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)

FBI b6 b7C

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

DOE b6 b7C

---

[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

should have been plain to SA [redacted] and to anyone who read the 302s, that gaining access to Lee's computer should have been a task assigned the highest priority.[620]

(U) [redacted] provided SA [redacted] with the name of someone who could have greatly helped in this regard. According to SA [redacted] January 8, 1997 EC to Albuquerque, [redacted] "advised that should the FBI need assistance, [redacted] is the [redacted] for X Division." (AQI 01143) Although the FBI did not know it at the time, [redacted] the "Rules of Use" forms which Wen Ho Lee [redacted] consenting to the monitoring, recording, and auditing of his computer use.[621] (Omnibus 11/30/99) Had [redacted] been asked about a LANL employee's expectation of privacy in the use of a LANL computer, [redacted] would have told SA [redacted] emphatically that there was none. (Id.) [redacted] certainly would have mentioned that every employee in X Division signed a "Rules of Use" waiver and could have provided SA [redacted] with the two waivers that Wen Ho Lee signed on April 19, 1995. (Id.)

(U) At this point in the investigation, then, the FBI was one interview away from discovering that Wen Ho Lee had executed a document that would have permitted the searching and monitoring of his LANL computers. But in fact, the FBI was one question away: [redacted] X Division, knew about the "Rules of Use" waivers that the employees under [redacted] were required to sign. [redacted] 12/21/99) So did

---

copier machine." (Id.)

[620](U) There is no indication in the relevant documents from FBI Albuquerque or FBI Headquarters that these 302s of [redacted] and [redacted] were forwarded to Headquarters. As discussed below, however, communications which should have been similarly enlightening were regularly sent to Headquarters.

[621] (U) [redacted] was [redacted] of [redacted] "Rules of Use" and the X Division banner. (Omnibus 11/30/99)

[redacted] 12/20/99) Neither was asked about Wen Ho Lee's expectation of privacy, however.[622] Had they been asked about this, both said, they would have referred the FBI agent to the "Rules of Use" forms. [redacted] 12/21/99; [redacted] 12/20/99)

(U) SA [redacted] did not pursue the computer issue further. [redacted] 8/12/99; Omnibus 11/30/99; [redacted] 12/21/99; [redacted] 12/20/99) Nor, apparently, did any supervisor from FBI Albuquerque or FBI Headquarters suggest that he should.

6. (U) The investigation is re-assigned to SA [redacted] who gathers more information on the significance of Wen Ho Lee's computer access

(U) SA [redacted] became the sole case agent in the Wen Ho Lee investigation in April 1997. [redacted] 9/12/99) According to SA [redacted] in reviewing the case file, he saw the November 14, 1996 EC from SSA [redacted] and understood that a FISA order was needed to conduct a search of Lee's computer. (Id.) SA [redacted] also recalled being told by SSA [redacted] that it was better to wait for a FISA court order before searching Lee's computer. (Id.) Therefore, SA [redacted] said that he did not give the idea of searching Lee's computer "a second thought."[623] (Id.)

(U) SA [redacted] did not recall ever being told anything about banners or waivers. (Id.) Nor did SA [redacted] ever ask [redacted] and [redacted] about banners or waivers, because

---

[622](U) Both [redacted] and [redacted] said that they were never asked by the FBI about searching Wen Ho Lee's computer. [redacted] 12/21/99; [redacted] 12/20/99) [redacted] "assumed" that Lee's computer would be monitored, since Lee was a suspect. [redacted] 12/21/99)

[623](U) In the spring of 1997, SA [redacted] spoke with SSA [redacted] about strategy of the investigation. SSA [redacted] related a story about another investigation in which three years of FISA surveillance had yielded so much information that when the suspect lied to the FBI agents in an interview, the agents were able to confront him, resulting in the suspect's confession. [redacted] 9/12/99) SSA [redacted] instructed SA [redacted] to collect enough probable cause to obtain a FISA order, and, according to SA [redacted] it was clear that the goal of the investigation at this point was to obtain FISA authority for telephone surveillance of Wen Ho Lee. (Id.)

"that decision had already been made."[624] (Id.) Meanwhile, the FBI continued to amass information pointing to the importance of Wen Ho Lee's computer access.

FBI b6 b7C

~~(S/RD/NF)~~ In a March 28, 1997 EC to SSA [redacted] at FBI Headquarters, SA [redacted] described, as had SA [redacted] before him, the significance of the computer codes to which Wen Ho Lee had continuing resort. (AQI 01210; FBI 00799) SA [redacted] reported that he had learned [redacted] (Id.) SA [redacted] then went on to explain that Lee would soon be working again with these two codes on a project to develop new weapons codes that "will be used to determine the effectiveness/status of the U.S. Nuclear Stockpile." (Id.; FBI 00973) b1

~~(S/RD/NF)~~ [redacted]

(AQI 01210; FBI 00799)[625]

---

[624](U) Therefore, when SA [redacted] was told by [redacted] in April or May of 1997 that LANL had an "administrative right to look at e-mail," SA [redacted] "probably" told [redacted] that a court order would be necessary. [redacted] 9/12/99) According to SA [redacted] he was afraid of jeopardizing the investigation by getting e-mail information through the DOE administrative process rather than through a FISA court order. (Id.) Note that SA [redacted] conversations with [redacted] concerned access to e-mail; not a search of Lee's computer. (Id.) [redacted] did not recall discussing Wen Ho Lee's computer with SA [redacted] 9/13/99) DOE b6 b7C

[625](U) SSA [redacted] did not recall hearing that Lee could have had access to the W-88 design from the computer. [redacted] 2/15/99) SSA [redacted] thought that Lee would have had to go to the vault. (Id.) That is what he was told by LANL scientists in

