TOP SECRET [redacted]

FINAL REPORT

ATTORNEY GENERAL'S REVIEW TEAM ON THE HANDLING OF THE LOS ALAMOS NATIONAL LABORATORY INVESTIGATION

VOLUME III

CHAPTERS NINE - TWELVE

This document contains Restricted Data as defined in the Atomic Energy Act of 1954, as amended.

Derived From: Multiple Sources
Reason: 1.5(b), (c), (d) and (f)
Declassify On: X1

May 2000

Copy 32 of 45

TOP SECRET [redacted]

CHAPTER NINE

(U) THE SEARCH OF WEN HO LEE'S COMPUTER

Questions Presented:

Question One: (U) Whether Wen Ho Lee had a reasonable expectation of privacy in the LANL computer systems to which he had access.

Question Two: (U) (S/NF) Whether the preliminary inquiry concerning Wen Ho Lee in 1994 presented an opportunity to search the LANL computer systems used by Lee, without a warrant, on the grounds that Lee had no reasonable expectation of privacy in them.

Question Three: (U) Whether the FBI assigned agents with appropriate training and experience in computer crime investigations commensurate with the needs of the Wen Ho Lee investigation.

Question Four: (U) Whether FBI Albuquerque provided FBI Headquarters' National Security Law Unit with all facts in its possession that were relevant to whether a warrantless search of the LANL computer systems used by Wen Ho Lee was permissible.

Question Five: (U) Whether FBI Albuquerque displayed appropriate investigative zeal, and developed an appropriate liaison with knowledgeable LANL personnel, to uncover all facts relevant to the computer search issues.

Question Six: (U) Whether FBI Headquarters provided appropriate oversight and guidance to assist FBI Albuquerque to develop all facts relevant to the computer search issues.

Question Seven: (U) Whether FBI Headquarters' National Security Law Unit applied the correct legal standard in assessing whether a warrantless search of the LANL computer systems used by Lee was permissible.

Question Eight: (U) Whether the advice provided by FBI Headquarters' National Security Law Unit was legally correct and complete, appropriately communicated from FBI Headquarters to FBI Albuquerque, and accurately understood by the agents in the field.

(U) *PFIAB Question #4: Why the FBI's FISA request did not include a request to monitor or search the subject's workplace computer systems, particularly since an attorney in the FBI's General Counsel's Office had provided an opinion in 1996 that such monitoring or searching in this case would require FISA authorization.*

(U) *PFIAB Question #5: Why the FBI did not learn until recently that in 1995 the subject had executed a series of waivers authorizing monitoring of his workplace computer systems.*

A. (U) Introduction

(S/NF) In April 1994, the FBI opened a preliminary inquiry of Wen Ho Lee based upon [redacted] There is no indication, however, that any thought was given, at any point during the 18 months that the preliminary inquiry was open, to searching the computer systems to which Lee had access at the Los Alamos National Laboratory ("LANL"). In May 1996, the FBI opened a full foreign counterintelligence investigation of Wen Ho Lee, whom the FBI suspected of passing classified information concerning the W-88 nuclear weapons system to the PRC. In November 1996, FBI Albuquerque sought advice from the FBI National Security Law Unit ("NSLU") about searching Lee's LANL computer. Much remains unclear about this request for advice and the response to it from the NSLU and FBI Headquarters. This much is certain, however: The computer should have been, but was not, searched in 1996, and it should have been, but was not, searched in 1997 or 1998. Moreover, although it is a somewhat closer question, the computer should have been, but was not, searched in 1994. The consequence of these failures is breathtaking and

b1

potentially catastrophic: One of the most serious breaches in national security in modern United States history might have been stopped in its tracks, but was not.

(U) The FBI's attempt to gain access to LANL computer systems used by Wen Ho Lee was a catalog of missed opportunities, bad communication, inadequate legal advice, undue caution, lack of investigative zeal and ingenuity, and a wholesale failure to recognize the significance of Wen Ho Lee's work with and access to highly classified computer software and systems. Moreover, the FBI personnel working these issues were far too easily stymied by obstacles that could have, and should have, been overcome. For example, when the FBI was inaccurately told that the LANL computers did not have banners, which notify computer users of the possibility of monitoring, the FBI never investigated whether facts existed which might undercut any expectation of privacy on Lee's part, and which might thus obviate the need for such notice. When the FBI was told that Lee had not yet been registered into an on-line system containing an acknowledgment of computer monitoring, it took no steps to insure that Lee was immediately registered, or even to ascertain subsequently whether the registration had taken place. And, when it determined that a FISA order and probable cause was required to search Lee's computer, the FBI never considered whether significant – and, as it turns out, incriminating – information about Lee's computer usage could be obtained through other means that would not have required a showing of probable cause.

(U) In part, the FBI's computer search problems were the natural consequence of the FBI's focus on obtaining FISA coverage to the exclusion of other logical investigative strategies. In pursuit of FISA, the FBI adopted a "non-alerting" strategy that was, nominally at least, intended to preserve the maximum usefulness of the hoped-for FISA surveillance by minimizing contact with individuals at LANL, in the belief that they might, inadvertently or otherwise, alert Lee to the investigation. What proved more unfortunate, however, is that because of this singular focus on FISA, the FBI did not thoroughly question those at LANL who were interviewed about Lee's work with computers, beyond the minimum needed for inclusion in a FISA application. Consequently, the FBI cut itself off from, or failed appropriately to question, those who were most knowledgeable about LANL's computer systems and who would have been most helpful in supplying the facts that would have permitted a lawful search of Lee's computer. By this strategy, for example, the FBI kept itself from learning a fact that was literally just one question away: that Lee had executed a waiver in 1995 that would have

permitted the searching and monitoring of Lee's computer and e-mail messages, and that would have made a court order unnecessary.

(U) By a similar strategy, also intended to preserve the option of obtaining FISA surveillance, the FBI cut itself off from the Criminal Division at the Department of Justice, and in particular, from the Criminal Division's Computer Crime and Intellectual Property Section. Having deliberately avoided those most knowledgeable of the facts relevant to a search of Lee's computer, the FBI then avoided those most knowledgeable of the relevant law. The result, as discussed below, was that the agents in the field received advice that was inaccurate, incomplete and poorly communicated.

(U) Remarkably, this failure to pursue available information continued even after the FISA application was rejected, indeed, even after FBI Headquarters senior management was told that a more alerting strategy was to be adopted in the wake of the FISA rejection.

(U) The combined result of these and other lapses to be discussed in this chapter is that the FBI learned in 1999 what it could have, and should have, learned in 1996, or even in 1994. Had it done so, it would have become aware of Lee's computer misconduct years earlier – with all that implies about the possibility of minimizing damage to national security – and it well might have actually caught Wen Ho Lee "in the act" of downloading classified information in 1997.

B. (U) The relevant facts

1. (U) Wen Ho Lee's access to, and movement of, some of the nation's most sensitive nuclear weapons information, using his LANL computer.

