reengineering as critical components of NSA's transformation effort to improve intelligence production processes.

6) Distributed Computing Services Organization/National Security Agency

July 1996 through December 1997 – Mr. Wiebe collaborated with senior management to obtain congressional support resulting in the first NSA budget containing funding specifically for IT infrastructure. Led the organization's effort to define and implement performance goals and objectives, replete with metrics for measuring progress over time. Initiated and led a planning team composed of technical and operations experts to define critical planning issues

involving modern networked communications that culminated in the publication in December 1997 of a key planning document supporting transformation goals.

February 1995 through July 1996 – Mr. Wiebe managed an IT development and support organization of 70 computer scientists, programmers, and language analysts focused on improving digital storage and distribution processes supporting analysis and intelligence production activities for the operations organization.

7) Operations Senior Staff Organization/National Security Agency

March 1993 through January 1995 – Mr. Wiebe managed policy, auditing, property accountability, and internal management control issues and strategic planning activities for the operations organization.

8) Collection Operations Organization/National Security Agency

May 1992 through February 1993 – Mr. Wiebe developed concepts of operations and functional standards definitions for major systems development planning, and he led a small team of operations and technology experts to develop requirements for dynamic communications supporting NSA and three regional operations centers.

9) Strategic Weapons Analysis Organization/National Security Agency

October 1989 through May 1992 – Mr. Wiebe managed a work center of 50 analysts responding to intelligence requirements levied by President Reagan and U.S. national command authorities. Mr. Wiebe collaborated with Intelligence Community partners to study foreign strategic missile systems and to define improvements to national technical means. He also presented key analysis and planning briefings to senior managers, senior officers of the Strategic Air Command, as well as dignitaries, including the Secretary of the Air Force, Chiefs of the HPSCI and SSCI staffs, as well as the then Secretary of Defense designate, Congressman Dick Cheney.

Prior Career History

- ♦ June 1975 – October 1989: Numerous technical and supervisory positions focused on training and performing intelligence analysis in support of NSA operations
- ♦ June 1969 – June 1975: Direct sales and regional sales manager positions with Health Mor, Inc. in the state of Indiana.

Military Service

- ♦ United States Air Force Security Service: December 1964 – August 1967, with assignments at Karamursel, Turkey and Wakkanai, Japan respectively

Honors, Awards, and Special Achievements

- ◆ The Pennsylvania State University, College of IST Colloquium Speaker's award - 2007
- ◆ Strategic planning (NSA) award for initiating and leading a collaborative planning activity leading to the publication of a key Concept of Operations planning document focused on the global digital network - 2001
- ◆ Ann Caracristi Award (NSA) for work leading to a greatly improved ability to produce intelligence from a specific type of source material - November 2000
- ◆ Strategic planning (NSA) awards for critical transformation planning activities during the period April - December 1999
- ◆ National Meritorious Unit Citation (Intelligence Community) from the Director of the CIA for work accomplished while leading a group of NSA analysts working on a defense project of national-level significance - June 1991
- ◆ Meritorious Civilian Service Award (second highest NSA award) for efforts leading to major system acquisition to monitor foreign strategic weapons systems - January 1990
- ◆ Numerous awards for sales proficiency (50% closing average) while employed with Health More Industries in the state of Indiana June 1969 - June 1975

Self - Development and Training

- ◆ Change Management topics (NSA): 2001
- ◆ Enjoy building and upgrading computers and computer networks: 2000 - Present
- ◆ Course work (NSA) involving executive issues and management techniques: 1994 - 1995
- ◆ Information Resources Management College: Improved Factors in Decision-making - National Defense University - 1993
- ◆ Amateur ("Ham") Radio Operator since 1956