(S/RD/NF) If any doubt remained concerning the importance of Wen Ho Lee's computer access, it should have been dispelled by the FBI's April 10, 1997 re-interview of [redacted] (FBI 00803) According to the 302, which was forwarded to FBI Headquarters on May 15, 1997, [redacted] told SA [redacted] that Lee "will be assigned in the near future to a team that will develop a simulation code (design code). [redacted] They would simulate this weapon on a computer to test it."[626] (FBI 00803)

DOE FBI b6, b7C

b1

(U) (S/RD/NF) On April 15, 1997, SSA [redacted] and SA [redacted] met with [redacted] and [redacted] and others from LANL and DOE to discuss, among other things, Wen Ho Lee's assignment to work on the team to develop the new computer codes. [redacted] of DOE's Counterintelligence Division, summarized the meeting in a memorandum that was faxed to SSA [redacted] at FBI Headquarters on April 24, 1997:

DOE FBI b6, b7C

> (S/RD/NF) [redacted] . . The [redacted] are important to the primary design of future thermonuclear weapons designed by X Division. . . [redacted] Further, SUBJECT was considered an "expert" in this area.

b1

(AQI 01257)

FBI b6, b7C

1996, according to SSA [redacted] (Id.) Whatever SSA [redacted] may have been told in 1996, however, it is clear from these documents sent to SSA [redacted] that Lee's most dangerous access was through the computer.

[626](U) This interview also represents another missed opportunity for the FBI to have learned of the "Rules of Use" waiver signed by Wen Ho Lee, and other X Division personnel, including [redacted]

DOE b6 b7C

(U) According to [redacted] he was trying to be very clear at this meeting that the process of developing weapons codes was like software development. [redacted] 12/20/99) [redacted] explained at the April 1997 meeting that codes are the same thing as software programs. (Id.) [redacted] recalled that he tried to explain this because he felt that there may have been some confusion about what weapons codes were. (Id.) According to [redacted] if the FBI did not understand at the April 1997 meeting that Wen Ho Lee's work was on computer, [redacted] 'would be concerned about their being on the investigation." (Id.)

(U)
(S/NF) According to [redacted] summary of the meeting, it was decided at the April 15, 1997 meeting that it would be "illogical" not to assign Wen Ho Lee to the Legacy code team, first, because he was merely a suspect, and, second, because he would become suspicious if he were not assigned, since he was an expert in this area. (FBI 00846) It was agreed, however, that Lee's [redacted] would be briefed on the investigation so that [redacted] could monitor Lee's activities.[627] (Id.) According to [redacted] it was discussed at the meeting that they would restrict Lee's *reason* for having access to certain classified information by limiting what he would be

---

(U)
[627] (S) This presented yet another opportunity for the FBI to learn about the X Division "Rules of Use" forms relating to computer monitoring. [redacted] 12/21/99) SSA [redacted] and SA [redacted] briefed and interviewed [redacted] on April 28, 1997. (FBI 00883; AQI 01324) [redacted] told SSA [redacted] and SA [redacted] that Wen Ho Lee had been on the "Q" team for "a couple of years," at least until 1986. As part of the new team [redacted] told them, "Lee would have access to the crux of the research." [redacted] also explained that Lee had "unlimited access to computers." (Id.) This 302 was sent to SSA [redacted] on May 6, 1997. (AQI 05022) According to [redacted] told SA [redacted] about the weapons design process and how codes work in the lab. [redacted] explained that Lee was a code developer. [redacted] made clear to SA [redacted] that "codes" referred to computer codes. [redacted] 12/21/99)

working on and whom he would be working with; nevertheless, because Lee was an X Division scientist, "Lee's access would be the same before and after" the meeting.[628] [redacted] 12/20/99)

(S) Following the meeting at LANL, SSA [redacted] undertook to draft a FISA application, in light of Lee's request to have a PRC student [redacted] work with him on a project at LANL. [redacted] 7/23/99; FBI 00847) Although it was SSA [redacted] intent, at least initially, to include Lee's computer among the targets of the anticipated surveillance [redacted] 9/12/99; AQI 05568), evidently no one ever sought additional advice from the NSLU or elsewhere concerning how the FBI might immediately search or monitor Lee's computer. [redacted] 7/28/99 [redacted] 7/16/99) No one asked about the materials SA [redacted] said he would obtain concerning LANL's ability to monitor its employees' e-mail. [redacted] 12/15/99) No one asked about the electronic waiver that by now Lee had executed as part of the new computer training. [redacted] 9/12/99) Instead, the FBI focused exclusively on obtaining FISA surveillance of Lee.

7. (U) SA [redacted] assembles information concerning Wen Ho Lee's computer for use in the FISA application

(U) SA [redacted] notes reflect that, at SSA [redacted] instruction, SA [redacted] assembled information concerning the computers used by Wen Ho Lee so that these computers could be included as targets of the FISA surveillance. On April 25, 1997, SSA [redacted] told SA [redacted] that he was drafting the FISA application and that, among other things, he wanted to "get coverage for computer." (AQI 05570) On April 28, 1997, SSA [redacted] called SA [redacted] to discuss information that was needed for the application, and in discussing coverage for the computer, SSA [redacted] asked "does he have his own computer or is it shared." (AQI 05573)

(S/NF) On April 29, 1997, SSA [redacted] sent Albuquerque a draft FISA application for SSA [redacted] and SA [redacted] to review. (AQI 05387) In the first draft of the

---

628 (S) In an April 25, 1997 EC, SA [redacted] informed SSA [redacted] that it was agreed at the meeting that Wen Ho Lee "would not be restricted as far as his normal duties at the lab are concerned. It was agreed that Lee's new team assignment would go into effect as previously planned." (FBI 00851)

FISA application, as the centerpiece of the evidence offered to establish probable cause, SSA described the incident at LANL

(Id.)