~~(S/RD/NF)~~ The FBI now knows that at least as early as 1993, Wen Ho Lee began transferring classified files from the secure LANL computer systems to the open system.[574] According to the current case agent, SA [redacted] Lee gathered the classified files on the secure LANL computer system, altered the files to remove the classified marker preventing their transfer, moved the files to the open side of the system,

FBI
b6
b7C

[574](U) The LANL computer systems are described below. See Section B(13).

and from the open system downloaded the files onto 10 tapes. [redacted] 9/11/99 [redacted] 3/1/00; see also Wampler 12/17/99) All but one of the tapes was created in 1993 and 1994. (LANL 001954) [redacted] (Id.) The last tape, however, downloaded by Lee in April 1997, is the most significant, according to LANL experts, because it contains the most sensitive material of all those he created. [redacted] 9/11/99)

(U) (S) According to SA [redacted] the FBI has obtained logs from LANL showing the gathering, transferring, and downloading of these classified files, as well as the dates on which these actions were taken. [redacted] 9/11/99) This information was available on the LANL computer systems in November 1996 when FBI Albuquerque first sought advice regarding a search of Lee's computer. (Id.) It was also available in 1994. (Id.) According to SA [redacted] the names of the files Lee transferred were such that LANL scientists would have recognized them as classified from the file names. (Id.; see also Wampler 12/17/99; [redacted] 12/21/99) Had they been asked to review the list of file names contained on the logs, the LANL scientists would have been immediately suspicious that Lee had transferred and downloaded classified data onto the open system. (Id.) According to SA [redacted] if FBI Albuquerque had searched Lee's computer in November 1996, it would have found the vast majority of what it later discovered when Lee's computer *was* searched in March 1999. (Id.; see also Detention Hearing 12/27/99 Tr. 83-84)

(U) According to the December 10, 1999 Indictment against Wen Ho Lee, during 1993 and 1994, Lee collected, from LANL's secure computer network, secret restricted data ("SRD") and confidential restricted data ("CRD") contained in classified computer files, assembled the SRD and CRD material into "TAR" files,[575] and transferred these classified TAR files onto the open network at LANL. (Indictment ¶ 16) Nineteen such TAR files are involved in the Indictment. (Indictment ¶ 18) Once on the open network,

---

[575](U) A TAR file is an archive file into which groups of other files, perhaps thousands of files and file directory structures, can be collected and thereafter can be treated as a single file. (Detention Hearing 12/27/99 Tr. 31)

Wen Ho Lee, or anyone with Lee's "Z number"[576] and password, could have accessed and downloaded the classified TAR files, from anywhere in the world, through the Internet.[577] (AQI 06196)

(U) During 1993 and 1994, Wen Ho Lee downloaded 17 of these 19 classified TAR files onto nine portable tape cartridges. (Indictment ¶ 20) Then in 1997, according to the Indictment, Lee downloaded six more classified files onto a tenth portable tape cartridge. (Indictment ¶ 21) Some of these tapes were recovered during a search of Wen Ho Lee's LANL office in March 1999. [redacted] 9/11/99) Seven tapes, however, including the tape created in 1997, are presently unaccounted for. (Indictment ¶ 22; [redacted] 9/11/99)

FBI
b6
b7C

(U) Witnesses at the detention hearings following Lee's arrest described the significance of these classified materials. According to Stephen Younger, Associate Laboratory Director at LANL, the classified computer files that Wen Ho Lee downloaded and transferred to portable tapes included "source codes," which are written in a "human readable" computer language used in the design of nuclear weapons. (Detention Hearing 12/13/99 Tr. 11) These codes can be hundreds of thousands of lines long, and, according to Younger, "You can read it, so it represents, in essence, a graduate

---

[576](U) A "Z number" is a unique number assigned to each employee at LANL. (Detention Hearing 12/27/99 Tr. 27)

[577](U) (S/NF) Indeed, on March 2, 1998, shortly before a trip to Taiwan, Lee asked the LANL computer help desk how he could access the LANL system from overseas. (FBI 01986) Lee was given help on how he could access the open system from overseas. (FBI 13525) While in Taiwan, Lee accessed the directory on the open LANL system where he had previously moved the classified files. (Detention Hearing 12/27/99 Tr. 121-23) From Taiwan, Lee accessed File 19, one of the files charged in the Indictment, which contained a collection of classified files that Lee had assembled from the secure LANL system. (Id.) Lee then transferred two unclassified files from File 19, from the open LANL system to the computer he was using in Taiwan. (Id.) The FBI has been unable to ascertain from the available computer logs whether other, *classified* files were similarly accessed and transferred by Lee or by someone using his "Z number" and password. (Detention Hearing 12/29/99 Tr. 446-49)

course in nuclear weapons design." (Id.) These codes are "among the most complex computer simulation tools ever developed on the planet," they represent "person-centuries of effort," and "they have inside them the results of . . . a thousand nuclear tests that the United States has done over the past 50 years." (Id. at 12) These source codes were described by Richard Krajcik, Deputy Director of X Division at LANL, as the "crown jewels of the nuclear weapons program" in the United States. (Detention Hearing 12/27/99 Tr. 179) Younger described them as "priceless, they can't be duplicated." (Detention Hearing 12/13/99 Tr. 36)

(U) Lee downloaded source codes for both primaries and secondaries.[578] (Detention Hearing 12/27/99 Tr. 191) Code A, one of those involved in the Indictment, could be used for both secondaries and primaries. (Id.) Another code involved in the Indictment, Code G, was used for secondaries. (Id.) According to Krajcik, Lee "took, in essence, all that was worth taking with regard to American secondary thermonuclear design." (Id. at 193) Code B and Code I, also charged in the Indictment, were "the major codes to be used on the primary side." (Id. at 192) Code B "was the very latest information that we had. It was the very latest update," according to Krajcik, and Code I, "also was the latest vintage version of that code." (Id. at 194-195)

(U) Wen Ho Lee also downloaded onto the open system and transferred onto tapes "input decks," which, Younger explained, contain "[a]ll the materials and the geometry of the nuclear device." (Detention Hearing 12/13/99 Tr. 11) Krajcik described an input deck as containing the "electronic blueprint" of a nuclear weapon. (Detention Hearing 12/27/99 Tr. 189) "Basically, what it does is it tells you how you might build such a device," according to Krajcik. (Id.)

---

[578] (U) According to Younger, a modern nuclear weapon has two major parts. "There is a primary stage and a secondary stage. The primary stage is the part that has the plutonium in it. It's surrounded by high-explosive; high-explosive is detonated and presses the plutonium. The plutonium goes critical when it starts to generate nuclear energy. That energy is used to compress the second stage of the weapon, which is the secondary, and that is the stage that produces most of the military-effective yield of the device." (Detention Hearing 12/13/99 Tr. 9-10)

(U) Krajcik described the codes, input decks, and data files downloaded by Lee as "a chilling collection of codes and files." (Detention Hearing 12/27/99 Tr. 189-190)

> (U) Chilling in the sense that it contained the codes important to doing design or design assessment, files important to determine geometries, important successfully tested nuclear weapons. It contained important output setups, nuclear output setups. It contained devices across a range of weapons, from weapons that were relatively easy to manufacture, let's say, to weapons that were very sophisticated and would be very difficult to manufacture. It contained the databases that those codes would require to run. And for someone who used those codes to incorporate them into any kind of calculations that were made in terms of designing something new or checking something old, it was all there.

(Id.)

(U) According to Younger, "[t]he codes and the databases that were downloaded represent a complete nuclear weapons design capability, everything you would need to install that capability in another location, everything." (Detention Hearing 12/13/99 Tr. 27)

> (U) These codes and their associated databases, and the input file, combined with someone that knew how to use them, could, in my opinion, in the wrong hands, change the global strategic balance. They enable the possessor to design the only objects that could result in the military defeat of America's conventional forces. The only threat, for example, to our carrier battle groups. They represent the gravest possible security risk to the United States, what the president and most other presidents have described as the supreme

national interest of the United States, the supreme national interest.

(Id. at 38)

(U) The seven tapes that remain unaccounted for are, according to Younger, "a complete portable nuclear design capability which could be installed on a super computer center or on even lesser computer capabilities." (Detention Hearing 12/13/99 Tr. 39) According to Krajcik, the collection of the weapons codes and files downloaded by Wen Ho Lee existed only in two places in the United States: LANL and Lawrence Livermore National Laboratory. (Id. at 206) "And there is also this private collection that Dr. Lee has put together." (Id.)