EXHIBIT B

Discovering and Protecting

- Guarding Privacy While Finding the Threat -

Mullah Omar
Kandahar,
Afghanistan

Ramzi Binalshibh
Hamburg, Germany

Muhammad
Hollywood, FL

Muhammad
Daytona Beach, FL

Mustafa Alhansawi
Dubai, UAE

Nawaf Alhazmi
San Diego, CA

Rhafiq Alhazmi
San Diego, CA

Muhammad
Hollywood, FL

Muhammad
Hollywood, FL

○	WANTED
○	U.S. WANTED
○	UNKNOWN
○	U.S. PROTECTED

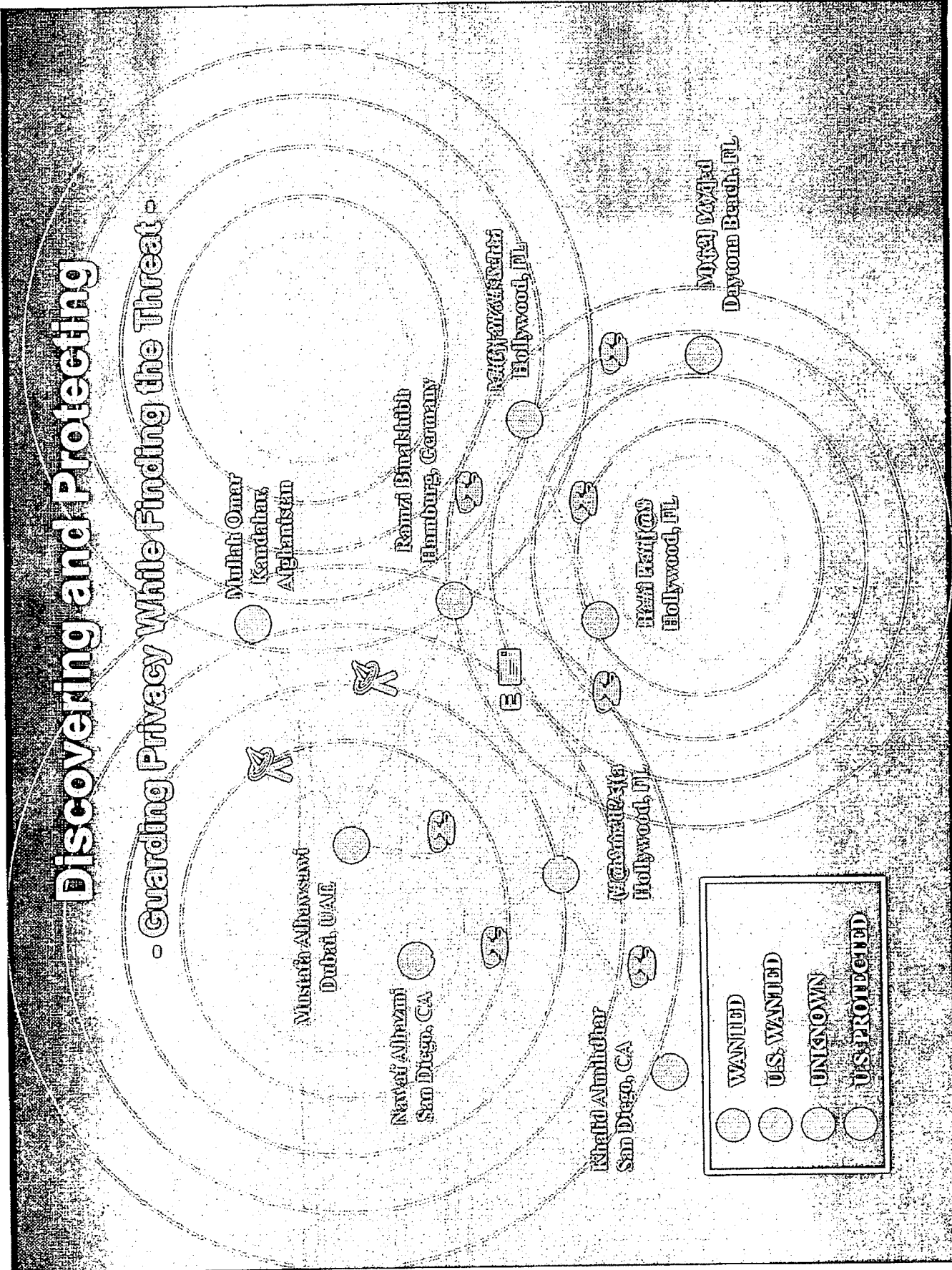


EXHIBIT C

1. Conflicting governmental interviews:

Statement #1 to S/A RP: MI called her; asked some questions, but she didn't tell him anything. That was the "only time she spoke with him."

Statement #2 to DOJ ER: "MI called and left message. I didn't talk to him."

2. Phone logs reveal multiple and lengthy (in the case of two such calls) voice and fax communications:

6/5 24 seconds - MI to JR

6/12 11:22 a.m. 20 minutes - MI to JR

6/13 11:36 24 seconds - MI to JR

12:00 MI to AUSA Bellows re: fishing

4:10 19 minutes - MI to JR

4:44 3 minutes 26 seconds - HDW fax to MI

5:46 28 seconds - MI to JR

6/14 11:00 MI to DOJ DuPew - "I have the e-mails."

12:00 21 seconds - MI to JR

6/15 Article published.

3. Three or four months ago, TF saw a "JR-MI" fax cover sheet on the printer table that he shares with JR. He asked her what she was faxing to MI and she froze up and never answered the question.