The draft goes on to explain the importance of these codes: "[U]sing supercomputers and knowledge of fluid dynamics, [the energy released in a thermonuclear explosion] can be mathematically modeled and weapons subsequently designed for maximum size, weight, and yield." (AQI 05400) From the start of the drafting process, therefore, it should have been apparent to all involved that gaining access to Wen Ho Lee's computer was essential.

(U) SA notes show that he had a meeting with SSA on April 29, 1997 regarding the FISA application. (AQI 05367) Among the targets of surveillance, SA had listed "home computer" and "office computer." (Id.) Next to this last item, SA had written, in parentheses, "I think" and "has he attempted to access areas of computer which he is not authorized to access." (Id.) Thus, SA was zeroing in on a crucial investigative step.

(U) (S/NF) In fact, on May 6, 1997, SA interviewed and learned that Wen Ho Lee was "quite sophisticated on a mainframe computer . . . [but] less sophisticated regarding a personal computer."[629] (FBI 00891) SA and then discussed whether Lee was "sophisticated enough . . . to download information from a main frame computer to a disk." (Id.) As it turns out, of course, Lee was quite able to

[629](U) This 302 was sent to SSA on May 15, 1997. (AQI 01293; FBI 00910)

download from the LANL closed computer system, and had most recently done so, with some of the nation's most valuable secrets, less than a month before SA [redacted] and [redacted] had this conversation.[630] [redacted] 9/11/99)

(U) Unfortunately, however, this is as close as the FBI ever got to discovering the importance of the computer search issue, until Wen Ho Lee's computer was finally searched in March 1999. On the draft FISA application SSA [redacted] sent to SSA [redacted] and SA [redacted] under the section entitled "Requested Surveillance," SA [redacted] had added in handwriting "home computer" and "office computer." (AQI 05408) This last entry is lined through, however, with the words "per JS [SSA [redacted] 5/2/97." (Id.)

(U) There are a number of additional references in SA [redacted] notes relating to Lee's office and home computers, in anticipation of including them in the FISA application. (E.g., AQI 05562; AQI 05566; AQI 05563; AQI 05353) Many of these reflect conversations SA [redacted] had with [redacted] or both. (AQI 01273; AQI 05357; AQI 05575; AQI 05578; AQI 01322) One on May 16, 1997 states that [redacted] had suggested that Lee's e-mail be included. (AQI 05359) Another on May 20, 1997, reflecting a conference call among SSA [redacted] SSA [redacted] and SA [redacted] states "We will include the following items in the request to FISA court: . . . (C) work computer (D) clone account for work computer." (AQI 05353; see also AQI 05354; FBI 01015) However, SA [redacted] notes from June 5, 1997, the day that the draft FISA application was completed and sent to the NSLU, show that SSA [redacted] decided that he wanted to "get up on the phones" right away and did not want to wait to obtain the necessary information regarding Lee's home computer. (AQI 05348) It remains unclear why a request for Lee's office computer was also omitted, however.[631]

---

[630] (U) (S) SA [redacted] reported in the 302 of this interview with [redacted] that "Lee would not have been able to access data from his home. Lee would have had to load the information on a floppy disk, and take it home." (FBI 00891) This presumes, however, that Lee had not transferred files from the classified to the open system, which, of course, Lee was ultimately charged with doing.

[631] (S) According to SSA [redacted] the focus of the FISA application was on potential conversations between Wen Ho Lee and the PRC student [redacted] Initially, SSA [redacted] said that the computer was not included because he "did not think of it."

FBI b6 b7C

DOE b6 b7C

(U) It is baffling that SA and Lee's X Division could have had so many conversations regarding Lee's LANL computer, in the particular context of seeking authority to search it, and neither the subject of Lee's X Division "Rules of Use" waiver, nor that of the newer, on-line acknowledgment of computer monitoring, ever came up.[632] It is evident from interviews of however, that had FBI management – properly advised by the NSLU – directed the agents in the field to focus on gathering the facts necessary to determine whether Lee had a subjective expectation of privacy in the first instance, the waivers must certainly have been uncovered.[633]

7/28/99) It is obvious from SA notes that the computer was thought about and was *intentionally* excluded. When told of SA notes, SSA said that he believed that the computer was not included in the FISA application because SSA did not have information from SA although SSA was not clear about what information he thought was lacking. 12/15/99)

[632](U) recalled SA asking about the computer equipment used by Wen Ho Lee. He recalled providing SA with a list of Lee's equipment. did not recall if knew at the time why SA wanted this information. did not think that he ever asked. did not recall a discussion of searching or monitoring Lee's computer in the 1997 or 1998 time frame. could not recall ever talking to SA about searching Lee's computer. In fact, did not recall talking to anyone about searching Lee's computer before March 1999. believed that did tell SA about the "Rules of Use" forms. said that this is "the type of thing" would have mentioned to SA could not be certain of this, however. 12/21/99)

[633](U) One of the explanations given for the FBI's failure to discover the waivers was its desire during the investigation to be "non-alerting," which constrained its ability to interview individuals who had knowledge of the waivers or the architecture of the LANL computer system. This is unpersuasive, however, since the FBI was already in contact with those with knowledge Moreover, the FBI was willing to expand the list of those with knowledge of the investigation when it deemed such an expansion necessary. For example, the FBI notified two individuals in LANL Telecommunications to assist in planning the installation of equipment necessary to monitor Lee's telephone in anticipation of the granting of the FISA order. (AQI 01452)

(U) On August 12, 1997, OIPR rejected the FISA application. This event should have caused a comprehensive review of the FBI's efforts to gain access to Wen Ho Lee's computer files and to consider alternative means of gaining access. It did not. Instead, the computer search issue simply fell off the map, not that it was ever very much on it to begin with. It would not be until the spring of 1998 that the issue even came up again.