2. ~~(S/NF)~~ Wen Ho Lee's [redacted] and the opening of the 1994 preliminary inquiry

b1

~~(S/NF)~~ [redacted] (FBI 02104)

FBI
b6
b7C

~~(S/NF)~~ The information provided by the source was transmitted by FBI San Francisco to FBI Headquarters in a March 1, 1994 teletype with a request that it be forwarded to, among others, SA [redacted] at FBI Albuquerque, who was

following the activities of [redacted] (FBI 02099) On March 31, 1994, FBI Albuquerque sent FBI Headquarters a teletype further describing [redacted] (Source #2). (AQI 03889) The teletype described Wen Ho Lee as "a weapons designer and part of the code development group in LANL's applied theoretical physics division." (AQI 03892) The teletype then went on to elaborate upon [redacted]

b1

(S/NF) [redacted]

(AQI 03892 (italics added)) The teletype concluded by noting the opinion of Source #2 [redacted] (AQI 03893)

FBI b6, b7C

(S/NF) On April 18, 1994, SA [redacted] sent an EC to the SAC Albuquerque recommending that a preliminary inquiry be opened "to determine the nature and extent of LEE WEN-HO's contact with PRC nuclear weapons scientists."[580] (AQI 02882) On April 20, 1994, a preliminary inquiry was initiated on Wen Ho Lee. (AQI 02830) On June 1, 1994, FBI Albuquerque sent a teletype to FBI Headquarters requesting that Source #1 be questioned about Lee. This teletype again repeated the earlier reporting

b1 [redacted]

(u)

FBI b6, b7C

[579](S/NF) In June 1998, Source #2 again provided essentially the same information to the FBI, specifically to SA [redacted] SA [redacted] and SA [redacted] (AQI 01795, 1796)

[580](S/NF) The EC recounts, nearly verbatim, the description contained in the March 1, 1994 teletype (FBI 02098)

b1 [redacted] (AQI 02882)

b1

[redacted] (AQI 02891) On November 7, 1994, FBI Albuquerque sent a teletype to FBI Headquarters requesting an extension of the preliminary inquiry "to bring this matter to a logical conclusion."[581] (AQI 02830) This teletype states [redacted] (AQI 02831)

(U) (S/NF) Under the AG Guidelines in effect in 1994, the FBI was permitted during a preliminary investigation to conduct searches "where there is no expectation of privacy and a warrant would not be required for law enforcement purposes." (OIPR 02034) As will be seen, Wen Ho Lee, like other computer users at LANL, had no reasonable expectation of privacy, and a search of Lee's computer could have been conducted at any time after the preliminary investigation began on April 20, 1994.[582] Had the FBI looked, it would have found startling evidence. For several months before the opening of the preliminary investigation, and for more than a month after, Wen Ho Lee had been moving highly prized and highly classified nuclear weapons computer codes and files from the secure computer network into a directory under his name on the open network at LANL. (LANL 001954 & 2054) There they remained until January 1999, where they could be accessed and downloaded by Lee, or by anyone who had obtained his Z number and password, from anywhere in the world. (Detention Hearing 12/27/99 Tr. 81-89)

---

[581] (U) (S) Under the Attorney General Guidelines for Foreign Counterintelligence Investigations ("AG Guidelines"), FBI Headquarters approval was required to extend the preliminary investigation. (OIPR 02035)

[582] (U) Because some of the factors that invalidate any reasonable expectation of privacy, such as the document Lee signed April 19, 1995 containing an express consent to monitoring and certain banners on LANL computer systems, came into existence after 1994, the question is somewhat closer in 1994 than when it later arose in November 1996. In our view, however, even without these additional factors, the LANL computer systems used by Lee could have been lawfully searched without a warrant in 1994. At the very least, the predicate for the preliminary investigation of Wen Ho Lee should have demonstrated to the FBI the importance of searching Lee's computer when the full foreign counterintelligence ("FCI") investigation of Lee began in earnest on May 30, 1996.

Had LANL scientists been asked by the FBI to look at Lee's computer directories in 1994, the file names of the computer codes themselves would have been recognizable to the scientists and would have alerted them to the possibility that Lee had left the "crown jewels," as Krajcik described them, out on the open network. (Id. [redacted] 9/11/99; [redacted] 12/21/99; AQI 06196)

FBI b6, b7C

DOE b6 b7C

(S/NF) Acting with reasonable dispatch after the initiation of the preliminary investigation, the FBI might have literally caught Lee in the act of downloading some of the computer codes and files, and creating some of the portable tapes, that are involved in the charges in the Indictment. Unfortunately, however, Lee's computer was not searched for another five years, and the preliminary investigation was closed in November 1995, in deference to DOE's administrative inquiry into the possible loss of the W-88 technology. (FBI 00404)

3. (U) Waivers, banners, booklets, and other documents bearing upon the expectation of privacy of computer users at LANL

(U) There appeared to be a universal sentiment among the LANL scientists interviewed by the AGRT that a computer user at LANL has no expectation of privacy whatsoever in his LANL computer. (Omnibus interview of [redacted] on 11/30/99 [hereinafter "Omnibus 11/30/99"]; [redacted] 12/20/99; [redacted] 12/21/99 [redacted] 12/21/99) This is well supported by banners appearing on computer screens, by express LANL policy articulated in booklets widely distributed to LANL employees, as well as by the "Rules of Use" waivers employed in X Division, where Wen Ho Lee worked.

DOE b6 b7C

(U) Computer users in LANL's X Division, where Wen Ho Lee worked, were required to sign "Rules of Use" forms that contained the following warning of possible monitoring:

> (U) WARNING: To protect the LAN [local area network] systems from unauthorized use and to ensure that the systems are functioning properly, activities on these systems are monitored and recorded and subject to audit. Use of these systems is expressed consent to such monitoring and

recording. Any unauthorized access or use of this LAN is prohibited and could be subject to criminal and civil penalties.

(Omnibus 11/30/99; [redacted] 12/20/99; [redacted] 12/21/99; [redacted] 12/21/99)

(U) Wen Ho Lee signed such a form on April 19, 1995 (FBI 00181 & 00183), although he had signed similar forms on previous occasions. According to [redacted] "Rules of Use" forms have been in use in X Division since the late 1980s. [redacted] 2/3/00) [redacted] produced an unsigned copy of a "Rules of Use" form, with a revision date of April 1991, that was in use prior to the form signed by Wen Ho Lee on April 19, 1995. (DOE 03562) The prior version, which was the one in use in April 1994 when the preliminary investigation was opened [redacted] 2/3/00), contained the following paragraph:

> (U) The resources of the X-DIVISION SECURE LOCAL AREA NETWORK are to be used only for official business purposes. DOE and Laboratory security policies require the audit of user files by security officers to assure this.[583]

(DOE 03562)

---

[583](U) A footnote to this paragraph reads:

> **(U) Audits are normally conducted by requesting information on selected files from the owner; however, inspection of individual files may be conducted by security officers under special circumstances, such as an actual or suspected security incident. In addition, individual files may be viewed by administrators in order to assist users, troubleshoot system problems, or upgrade systems. You will normally be notified of such access.**

(DOE 03563)

DOE b6 b7C

(U) According to [redacted] a copy of the "Rules of Use" form was to be posted near the user's workstation. In anticipation of annual, or sometimes more frequent, visits by DOE Albuquerque security auditors, members of [redacted] staff periodically inspected X Division offices to ensure that each workstation had the appropriate "Rules of Use" forms posted nearby.[584] (Omnibus 11/30/99)

(U) According to [redacted] both the open X Division LAN and the secure X Division LAN displayed a banner that alerted the user to the possibility of monitoring by referring to the "Rules of Use" forms each X Division user had signed.[585] (Omnibus 11/30/99) The banner read:

> (U) If you are an authorized user, your continued access to this computer facility carries with it your acceptance of the Rules of Use for this facility and your explicit agreement to abide by those rules.