FBI 66 67C

8. (U) SA [redacted] arrives at the Albuquerque Division and is assigned to be the FBI's liaison with LANL

(U) In the spring of 1998, SA [redacted] who had been assigned to work as the FBI's counterintelligence liaison with LANL, was asked by her supervisor, SSA [redacted] to review the file in the Lee investigation. Because it involved LANL, SSA [redacted] wanted SA [redacted] to become "intimately familiar" with the investigation, although she was not then assigned to it. [redacted] 9/7/99) As a result of this review, SA [redacted] learned that a search of Wen Ho Lee's computer had never been performed. According to SA [redacted] who had previously worked on the FBI's National Computer Crime Squad, the fact that the computer had not been searched in the Lee investigation "stuck out like a sore thumb." (Id.) SA [redacted] wanted to know "why on Earth haven't they looked at the guy's computer, this being an espionage case." (Id.) To find out why, SA [redacted] spoke with her supervisor, SSA [redacted] with the case agent at the time, SA [redacted] and with [redacted] (Id.)

DOE 66 67C

(U) Some time in the spring of 1998, SA [redacted] spoke to [redacted] who told her about [redacted] earlier conversations with SA [redacted] 9/7/99; [redacted] 9/13/99) According to [redacted] told SA [redacted] that SA [redacted] had said that it was the FBI's position that unless a banner appeared on Lee's LANL computer, the FBI could not search Lee's computer without a warrant. [redacted] 9/13/99) According to SA [redacted] told her that SA [redacted] had said that the FBI could not search Lee's computer without a warrant, and, since the FBI did not yet have sufficient probable cause to obtain a warrant, there was nothing else that could be done. [redacted] 9/7/99)

The FBI simply did not recognize the necessity of additional interviews of individuals knowledgeable about LANL's computer systems.

FBI 66 67C

DOE 66 67C

(U) According to SA [redacted] she asked [redacted] to determine whether a banner had been put on the LANL computers, but never received a response. [redacted] 9/7/99) SA [redacted] said that she understood that SA [redacted] discussions with [redacted] had focused on searching Lee's e-mail, whereas she was interested in searching Lee's hard drive. (Id.) According to [redacted] SA [redacted] did ask [redacted] about a banner, but it was in the context of capturing e-mail messages, and [redacted] told her that there was no banner. (FBI 00210) [redacted] also said that after [redacted] told SA [redacted] of [redacted] discussions with SA [redacted] SA [redacted] later told [redacted] that [redacted] was correct, that it was the FBI's position that banners were required to remove the expectation of privacy. [redacted] 9/13/99)

(U) SA [redacted] acknowledged that during their conversations [redacted] told SA [redacted] about the materials [redacted] had previously provided to SA [redacted] (FBI 00216) Presumably, SA [redacted] would have seen SA [redacted] reference to these documents – which restated LANL's policy that "the federal government may, without notice, audit or access any user's computer system" – in the process of reading the file as instructed by SSA [redacted] According to SA [redacted] however, at the time she did not see these materials, which were located in the "1A section" of the file.[634] [redacted] 3/10/00)

(U) [redacted] did not know with whom SA [redacted] spoke to obtain the advice that a banner was required [redacted] 9/13/99), but at some time in the spring of 1998, SA [redacted] raised with SSA [redacted] her concern that Lee's computer had not been searched. [redacted] 9/7/99) According to SA [redacted] SSA [redacted] told her that he would look into it and later told her that FBI Headquarters had determined that a search warrant was required to search Lee's computer.[635] [redacted] 9/7/99) SA [redacted] also spoke to SA [redacted]

---

[634](U) It should be emphasized here that SA [redacted] was not the case agent at this time and did not become the case agent until November 6, 1998. Until November 1998, therefore, the Wen Ho Lee investigation was not SA [redacted] responsibility, although she did assist SA [redacted] on a number of matters. Nevertheless, SA [redacted] was the FBI's liaison with LANL and, for that reason, had been specifically instructed by SSA [redacted] to become "intimately familiar" with the investigation and had been told by him that the case would eventually be re-assigned to her. [redacted] 9/7/99)

[635](U) SA [redacted] did not know whom SSA [redacted] consulted at Headquarters. [redacted] 9/7/99 & 3/10/00) According to SSA [redacted] he did not recall discussing the

FBI 66 67C

who was the case agent on the Lee investigation at the time, about the possibility of searching Lee's computer. (Id.) SA [redacted] told SA [redacted] that SA [redacted] had raised the question of searching Lee's computer, but SA [redacted] was told by FBI Headquarters that a search warrant was required. (Id.)

(U) SSA [redacted] response that a warrant was required "did not sit right" with SA [redacted] and she told SSA [redacted] that she had worked on many computer cases in which the subject of the search had no expectation of privacy.[636] [redacted] 9/7/99) In particular, according to SA [redacted] her experience with the National Computer Crime Squad had involved investigations where it had been determined that an employee had no expectation of privacy while using his employer's computer. (Id.) It is for this reason particularly unfortunate that SA [redacted] did not review the materials which she had been told had been given to SA [redacted] by [redacted][637] Perhaps, in light of the seemingly categorical advice from FBI Headquarters that rejected a search in the absence of a banner, SA [redacted] as had SA [redacted] before her, regarded these materials as irrelevant. In any event, this is where the question died for all intents, when the documents were, for a second time, not forwarded to FBI Headquarters for further advice.

DOE 66, 67C

---

matter of searching Wen Ho Lee's computer with SA [redacted] or with anyone at FBI Headquarters. [redacted] 12/7/99) SSA [redacted] did recall consulting Albuquerque's [redacted] about searching the computers of LANL employees in two unrelated matters. (Id.) In those other investigations, the CDC had advised that a search warrant was required, and one was obtained prior to the search of the computers. (Id.) SSA [redacted] said that he did not consult with the CDC in connection with the Wen Ho Lee investigation. (Id.)

DOE 66 67C

[636](U) According to SA [redacted] she had worked with [redacted] and [redacted] of the Computer Crime Section many times. SA [redacted] acknowledged that she could have contacted [redacted] directly regarding the computer search issue, but felt that it would be inappropriate because she was not the case agent. [redacted] 9/7/99)

[637](U) According to SSA [redacted] he does not recall being aware of the documents [redacted] gave to SA [redacted] in November 1996. [redacted] 12/7/99)

DOE 66, 67C

FBI b6 b7C

(U) In what appears to have been a last ditch effort to obtain a search of Wen Ho Lee's LANL computer, SA [redacted] "kind of hinted" to [redacted] that DOE could search Lee's computer. ([redacted] 9/13/99; [redacted] 9/7/99) From her experience in investigations involving computers, SA [redacted] believed that a computer system administrator had the right to monitor the use of its computers. ([redacted] 9/7/99) [redacted] demurred, however, citing Executive Order 12333 as prohibiting DOE from undertaking any investigative steps once the matter had been referred to the FBI.[631] ([redacted] 9/13/99; [redacted] 9/7/99)

DOE b6 b7C

9. ~~(S/RD/NF)~~ [redacted]

b1

~~(S/NF)~~ In June 1998, SA [redacted] and SA [redacted] received information from Source #2, see Section B(2) of this chapter. [redacted] (AQI 01796)

~~(S/NF)~~ According to Source #2's written report [redacted] (AQI 01795) As

---

[631] (U) ~~(S/NF)~~ As discussed below, Executive Order 12333 would not, in our view, have presented a legal obstacle to DOE conducting its own search of the LANL computer systems used by Wen Ho Lee.

[632] ~~(S/NF)~~ SA [redacted] received similar information from another source when she interviewed a former LANL employee on March 26, 1998. [redacted]

FBI
b6, b7C

discussed above, the essence of the information imparted to SAs [redacted] and [redacted] in March and June 1998 had actually been known to the FBI since 1994, shortly after Wen Ho Lee's encounter [redacted]

b1

(S/RD/NF) [redacted]

[redacted]

(S/NF) [redacted]

(AQI 01667)

(S/NF) As an indication of the importance of [redacted] particularly when combined with the information provided by Lee's [redacted] should have set off alarms at the FBI. None of this information, however, led the FBI to revisit the issue of how to gain access to the computer systems used by Wen Ho Lee.

10. (U) Banners remain the focus into 1999 until Wen Ho Lee's LANL computer is finally searched, with Lee's consent

(U) According to [redacted] at LANL since December 1998, [redacted] asked SA [redacted] in January 1999 whether the FBI would be searching Lee's computer.[640] [redacted] 9/13/99) SA [redacted] responded that Albuquerque's Chief Division Counsel had said that they could not search the computer unless there was a banner on the computer.[641] (Id.) According to [redacted] who had recently retired from the FBI, [redacted] told SA [redacted] that although the FBI's position had been that it could not search computers unless there was a banner, that position had changed. (Id.) [redacted] encouraged SA [redacted] to contact [redacted] of the FBI's NSLU, who [redacted] said had rendered an opinion, in a 1998 matter unrelated to LANL, that a waiver was sufficient to permit a search of a computer.[642] (Id.)

---

[640](U) In a letter to Edward J. Curran, Director of DOE's Office of Counterintelligence, [redacted] states that the date of this conversation was January 7, 1999. (FBI 04654)

[641](U) SA [redacted] told the AGRT that she did not consult with Albuquerque's CDC, [redacted] about searching Lee's computer. [redacted] 3/10/00) [redacted] did not recall ever discussing the Wen Ho Lee matter with any of the FBI Albuquerque case agents or supervisors, including SA [redacted] 3/1/00)

[642](U) [redacted] said that the matter in which [redacted] assisted [redacted] involved a corporate policy and an explicit banner advising employees of the possibility of computer monitoring. [redacted] 10/19/99) According to [redacted] to search a computer without a warrant or FISA order, the investigator must be able to show that the user is aware that the computer system may be monitored and has given consent to do so,

DOE FBI b6 b7C

(U) According to [redacted] SA [redacted] already knew about the on-line acknowledgment of computer monitoring,[643] which by then had been implemented lab-wide, because he had obtained such records for her in unrelated waste, fraud, and abuse cases. [redacted] 9/13/99) Moreover, [redacted] recalled that he had obtained the e-mail of other LANL employees for SA [redacted] in other investigations.[644] (Id.) Nevertheless, it appears that no action was taken by SA [redacted] in response to the information provided by [redacted] This may be explained, however, by the fact that at the time of the conversation, and until early February, the FBI was under the misimpression that Lee had passed the DOE administered polygraph examination on December 23, 1998.

(U)

(S) As late as February 1999, however, it appears that the existence of a banner was still the FBI's touchstone for determining whether a warrantless search of Lee's computer was permissible. In a February 22, 1999 EC, SSA [redacted] wrote to FBI Albuquerque:

> (U)
> (S) On 2/17/99, DOE's Ed Curran suggested AQ FBI may be able to access, copy, and retain electronic communications contained in or retrievable from subject's e-mail account at LANL. FBIHQ advised this depends on the existence and wording of any banner warnings that LANL may use to warn subject of no expectation of privacy.

---

through a banner, waiver, or clear corporate policy stating that the employee has no reasonable expectation of privacy. (Id.)

[643] (U) [redacted] referred to this on-line acknowledgment as a "waiver" [redacted] 9/13/99), as have other witnesses and reports.

[644] (U) According to SA [redacted] however, she does not recall being told of the on-line registration program, and she was never given any such documents by [redacted] 3/10/00)

(AQI 00180) The EC tasked Albuquerque with determining "what, if any, warnings are on subject's computer" and to coordinate with the NSLU "to determine if the warning is legally sufficient to allow LANL to access and copy subject's e-mails or other files." (Id.)