(DOE 02052) The banner concluded with a notation indicating where the "Rules of Use" could be accessed on-line. In addition, the forms were posted at each computer

---

[584](U) According to [redacted] the forms were to be signed annually, and when a new form was signed, the old forms were discarded. (Omnibus 11/20/99) [redacted] confirmed that the April 19, 1995 "Rules of Use" forms signed by Wen Ho Lee (FBI 00181 & 00183) are the most recent, and only, forms available. (Omnibus 11/30/99) This is apparently because X Division was in the process of developing an on-line system to replace the paper "Rules of Use" forms. (Id.) From at least the time that [redacted] was responsible for [redacted] in 1991, [redacted] "can say with assurance that [Wen Ho Lee] would have signed a Rules of Use form or his account would have been disabled." [redacted] 2/3/00) [redacted] can thus say that Wen Ho Lee signed the Rules of Use form applicable in April 1994. (Id.)

[585](U) Signing of the "Rules of Use" forms was part of an annual re-validation process required of LAN users. In 1995 and 1996, as part of a process of going to electronic, rather than paper, re-validation, banners were put on the X Division LANs. The banners therefore were not on the X Division LAN in April 1994, but were certainly on all X Division LAN systems by November 1996. [redacted] 2/3/00)

DOE
66
67C

workstation. According to [redacted] this banner appeared each time a user logged onto his X Division workstation. (Omnibus 11/30/99)

(U) In addition to the X Division banners, a LANL computer user would also encounter banners each time she accessed any one of the machines on either of the lab-wide computer networks, the secure Integrated Computing Networks ("ICN") or the open ICN.[586] (Omnibus 11/30/99) This banner, which appeared throughout the period of the Kindred Spirit investigation, read as follows:

> (U) This computer is for authorized use only. All use is subject to audit and all use may be monitored. This computer system is operated under the auspices of the Department of Energy. Any misuse or unauthorized access is prohibited, and is subject to criminal and civil penalties. Evidence of unauthorized use may be provided to law enforcement officials.

(DOE 02053)[587] [redacted] confirmed that Wen Ho Lee would have regularly accessed one or more of these mainframe worker machines, such as Sigma, as part of his

---

[586](U) According to [redacted] the secure ICN contains supercomputers, storage, and specialized servers connected to users in other laboratory divisions and groups. The secure ICN includes the Central Filing System ("CFS"), which is a file storage server, and supercomputers, certain of which were known as Sigma, Tao, and Theta, on which complex computer functions could be performed on files accessed on the secure CFS. According to [redacted] the LANL open ICN provides internal and Internet access to 20,000 workstations and PCs across all divisions and groups. Services available in the open ICN include supercomputing, storage and archive, Web access, and Internet mail. The open ICN includes the open CFS. (Omnibus 11/30/99)

[587](U) This banner was not present in April 1994, but came into use in 1995. [redacted] 2/3/00) The banner quoted here thus was in use in November 1996. (Omnibus 11/30/99) It remained the same through July 1999. (Id.)

day-to-day job activities. (Omnibus 11/30/99) Each time Wen Ho Lee accessed one of these machines, the banner would have appeared. (Id.)

(U) In addition to the X Division banners, the ICN banners, and the "Rules of Use" waivers, there were other ways in which LANL personnel were informed that they had no expectation of privacy in their use of LANL computers.

(U) For example, when a user applied for an "account" on the lab-wide ICN system, which was necessary to gain access to the ICN systems, the user was given documents warning of monitoring as part of the process of obtaining a password from the Computing, Information and Communications ("CIC") Division at LANL.[588] Each user who applies for an ICN account was required to fill out a user validation form that contained a statement that the Operations Security and Computing Divisions had the right and responsibility to audit the user's computer use. (Omnibus 11/30/99) Once the application was made and the password was generated,[589] the user would be given a set of general rules that contained a similar statement. (Id.) According to [redacted] upon the issuance of a secure ICN password, each computer user would be given a document entitled "Receipt for Classified Password," for which the user would sign an acknowledgment of receipt. (Id.) The document states:

> (U) As an ICN user, you are responsible for assisting in the protection of the classified, unclassified sensitive, and unclassified data processed in the ICN from accidental or malicious modification, destruction, or disclosure. . . . All Laboratory computers, computing systems, and their associated communication systems are to be used only for official business. . . . The Facilities Security and Safeguards Division and Computing, Information and Communications

---

[588](U) To obtain an account on the X Division LANs, the user must first have obtained an account on the ICNs. (Omnibus 11/30/99)

[589](U) Passwords were assigned to users of the secure and open ICNs as well as the X Division LANs. Users were not permitted to choose their passwords. (Omnibus 11/30/99)

Division can and will audit your files to ensure that you abide by these rules.

DOE b6 b7C

(DOE 02054, 02057)[590] According to [redacted] a user's password expired periodically and the user would have to sign a similar document to obtain a new password.[591] (Omnibus 11/30/99)

(U) LANL personnel periodically received booklets that notified them that their computer use could be monitored and audited. According t[redacted] and former [redacted] Wen Ho Lee received regular briefings relating to computer security because DOE required annual refresher courses on the subject. (Omnibus 11/30/99) As part of this briefing, Lee would have been informed that the computer security staff had the right and responsibility to monitor LANL computers.[592] (Id.) [redacted] produced a booklet entitled "Security Refresher Briefing," dated [redacted] which [redacted] said had been distributed to all LANL personnel. (Id.) It states:

> (U) Laboratory computers, computing systems, and associated communications systems are to be used only for *official* business. OS Division and line managers have the responsibility and authority to audit all users' files. C

---

[590](U) The document produced by [redacted] which contains this statement is dated 6/19/97, but according to [redacted] the statement had remained the same since at least 1989. (Omnibus 11/30/99; [redacted] 2/3/00; DOE 03564) The only change was to reflect changes in the names of the responsible divisions. (Omnibus 11/30/99)

FBI b6 b7C

[591](U) The system administrator had access to all files of any LANL computer user, without the need for the user's password. [redacted] 9/11/99; Omnibus 11/30/99) According to SA [redacted] this was common knowledge at LANL, although SA [redacted] did not know specifically if Lee knew that the system administrator had this ability. [redacted] 9/11/99)

[592](U) This point was also made in periodic security briefings in X Division. (Omnibus 11/30/99)

Division also has this responsibility and authority to audit users' files in the Integrated Computing Network (ICN).

(DOE 02061, 02062 (italics in original))

DOE
b6
b7C

(U) a similar booklet entitled "Computer Security Reference Guide," dated It states:

> (U) Government resources, including computing and communications systems, are to be used *only* for official business . . . . The Laboratory has the responsibility for implementing an audit program to detect and deter infractions, waste, fraudulent use, and abuse of computing resources. To provide assurance and to comply with DOE Orders, *all* systems are subject to file audits. When you use Laboratory computing and communication resources, you should have no expectation of privacy. Your management . . . and DOE have both the authority and the responsibility to audit your files on *any* computing system used for Laboratory business.

(DOE 02058, 02059 (italics in original) (underline added)). According to distributed this booklet to each X Division employee. In addition, the computer security staff had the right and responsibility to audit and monitor LANL computers.[593] (Omnibus 11/30/99)

(U) In fact, according to booklets of the kind produced by from which the

[593](U) According to a "blue book" was distributed to LANL employees in 1996 that also stated that computers were subject to monitoring. According to a "no expectation of privacy" statement similar to that contained in the "Computer Security Reference Guide" was contained in the blue book. (Omnibus 11/30/99)

above quotations were taken, came out at least every year and were widely distributed to LANL employees. [redacted] was therefore adamant that LANL personnel had no expectation of privacy in the use of LANL computers.[394] (Omnibus 11/30/99) [redacted] sentiment was widely shared. According to [redacted] "if you're an X Division employee, you're told over and over and over again" that the computer systems are subject to being audited and monitored. (Id.) Similarly, according to [redacted] it has been clear since the 1980s that LANL employees have no expectation of privacy in their computers, that their computers are for official use only, and that LANL computers are subject to auditing and monitoring. [redacted] 12/21/99)

DOE 66 67C

(U) All of the foregoing documentation – the waivers, the banners, the booklets, and the other documents – dispelled whatever expectation of privacy Wen Ho Lee might otherwise have had. Yet, the FBI failed to learn of any of this until 1999. As discussed below, the explanation for this lies in a concatenation of failures at FBI Headquarters and FBI Albuquerque, including inattentive management, lax field work, poor communication within the FBI and between the FBI and DOE, and inaccurate and inadequate legal advice.