(U)
(S) According to an investigative update that ASAC William Lueckenhoff faxed to DAD Sheila Horan on February 26, 1999, FBI Albuquerque had that day "contacted LANL and [redacted] concerning issues raised by Ed Curran." (FBI 01591) The document goes on to say that "LANL personnel advised that a 'banner warning' does not exist on the LANL system to warn users of no expectation of privacy." (Id.) It is not clear who the "LANL personnel" were who were responsible for communicating this information, which we now know to be inaccurate, to the FBI.

DOE
FBI
b6
b7C

(U) This investigative lead to Albuquerque was ultimately overtaken by events, as Lee's LANL computer was searched, with Lee's consent, on March 5, 1999.

11. (U) The discovery that Wen Ho Lee had taken the "crown jewels"

(U) When the FBI searched Wen Ho Lee's X Division office, it discovered a notebook containing, among other things, a printout of computer file names from one of Lee's directories on the open CFS of LANL's computer system. [redacted] 9/11/99; [redacted] 12/17/99; AQI 06196) When the LANL scientists assisting the FBI examined the file names contained in this listing, they were immediately suspicious that Lee had moved highly classified computer files from the secure LANL system to the unclassified, open system. [redacted] 12/21/99; [redacted] 12/17/99) When the LANL scientists went to examine the contents of these files, however, they discovered that the files had been deleted in January and February 1999. (AQI 06197) From LANL computer system backup tapes, LANL scientists were able to reproduce the directory as it existed prior to the deletion of the files. (Id.) When the restored files were examined, the LANL scientists' fears were confirmed: Wen Ho Lee had transferred computer files containing classified nuclear weapons design information from the secure computer system onto the open system. (Id.) These classified files remained on the open system from the time that

Lee transferred them in 1993 and 1994 until they were deleted by Lee in 1999.[445] (Detention Hearing 12/27/99 Tr. 83-84)

(U) [redacted] one of the LANL scientists who first recognized the file names of the computer codes and other files that Lee had transferred onto the open system, was stunned by his discovery:

> (U) This is – it's unimaginable. I could not believe it. I cannot – I still cannot. I have trouble believing it. It's just -- all the codes, all the data, all the input files, all the libraries, the whole thing is there, the whole ball of wax, everything.

(Detention Hearing 12/28/99 Tr. 344)

12. (U) The discovery of Wen Ho Lee's April 1995 "Rules of Use" waivers

(U) (S) In May 1999, following Congressional hearings concerning the Kindred Spirit investigation, [redacted] learned that Lee had signed waivers consenting to monitoring of his computer. (FBI 00209) [redacted] received a request from SA [redacted] the newly assigned case agent on the Lee investigation, for any documentation LANL employees may have signed to acknowledge their understanding of the possibility of computer monitoring. (FBI 00209) At about the same time, [redacted] had a conversation with [redacted] during which [redacted] told [redacted] that Lee would have signed computer waivers in X Division. (FBI 00209) [redacted] then contacted the X Division [redacted] who provided [redacted] with the "Rules of Use" forms, containing an express consent to monitoring, signed by Lee.[446] (FBI 00209)

---

[445](U) The FBI also discovered, through the search of Lee's LANL offices, portable computer tapes, an examination of which confirmed that Lee had not only moved classified files to the open system, but had also downloaded classified files onto a removable medium. [redacted] 9/11/99)

[446](U) (S) At about the same time as his discovery of the "Rules of Use" form, [redacted] apparently spoke with [redacted] about the on-line registration system, which generated the "Computer Security Responsibility Acknowledgment," an example of which [redacted]

(U) predecessor was the person whom, in December 1996, X Division suggested that SA contact for assistance with [447] As discussed above, according to all X Division computer users were required to sign a "Rules of Use" form, containing a warning that their use of computers was subject to monitoring.[448] (Omnibus 11/30/99) the "Rules of Use" forms, which were specific to X Division. Had been asked by the FBI about searching or monitoring Wen Ho Lee's computer, or if had been asked about what expectation of privacy Wen Ho Lee might have in the use of his computer, Lee would have drawn attention to the "Rules of Use" forms. (Omnibus 11/30/99)

(U) Had the FBI asked in November 1996, it would have learned that Wen Ho Lee signed two such "Rules of Use" documents on April 19, 1995, one for the open X Division local area network ("LAN"), which is not secure and where processing

---

had given to SA in November 1996. (FBI 00211) When interviewed by the FBI on May 10, 1999, said that had confirmed that Wen Ho Lee "is listed in computer as one of the employees who did go through the online training process." (Id.) When interviewed by the AGRT, however, did not recall either being asked to verify that Wen Ho Lee had registered or ascertaining that Lee had registered. explained that the registration system existed only on the open ICN. Anyone with access to the open ICN could ascertain whether a user with an open ICN account had registered on line. Once the user was taken off the system due to the user's termination, however, the record of that user's registration was automatically removed from the system. Therefore, according to records pertaining to Wen Ho Lee's registration "went away" when Lee was fired. Until Wen Ho Lee was fired, anyone on the ICN could have asked the system whether he had registered. (Omnibus 11/30/99)

[447](U) According to Lee, he never met SA until the Senate Governmental Affairs Committee hearings into the handling of the investigation. (Omnibus 11/30/99)

[448](U) In addition to the lab-wide computer security protocols at LANL, each division's computer security director may implement additional security measures for the division.

of classified information is not permitted, and one for the secure X Division LAN. Since 1995, these waivers had been maintained in a binder in X Division, which is where [redacted] located them when they were finally requested by [redacted] (FBI 00209; Omnibus 11/30/99)

DOE
b6
b7C

(U) Three of Wen Ho Lee's [redacted] – each of whom was interviewed by the FBI on other matters during the course of the investigation – knew of the "Rules of Use" forms, as they themselves were required to sign similar forms, but they were never asked about waivers, banners, or, more generally, about a LANL computer user's expectation of privacy. [redacted] 12/20/99; [redacted] 12/21/99; [redacted] 12/21/99)

FBI
b6
b7C

(U) [redacted] described the "Rules of Use" forms as "part of the X Division culture or work life." [redacted] did not recall discussing the form with SA [redacted] however, and was never asked about them. [redacted] 12/20/99) [redacted] would have told the FBI about the "Rules of Use" forms had [redacted] been asked whether Wen Ho Lee had any expectation of privacy in his computer. [redacted] 12/21/99) Both men were interviewed by SA [redacted] in December 1996. In April 1997, [redacted] was interviewed again by SA [redacted] and [redacted] attended a meeting with FBI and DOE personnel to discuss Wen Ho Lee's access to new computer code development work. (AQI 01151, 01153, 01155; FBI 00803, 00804) Nevertheless, while [redacted] and [redacted] were asked about Wen Ho Lee's computer use, computer access, and his work on computer codes used in the development of nuclear weapons, neither was asked about Lee's expectation of privacy while using his computer. Consequently, the "Rules of Use" waivers never came to light in their interviews. (Id.; [redacted] 12/20/99; [redacted] 12/21/99)

(U) Similarly, SA [redacted] interviewed [redacted] Wen Ho Lee's [redacted] several times in the spring and summer of 1997. (FBI 00883, 00890, 00955, 01005, 01053) Ironically, one purpose of the interviews was to obtain information concerning Wen Ho Lee's computers so that they could be included in the FISA application that was then being prepared. According to [redacted] however, no one ever told [redacted] that the information that the FBI was gathering "was a prelude to a search warrant." [redacted] could not recall anyone talking to [redacted] about searching or monitoring Lee's computer until March 1999. [redacted] 12/21/99) Had [redacted] been asked, [redacted] would have told the FBI that Lee had no expectation of privacy concerning his computer use, and would surely have

mentioned the "Rules of Use" forms, which [redacted] knew to have been signed by everyone in X Division."[649] [redacted] 12/21/99)

DOE FBI 66 67C

(U) According to [redacted] he learned only in May 1999 that there was a banner on LANL's classified computer system, so that each time Wen Ho Lee powered up the computer work station in his office, the banner would appear."[650] [redacted] 9/13/99) It was also [redacted] who told [redacted] of the banner. [redacted] 9/13/99)

13. (U) The LANL computer systems used by Wen Ho Lee

(U) As part of a concerted effort to gain access to the LANL computer systems used by Wen Ho Lee, in addition to investigating the existence of banners, waivers, or written policies, the FBI should have sought to understand the details of how the LANL computer system was structured, its "architecture." This was important for at least two reasons: First, the architecture of the computer system is relevant to the user's expectation of privacy. For example, a user's expectation of privacy in a stand-alone desktop computer, to which he alone had access in his office, would be different, all other things being equal, from that of a user of a system at some remove from his office, accessed remotely on a network and to which many others had access. Second, various

---

[649](U) Actually, [redacted] believes that he did tell SA [redacted] about the "Rules of Use" forms. [redacted] said that this is "the type of thing" [redacted] would have mentioned to SA [redacted] believes that [redacted] also informed SA [redacted] of the educational efforts made at LANL to make people aware of computer security. [redacted] could not be certain of this, however. [redacted] 12/21/99) None of SA [redacted] 302s of [redacted] reflect that SA [redacted] was told of the "Rules of Use" waivers.

[650](U) Apparently, [redacted] was referring to the X Division secure LAN. It is worth noting, as an example of the confusion that apparently continues to surround the issue of banners and waivers regarding LANL computers, that [redacted] told the AGRT in September 1999 that there was never a banner on LANL's open computer system during any time relevant to the Wen Ho Lee investigation. [redacted] 9/13/99) In fact, as discussed above, there were banners on both the lab-wide secure and open systems, as well as both the X Division secure and open local area networks at the time that SA [redacted] asked [redacted] in November 1996.

logs and other data maintained on the lab-wide network could have provided information relevant to the investigation. These included logs that record when users access particular files and what actions they perform on the files, such as altering its classification or downloading it. Inquiries to the LANL computer help desk were also recorded. These logs and help desk records could have been a rich source of information concerning Wen Ho Lee's computer activities, much of which could have been obtained *without a warrant*, even in the absence of banners or waivers.

a. (U) The open and secure systems

(U) Wen Ho Lee had in his X Division office a Sun Microsystems workstation with which he could access the secure or X Division local area network ("LAN") and another Sun Microsystems workstation with which he could access the open X Division LAN.[651] Although both workstations had temporary memory capacity that allowed the user to work with files or data that had been accessed from the X Division LAN or the lab-wide Integrated Computing Network ("ICN"),[652] neither had a hard drive on which files could be downloaded or stored. For all intents and purposes, all memory on the Sun workstations was erased when the workstation was powered off. (Omnibus 11/30/99)

(U) To access the X Division secure, or "Enchanted," LAN, an X Division user would connect his workstation to a port located in a lockbox on the office wall. The workstations could not be left connected to the secure LAN, and at the end of each day,

---

[651](U) Lee's X Division office had a door with a lock, although it shared a common key with four nearby offices. Lee had bookcases in his office that made it impossible to see his computers, or what he was doing at his computers, from outside his office.