FBI 66 67C

4. (U) SA [redacted] discussions with [redacted] and the advice from NSLU

(U) In the fall of 1996, after the initiation of the full FCI investigation, SA [redacted] who had been assigned as case agent for the investigation, and [redacted] at LANL, spoke about Wen Ho Lee's computer at LANL. That is virtually all that can be said with certainty concerning the FBI's initial efforts, in 1996, to search Lee's computer or to monitor his use of e-mail. There is considerable disagreement among those involved as to whether "banners,"

---

[394](U) [redacted] also mentioned that his car has been searched by LANL security personnel on two occasions when [redacted] was leaving the LANL premises. This is not an uncommon occurrence, according to [redacted] Signs at the entrances to LANL and to the building where Wen Ho Lee worked state that all vehicles and containers entering and exiting LANL are subject to search. (Omnibus 11/30/99)

"waivers," or both were discussed,[595] and whether what was requested was the monitoring of Lee's e-mail, a search of Lee's computer, or both. It is also not clear whose idea it was to search Lee's LANL computer, nor exactly when it arose. According to SA [redacted] it was the idea of his supervisor, SSA [redacted] and came up during the discussion of another investigation. [redacted] 8/12/99) According to [redacted] it was his idea, which he mentioned to SA [redacted] when SA [redacted] had spoken to him about obtaining Lee's telephone toll records. [redacted] 9/13/99) According to SSA [redacted] it was first raised at a meeting with SA [redacted] and [redacted] while general investigative strategies were being discussed.[596] [redacted] 12/1/99)

(U)

(S) The earliest reference to this subject in the relevant documents is an electronic communication ("EC") indicating that on September 16, 1996, SA [redacted] had asked [redacted] for "the necessary paperwork which laboratory employees fill out concerning the right of the laboratory to review E-Mail messages." (AQI 01063) On October 16, 1996, SA [redacted] reported that [redacted] "had not devoted any attention to this matter but would do so soon." (AQI 01063)

(U)

(S) The next reference in the documents to searching Lee's computer concerns a November 4, 1996 telephone conversation between SSA [redacted] and [redacted] an attorney in the NSLU. (FBI 00192) According to SA [redacted] SSA [redacted] had called

---

[595](U) As used in this report, the term "waiver" refers to a document signed by the user affirmatively acknowledging that his use of the computer may be monitored, whereas a "banner" refers to a notice or warning that appears on the computer screen each time the computer system is "booted up." This appears to be the sense in which these terms were understood by those interviewed by the AGRT. A waiver may also be an electronic document subscribed to by the user as a condition of access to the computer system, the execution of which is done "on-line" and recorded electronically.

[596](U) According to [redacted] on the other hand, he knew nothing of the issue of searching Wen Ho Lee's computer and never spoke with the FBI about it. [redacted] 9/15/99)

for an opinion concerning whether the FBI could search Lee's computer.[597] According to SA [redacted] he was in the room at the time and memorialized the discussion in an EC:

FBI
b6
b7C

> (U) ~~(S)~~ SSA [redacted] questioned whether FISA authority would be necessary to conduct a search of Lee's computer at LANL or whether such a search could be conducted on the authority of LANL. [redacted] was of the opinion that such a search could be done on the authority of LANL authorities since the computer belongs to LANL, and there would be no expectation of privacy. [redacted] indicated his position may not be the majority view, and advised that he would research the issue.

(FBI 00192)[598]

---

[597](U) According to SSA [redacted] before his November 4, 1996 discussion with [redacted] he attended a meeting with SA [redacted] at which, among a number of other issues, accessing Wen Ho Lee's computer was discussed. One of the matters discussed was whether the FBI would be able to get physical access to the computer, and the LANL personnel told SSA [redacted] that that would be no problem. According to SSA [redacted] he speculated that the FBI would probably need a court order to search the computer. [redacted] 12/1/99) There was no discussion of waivers or banners at the meeting, according to SSA [redacted] (Id.) In a previous interview, however, SSA [redacted] said that he asked at this meeting about waivers and banners and was told by [redacted] that there were none. [redacted] 6/22/99)

DOE
66, 67C

DOE
66
67C

[598](U) [redacted] recollection of this first call is consistent with SA [redacted] EC. [redacted] understood that SSA [redacted] was inquiring about a government employee using a LANL computer in a suspected "65" (espionage) case, but not that it involved Wen Ho Lee. [redacted] 7/16/99) According to SSA [redacted] he had "maybe a couple" conversations with [redacted] SSA [redacted] does not recall the details of these conversations. SSA [redacted] said that SA [redacted] was not present when SSA [redacted] called [redacted] although SA [redacted] November 5, 1996 EC of SSA [redacted] conversation with [redacted] is accurate. SSA [redacted] could not recall if he had any conversations with [redacted] subsequent to the one documented in SA [redacted] EC. [redacted] 12/1/99)

DOE
FBI
b6
b7C

(U)
(S) In the November 5, 1996 EC, SA [redacted] informed SSA [redacted] at FBI Headquarters of this preliminary advice from [redacted] and of SA [redacted] discussions with [redacted]

(U)
(S) [A] request of LANL has been made for copies of the paperwork executed by LANL employees authorizing the review of E-mail traffic by LANL officials. Once this paperwork is obtained, it will be provided to FBIHQ for review by the [NSLU] for a determination as to whether the FBI would be able to obtain copies of E-mail on the authority of appropriate LANL officials.

(FBI 00192) Thus as early as this November 5, 1996 EC, confusion had crept into whether what was being sought was a "search of Lee's computer," as SSA [redacted] discussed with [redacted] or a "review of E-mail traffic," as SA [redacted] discussed with [redacted] (FBI 00192)

(U) According to [redacted] it was he who raised the issue of monitoring Lee's e-mail with SA [redacted] 9/13/99) In fact, according to [redacted] and SA [redacted] never talked about anything but how to capture Lee's e-mail, and they talked about that only because [redacted] raised it with SA [redacted] as a possibility. [redacted] 9/13/99) [redacted] recalled that LANL was in the process of creating a means to monitor e-mail in an unrelated matter. [redacted] asked SA [redacted] if the FBI would be interested in having this capability to monitor e-mail in the Lee investigation.[599] SA [redacted] said that he would check with FBI Headquarters. (FBI 00209; [redacted] 9/13/99)

(U) About a week later, SA [redacted] asked [redacted] for the administrative policy that permitted LANL to monitor e-mail. [redacted] 9/13/99) Because the LANL e-mail was a lab-wide system, when SA [redacted] asked for the administrative policy relating to e-

---

[599] (U)
(S) [redacted] recalled that the discussion followed a request by SA [redacted] for Lee's telephone toll records at LANL. [redacted] account is corroborated by SA [redacted] November 5, 1996 EC in which he notes his request to LANL for telephone records immediately before describing a request for "paperwork . . . authorizing the review of E-mail traffic." (FBI 00192)

mail monitoring, [redacted] went to the [redacted] at LANL. (Id.) According to [redacted] there was "never a discussion or hint or indication that I should look further to see if X Division had additional security." (Id.) [redacted] asked [redacted] for the documentation and provided it to SA [redacted] (Id.)

(U) (S) [redacted] gave the documents [redacted] had obtained from [redacted] to SA [redacted] on November 12, 1996, according to a file "insert" written by SA [redacted] (FBI 00194) Attached to the insert were the following documents: (1) a legal memorandum from LANL's general counsel's office, dated January 26, 1995, approving the monitoring of LANL electronic communications, "with appropriate notices and disclaimers to computer network users" (FBI 00197); (2) "computer security" documents containing suggestions for safeguarding information stored on computer (FBI 00204) and a notice of computer monitoring (FBI 00206); and (3) "Official Use Guidelines" for LANL computers (FBI 00195). According to SA [redacted] insert:

> (U) (S) [redacted] advised that the laboratory uses the authority of the opinion contained in item 1 above to monitor an employee's use of the Internet. Every employee who has a laboratory computer assigned must register that computer. By reading and agreeing to the information provided by [redacted] an electronic record showing that a laboratory employee had the opportunity to read and will abide by the rules will be created. This program was started approximately six months ago by Group 14 or the Facilities, Safeguards and Security Division. The goal is to have everyone at the laboratory with an assigned computer sign on to the new system. [redacted] advised that LEE has not yet registered his computer as of yet. [redacted] advised that LEE's division has not moved forward with this process.

(FBI 00194) This is consistent with [redacted] account.[600] [redacted] 9/13/99; FBI 00209)

---

[600] (U) (S) According to [redacted] he told SA [redacted] about a computer training program that was being implemented at LANL that was "designed to force every

FBI 66 67C

(U) The "electronic record" to which SA [redacted] referred in his insert included a "Computer Security Responsibility Acknowledgment" (FBI 00206), which had been given to [redacted] by [redacted] and which, in turn, [redacted] had given to SA [redacted] 9/13/99; [redacted] 8/12/99) The document contains the following notice:

> (U) Laboratory computer systems, networks, and communication facilities are for official use only and usage is subject to monitoring and/or auditing.

(FBI 00206)[601]

DOE 66 67C

---

computer user to read certain computer security information and notifications" and automatically record that the user had done so. After asking SA [redacted] permission to mention Lee by name, [redacted] checked with [redacted] who told [redacted] that Lee's division had not yet been included in this computer training program. (FBI 00210) According to SA [redacted] said that people in Lee's division had not yet signed "something," but SA [redacted] could not recall what it was. [redacted] 8/12/99) "Waiver" was not a term that was used, according to SA [redacted] (Id.)

[601](U) [redacted] identified the two "Computer Security Profile" documents (FBI 00204 & 00205) and the related "Computer Security Responsibility Acknowledgment" (FBI 00206), which were attached to the insert prepared by SA [redacted] as being documents that were generated as part of an on-line computer user registration program at LANL. Anyone with an account on the open computer network would have been asked to register, and DOE auditors checked to make sure that all users were registered, according to [redacted] As part of the registration process, the user would identify [redacted] security level and the program would generate two documents, one was a computer security profile that described the security precautions applicable to the selected security level, and the other was a computer security acknowledgment further outlining the user's security responsibilities. The notice quoted above appeared at the bottom of the second document. According to [redacted] the two documents would appear on screen when a user registered with the on-line system. They could then be saved or printed. The system would retain a record of who had registered. According to [redacted] made sure that X Division users registered with

(U) The third document that [redacted] gave SA [redacted] was entitled "Los Alamos National Laboratory Official Use Guidelines for Computing and Informational Systems." (FBI 00195) The document states:

> (U) Because these [computers] are government resources, Laboratory or the federal government may, without notice, audit or access any user's computer system or data communications. In addition, the Laboratory or the federal government may disclose any information obtained through such auditing to appropriate third parties, including law enforcement authorities.

(FBI 00195) Handwritten marginalia at the top of the "Official Use Guidelines" states that the document was "part of [safeguards and security] manual (on-line) published more than once in news bulletin."[602] (FBI 00195)

(U) According to SA [redacted] he read the documents he received from [redacted] but did not find them helpful. ([redacted] 8/12/99) Although SA [redacted] had undertaken in his November 5, 1996 EC to forward these materials to FBI Headquarters for review by the NSLU (FBI 00191), he never did so. ([redacted] 8/12/99) According to SA [redacted] he "got distracted." (Id.) Instead, SA [redacted] placed the documents in the FBI Albuquerque files and took no action on them. (Id.) SA [redacted] supervisor at the time, SSA [redacted] never asked him about the documents ([redacted] 8/12/99), and SSA [redacted] could not recall if he ever saw the insert with the attachments. ([redacted] 12/1/99) Nor did anyone from FBI Headquarters ask SA [redacted] for the materials ([redacted] 8/12/99; [redacted] 12/15/99), even though at the time, in the

---

the on-line system. (Omnibus 11/30/99)

[602](U) [redacted] confirmed that the "Official Use Guidelines," dated July 1995, were part of the Safeguards and Security Manual. The document was distributed via the news bulletin to every LANL employee. (Omnibus 11/30/99)

FBI
b6
b7C

margin of SA [redacted] EC, next to the passage indicating that SA [redacted] would obtain this documentation, SSA [redacted] penned the questions "So where is it? Sent to [redacted]"[603] (FBI 00717; [redacted] 12/15/99)

(U) It was *not* sent to [redacted] and, therefore, he did not have the benefit of these documents when SSA [redacted] came to him on November 13, 1996 to follow up on Albuquerque's request for advice. [redacted] had, however, spoken to his supervisor about the matter. [redacted] supervisor in the NSLU, Marion "Spike" Bowman told him that, as a general rule, there was an expectation of privacy on the part of government employees despite the fact that they are using government computers. [redacted] 7/16/99) According to [redacted] he was told by Bowman that unless there was a banner on the computer, a warrant would be required, and that even a banner might not be enough to permit the FBI, as opposed to the LANL system administrator, to search Lee's computer.[604] (Id.) In addition to talking with Bowman, [redacted] "thumbed through" some materials from the Computer Crime Section of DOJ's Criminal Division. (Id.) Ultimately, [redacted] concluded, since he had been told by FBI Albuquerque that there was no banner on the

---

[603](U) According to SSA [redacted] he expected the documents to be sent to the NSLU directly, because "it started with a direct question to NSLU." SSA [redacted] never asked SA [redacted] or SSA [redacted] about the documents. He did not ask [redacted] whether he had received them. He did not ask for the documents because "it was not my job." According to SSA [redacted] his only involvement in the computer search issue was to get an answer to FBI Albuquerque's question, as set forth in the lead at the end of the November 5, 1996 EC. The lead to the FBI's National Security Division was there, according to SSA [redacted] simply because [redacted] knew that it would be necessary to have someone at FBI Headquarters who could "twist an arm" to prod the NSLU to act on the request for advice. [redacted] 12/15/99)

[604](U) According to Bowman, he not only asked [redacted] if there was a banner on Wen Ho Lee's computer but also whether Lee had signed a waiver. (Bowman 8/11/99) Bowman said that he told [redacted] that unless there was some "fair notice" to Lee of possible monitoring, a warrant would be required to search the computer. (Id.) Thus, there is a significant discrepancy between [redacted] and Bowman's recollection of this conversation. If Bowman's recollection of what he told [redacted] is correct, this "fair notice" advice did not get imparted to FBI Albuquerque.

FBI
b6
b7C

computer at LANL, that the computer user had an expectation of privacy. (Id.) If there was no banner [redacted] therefore told SSA [redacted] he would need to get a warrant. (Id.)

(U) No one in the NSLU, however, considered whether the facts *specific* to Wen Ho Lee's LANL office or the LANL computer system might reveal that Lee had no cognizable expectation of privacy in the first place.[605] No one asked the agents about computer training LANL employees may have received that might shed light on their expectation of privacy. No one inquired about LANL policies concerning computer use. No questions were asked about the nature of the information available on the LANL computer system, to consider whether the employees might have differing expectations of privacy with respect to the various kinds of data captured by the LANL system about their computer usage. No one asked the agents to explore how the LANL computer system was structured, such as whether Lee had an office computer with a hard drive, or whether he merely had a "dumb terminal" connected to a remote server. No one in the NSLU raised with FBI Albuquerque or with SSA [redacted] whether something less than a comprehensive search of Lee's computer or real-time monitoring of Lee's e-mail might have been attainable without a FISA order. Most significantly, it appears that no one in the NSLU even asked the agents in the field a critical question: Had Lee signed a waiver? Finally, the NSLU never advised Albuquerque that it should ask LANL immediately to begin displaying banners on its computers, so that Lee's computer could have been searched at some time thereafter. Had it done so, FBI Albuquerque may have found out in 1996, rather than 1999, that banners were virtually ubiquitous at LANL and in X Division already.

---

[605](U) Whether an individual has a reasonable expectation of privacy involves two questions: First, whether the individual has exhibited an actual, subjective expectation of privacy, and second, whether the individual's subjective expectation of privacy is one that society would recognize as reasonable. Smith v. Maryland, 442 U.S. 735, 740 (1979). In the case of a government employee in particular, the Supreme Court has observed that "[g]iven the great variety of work environments in the public sector, the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis." O'Connor v. Ortega, 480 U.S. 709, 718 (1987).

(U) In short, the NSLU never asked any of the questions that, according to Scott C. Charney, former Chief of the Computer Crime and Intellectual Property Section, would have routinely been asked had the advice of the Computer Crime Section been sought in November 1996. (Charney 9/2/99) Instead, the NSLU simply advised SSA [redacted] that, unless there was a banner, a FISA order was required to search Lee's computer.[606]

FBI 66 67C

(U) (S) [redacted] advice to SSA [redacted] was communicated to FBI Albuquerque in a November 14, 1996 EC from SSA [redacted] addressed to the attention of SA [redacted] and SSA [redacted]

> (U) (S) On 11/13/96, SSA [redacted] met with [redacted] NSD-LU, ref AQ's 11/5/96 request for an opinion about the legality of monitoring subject's computer at LANL. Pointer advised it was the opinion of the NSD-LU that a FISA order would be the needed authority to surveil subject's computer.

(FBI 00207) Significantly, SSA [redacted] communication to FBI Albuquerque omitted [redacted] critical caveat: A warrant was required *unless there was a banner.*[607] Thus, the advice as to what was required in order to conduct a search had shrunk from what Bowman told [redacted] (FISA order, banners or waivers) to what [redacted] told SSA [redacted] (FISA order or banners) to what SSA [redacted] told FBI-AQ (FISA order). SSA [redacted] never had any direct conversation with SA [redacted] concerning the details of

---

[606](U) According to [redacted] if he were given the same information he was given in 1996, he would have given the same advice in 1999, though he allowed that he might ask whether Lee had signed a waiver. [redacted] 7/16/99)

[607](U) According to SSA [redacted] a copy of his November 14, 1996 EC to Albuquerque, relaying [redacted] advice (FBI 00720), would have gone to [redacted] "That's the custom," according to SSA [redacted] it is "always done." [redacted] 12/15/99)

this advice or its implications.[608] [redacted] 7/28/99 [redacted] 12/15/99 [redacted] 8/12/99) This writing is all that was communicated. [redacted] 8/12/99) SSA [redacted] did not recall his exchange with [redacted] except that the answer he got from [redacted] was "they can't do it."[609] [redacted] 12/15/99)

(U) Because SSA [redacted] EC stated categorically, and without [redacted] caveat, that "a FISA order would be the needed authority" to search Wen Ho Lee's computer, it was understood by Albuquerque to mean that a FISA order was the *exclusive* means by which the government could obtain access to the computer, regardless of whether a banner, waiver, or some other form of notice of monitoring existed. [redacted] 8/12/99) According to SA [redacted] the NSLU never said anything about waivers or banners, only that a FISA court order would be required to search Lee's computer. (Id.) The NSLU never suggested that he look into whether Lee had signed a waiver, according to SA [redacted] (Id.) In fact, according to SA [redacted] no one "up the chain" ever suggested any way to search Lee's computer other than through a FISA order, nor did anyone suggest that perhaps a waiver or banner would allow a search.[610] (Id.)

(U) This aspect of SA [redacted] account is in conflict, however, with statements made to the AGRT by [redacted] who said that shortly after [redacted] provided SA [redacted] with the three documents discussed above, SA [redacted] told [redacted] that it was the FBI's position that "if a banner did not pop up every time you log onto e-mail," the

---

[608](U) According to SSA [redacted] however, both he and SA [redacted] had a number of conversations with SSA [redacted] concerning the computer search issue. SSA [redacted] could not recall the details of these conversations. [redacted] 12/1/99)

[609](U) In fact, when initially interviewed on the subject, SSA [redacted] did not recall being involved in the computer search issue at all. [redacted] 7/28/99)

[610](U) SA [redacted] described himself as "computer illiterate," and at the time of the investigation would not have known what banners or waivers were, or the significance of them. [redacted] 8/12/99) In a different context, SSA [redacted] said that he was himself "computer illiterate." [redacted] 12/15/99)

DOE FBI 66 67C

FBI was not comfortable monitoring.[611] [redacted] 9/13/99) [redacted] then logged onto [redacted] e-mail and showed SA [redacted] that there was no banner.[612] (Id.) According to [redacted] SA [redacted] did not suggest, and [redacted] did not pursue, other means of gaining access to Lee's computer, because [redacted] understood from SA [redacted] that "it was a banner or nothing." (Id.) SA [redacted] account also appears to be in conflict with that of SSA [redacted] who said that SA [redacted] had told him that he had been told by [redacted] that there were no banners *or* waivers.[613] [redacted] 12/1/99)

---

[611](U) In an interview with the FBI, [redacted] said that SA [redacted] had asked [redacted] if there was a banner that appeared on the computer screen warning LANL employees that their communications could be monitored. (FBI 00209) According to [redacted] SA [redacted] later told [redacted] that "FBI HQ had made the determination that a court order would be required to conduct a search of LEE's computer." (FBI 00209) According to SA [redacted] although [redacted] mentioned banners "generally," SA [redacted] did not recall [redacted] saying anything, one way or the other, about banners on Wen Ho Lee's computer. [redacted] 3/12/99)

[612](U) According to [redacted] never talked to SA [redacted] about anything other than the lab-wide e-mail system. They never discussed the X Division computer systems. [redacted] 9/13/99) Although their accounts of their conversations differ, it appears that SA [redacted] questions to [redacted] about banners was limited, or at least was understood by [redacted] to be limited, to whether there was a banner on LANL's e-mail system. [redacted] 9/13/99; FBI 00209) It is undisputed that [redacted] told SA [redacted] that there was no banner. (Id.) According to [redacted] demonstrated this for SA [redacted] on his own computer. [redacted] 9/13/99) [redacted] did not encounter a banner, apparently, because [redacted] accessed only the LANL e-mail system, which, because it was an "off-the-shelf" software package, did not have a banner warning of possible monitoring. (Omnibus 11/30/99) [redacted] was unaware of the X Division banners and the banners that appeared when one of the machines in the ICN was accessed [redacted] 9/13/99), perhaps because [redacted] never had a need for the kind of computing for which one would have an ICN account (Omnibus 11/30/99).

[613](U) In an earlier interview, however, SSA [redacted] said that *he* had been told by [redacted] and [redacted] that there were no banners or waivers. [redacted] 6/22/99) Later, SSA [redacted] said that there was no discussion of banners or waivers with [redacted] and [redacted]

(U) (S) In any event, FBI Albuquerque was not satisfied with the guidance it received from SSA [redacted] and on November 21, 1996, a week after receiving SSA [redacted] EC telling FBI Albuquerque that it had to obtain a FISA warrant to conduct a search, SSA [redacted] and SA [redacted] called SSA [redacted] and pursued the issue with him. According to SSA [redacted] note to the file:

> (U) (S) [redacted] asked if it was okay to monitor subject's lab computer at LANL - not his private property, and e-mail is announced to be not private: NSD-LU said no - [FISA] needed - but now [redacted] asks if there might be a lower [FISA] standard here because the e-mail system is advertized as being not private. (?) I told [redacted] that the FISC judge is not going to swallow any concept of a lower standard - it's the law! [redacted] countered that perhaps a [FISA] really wasn't needed at all, and that NSD-LU was just being unnecessarily cautious! I told [redacted] I wanted electronic surveillance as much as he did - but this was not the way. We both agreed elsur on subject's home phone was what we really want.

(FBI 00714)[613] It appears from this note that although SA [redacted] may not have forwarded the documents he received from [redacted] the substance of them – that the computer "system is advertized as being not private" – was communicated to SSA [redacted] and SSA [redacted] and SSA [redacted] concluded, nevertheless, not only that a FISA was

---

[redacted] 12/1/99) [redacted] on the other hand, said that he did not discuss the computer search issue with SSA [redacted] (FBI 00212) And [redacted] said tha[redacted] had no involvement in the matter. [redacted] 9/15/99)

[613] (U) SSA [redacted] did not recall the specific conversation recounted in SSA [redacted] note, but said he had several conversations with SSA [redacted] about home and office privacy issues, and was attempting to determine if there might be a legal alternative to access the computer other than through FISA. SSA [redacted] recalls that SSA [redacted] said it had to be FISA. [redacted] 12/1/99) SSA [redacted] did not recall anything about this conversation, except that he thought it was "funny" that SSA [redacted] would think there was a lower standard for e-mail. [redacted] 12/15/99)

required, but also that whatever was "announced" or "advertized" did not warrant any further investigation or any consultation with the NSLU.[615] This suggests that SSA [redacted] too, believed a FISA order to be the *sine qua non* for a search of Lee's computer, regardless of [redacted] caveat about banners.

FBI 66 67C

(U) Clearly, the FBI agents involved in the investigation were familiar with the term "expectation of privacy" and its general significance in assessing the need for a search warrant. [redacted] 12/15/99; [redacted] 8/12/99; [redacted] 12/1/99) It is equally clear, however, that the agents lacked sufficient legal guidance to give the term real meaning in the context of the investigation and its objectives. Consequently, little or no thought was given to exploring the LANL work environment or the LANL computer system to determine whether other facts existed that would dispel any reasonable expectation of privacy.[616]

(U) NSLU's inadequate advice, and SSA [redacted] imprecision in communicating it, had unfortunate and far-reaching consequences for the investigation. The most immediate was that [redacted] did not take any steps to move up the date for X Division's implementation of the new computer training program. [redacted] 9/13/99) Nor did SA [redacted] ever request that [redacted] have the date for this program advanced for X

DOE 66 67C

---

[615](U) [redacted] was not contacted again after his November 13, 1999 discussion with SSA [redacted] According to [redacted] after talking to SSA [redacted] "the next thing that happened, I read about it in the Washington Post [in 1999]." [redacted] 7/16/99)

[616](U) In 1999, SA [redacted] SA [redacted] successor as case agent, wrote a note suggesting that FBI Albuquerque might have been aware of at least the theoretical possibility of conducting a search without a FISA warrant, but that, out of an abundance of caution, a warrant would be sought. According to SA [redacted] notes from May 1999, he "understood from [redacted] that it might be possible to look at E mail, but it had been decided to wait until we had court order, and therefore we would not take the chance of having incriminating evidence thrown out of court." (AQI 04249) To the extent that this suggests that FBI Albuquerque or SA [redacted] considered and rejected a search without a warrant as not being the safest course of action, there is nothing in the FBI records to support this. On the contrary, it is clear that throughout the investigation FBI Albuquerque believed that only a FISA order would permit a search.

FBI b6 b7C

Division. (Id.) Nor did SA [redacted] pursue information concerning the myriad banners, booklets, and waivers that would have conclusively established that Wen Ho Lee had no expectation of privacy in LANL's computer systems.[617]

(U) Obviously, had FBI Headquarters been aware of the waiver Wen Ho Lee signed in April 1995, a search of the computer systems to which Lee had access could have immediately taken place. Had that happened, we now know, the investigation would have taken a dramatically different turn.

5. (U) SA [redacted] learns of the significance of Wen Ho Lee's access to computer files, and nearly discovers Lee's waiver

(U) The FBI's failure aggressively and appropriately to pursue the computer search issue cannot be laid entirely at the FBI Headquarters' doorstep. Much of the blame for this potentially catastrophic error properly lies with FBI Albuquerque and its inexplicable failure to recognize that gaining access to Wen Ho Lee's computer files was the single most important investigative step that should have been taken. The truth, here, was only a tantalizingly few keystrokes away, but it depended on FBI Albuquerque discovering that Wen Ho Lee had no expectation of privacy. FBI Albuquerque's failure to discover this fact may be attributed *in part* to the bad advice it got from Headquarters, but only in part. Equally significant was that FBI Albuquerque was simply unmotivated

---

[617] (U) (S) As it turns out, Lee executed the on-line acknowledgment containing the notice of monitoring as part of this new training program sometime before May 1997. [redacted] 2/16/00; [redacted] 2/16/00) In a May 19, 1999 letter to Senator Murkowski of the Committee on Energy and Natural Resources, DOE General Counsel Mary Anne Sullivan states that Lee's execution of this acknowledgment took place in December 1996 and that SA [redacted] was notified of this at the time. (DOE 03579) SA [redacted] denied being told this, however, and [redacted] said that, after SA [redacted] told [redacted] of the FBI's position on banners, [redacted] did not have any further discussions with SA [redacted] concerning the search of Wen Ho Lee's computer. [redacted] 9/13/99; FBI 00210) [redacted] also said that [redacted] had not inquired into Lee's registering with this new system as of the time of [redacted] discussions with SA [redacted] in the late fall of 1997. [redacted] 9/13/99)

DOE b6 b7C

to pursue the "expectation of privacy" issue because it did not comprehend, or, if it comprehended, did not appreciate, the importance of Wen Ho Lee's computer activities. How that was possible, given what the FBI was learning, is unfathomable.

(U) (S/RD/NF) On December 9, 1996, SA [redacted] interviewed [redacted] X Division, where Wen Ho Lee worked.[618] SA [redacted] 302 of the interview captures the importance of the issue of Wen Ho Lee's access to W-88 weapons information through his LANL computer:

> (S/RD/NF) [redacted] Set-up decks are computer files which contain geometric and material information for the weapon design. Computer files are held individually with passwords but are shared widely among co-teams and design teams working on a problem pertaining to weapons design. [redacted]

(AQI 01151) From this interview, and that of [redacted] X Division, whom SA [redacted] interviewed on December 20, 1996 (AQI 01155),[619] it

---

[618](U) Albuquerque had been authorized to brief and interview Wen Ho Lee's supervisors, the director and deputy director of X Division on September 25, 1996. (FBI 00745)

[619](U) (S/RD/NF) [redacted] interview was as revealing as the interview of [redacted] on the significance of Wen Ho Lee's work with computers: "LBB writes software computer codes used to design nuclear weapons." (AQI 01156) [redacted] also told SA [redacted] that Lee had been working on such a code that "was used quite extensively for the W-88 design." (Id.) Yet the significance of Lee's access to these classified codes *through his LANL computer* obviously was lost on SA [redacted] who, after being given this information, questioned [redacted] about whether Lee had spent "excessive time . . . at the