[652](U) Thus, Lee had four "accounts" on the LANL computer system: Lee could store information on either of the two X-Division LAN's or on either of the two lab-wide ICNs. [redacted] 9/13/99) To access a computer account, a LANL user would need to input a "Z-number," an identifier assigned to each employee that appears on the security badge that each employee wears, together with a password that is assigned to each user by LANL. With a LANL user's Z-number and password, anyone can access the open system through the Internet from anywhere in the world. [redacted] 9/11/99)

DOE b6, b7C

FBI b6 b7C

the users were to disconnect the workstation from the port.[653] The X Division servers are located on the first floor of Building 43. Wen Ho Lee's X Division office was on the second floor of this building. The X Division servers are in vault rooms, which are alarmed and can be accessed only with a password. Wen Ho Lee did not have access to the vaults with the servers, unless he was escorted. (Omnibus 11/30/99)

(U) The secure ICN at LANL contains supercomputers, storage, and specialized servers connected to users in other laboratory divisions and groups. The X Division LANs were connected by "ether" networks to the lab-wide ICNs. The secure or "Enchanted" X Division LAN was connected to the secure ICN. The open X Division LAN was connected to the open ICN.[654] The secure ICN includes the secure Central Filing System ("CFS"), which is a file storage server, and supercomputers designated Sigma, Tao, and Theta, on which complex computer functions could be performed on files accessed on the secure CFS. Services available in the open ICN include supercomputing, storage and archive, Web access, and Internet mail. The open ICN includes the open CFS.[655] (Omnibus 11/30/99)

(U) The secure and the open CFS are in Building SM 132, a separate building from that in which Wen Ho Lee worked, in a controlled access area. The CFS system comprises more than 6,000 tape cartridges in a storage silo. The entire open and secure

---

[653](U) In some offices, an X Division user had one workstation through which to access both the open and the secure LAN, although a workstation could not be connected to both LANs at once. The user would have to disconnect from one port and reconnect to a separate port in the office in order to access the different LANs within X Division.

[654](U) The X Division secure and open LANs were physically separate systems.

[655](U) The closed ICN and the open ICN are separated by an "air gap," which means that the two systems are physically and electronically separate systems. In January 1995, the open CFS and the secure CFS were split, to introduce an "air gap" between the two file storage systems. Prior to that time, the open and secure CFS were contained on a single system that was "partitioned" to store secret restricted data files on the secure "red" partition and unclassified files on the open "green" partition.

ICN is contained in six rooms in the Central Computing Facility in SM 132. (Omnibus 11/30/99)

(U) To access the X Division LANs or the ICNs, an X Division user would connect the workstation to the port and boot up off the network. As part of the log-in process for both the secure and open LANs, the X Division banner, discussed above, would appear. Once logged on, a user in X Division could access machines that were part of the X Division LAN from his workstation. Whenever a user logged onto a machine in the X Division network, the X Division banner would appear on the workstation screen again. Wen Ho Lee had a "home directory" on the secure X Division LAN and one on the open LAN. He could store files or data on these home directories. Lee could also store files or data on directories he had on the CFS storage systems that were connected to the secure and open ICNs. The classified files Lee is accused of down partitioning and downloading onto tape were taken from directories on the secure ICN and moved to directories on the open ICN. (Omnibus 11/30/99)

b. (U) The logs generated by LANL computer systems

(U) The CFS system maintained logs recording the actions of users of the system. The CFS logs, also known as the System Maintenance Facility logs, would record changes in the classification or partitioning of a file. The CFS logs recorded the user, file name, the date and time of the action on the file, and the CFS commands issued with respect to the file. The logs are a chronological listing of actions performed by all users. Thus, for example, if a user modified a file to change its classification in the morning, down partitioned the file in the afternoon, and copied it at night, the user's activities on the CFS log could be separated by thousands of log entries pertaining to actions of other LANL users. If asked by the FBI, it would have been possible for someone to have looked at the CFS logs on a daily basis to see what actions Wen Ho Lee had executed. Logs were also maintained by each of the worker machines. According to [redacted] it would have been possible in 1996 to write a program to search the CFS logs for a given user's name and to generate a list of all files on the CFS that were access by the user for

DOE 66, 67C

DOE 66 67C

the 1993 to 1996 period. [redacted] estimated that the project could have taken from a week to two months, depending upon the urgency of the project.[656] (Omnibus 11/30/99)

(U) Until June 1994, to move files from the secure CFS to the open CFS required the use of "Machine C."[657] Machine C was a worker machine on the LANL ICN used to transfer files from the secure to the open partition on the CFS.[658] Machine C performed only this one function. It changed the designation of a file from a more secure partition to a less secure partition, such as from the secure "red" partition to the nonsecure "green" partition. This was called "down partitioning" a file. Technically, Machine C did not move the file, since the CFS as it exited at the time that Machine C was in use did not have separate drives for the secure and open partitions. Rather, files existed on a single physical storage facility, but were designated "red" or "green." Machine C would not change the partition of a file from red to green unless the file was unclassified. Machine C could not be used to change the classification of a file. The user would have to first change the "header" of the file that contained the secret classification to unclassified on the red partition before using Machine C to change the partition from red to green. The partition of a file could only be changed using Machine C. (Omnibus 11/30/99)

DOE 66 67C

[656](U) The CFS logs are maintained back to 1993. According to [redacted] the logs began in 1993, so that, had the FBI asked for them in 1996, the earliest logs would still be from 1993. The CFS logs are stored on tape on the CFS system.

[657](U) (S/NF) With the exception of the last file, which was moved directly from the secure CFS onto a portable tape, all of the files involved in the Indictment were moved prior to June 1994. (LANL 001954 & 2054)

[658](U) It has always been forbidden to process or store classified information on the open system. However, a LANL scientist may have had a legitimate need to transfer files from the open to the secure system to use, for example, an unclassified program to manipulate classified information. A scientist might also have legitimately transferred to the open system unclassified files or data which had been stored on the secure system. Classified files were coded in a way intended to prevent their being transferred from the closed to the open system. (Omnibus 11/30/99)

(U) Machine C was located in the Central Computing Facility in Building SM 131, Room 280. It was thus in a separate building from the X Division. To access Machine C, an X Division user would first have to log onto a secure workstation and, from that workstation, log onto Machine C. Thus logged onto Machine C, the user could access files on the red partition on the CFS and change the partition from red to green. (Omnibus 11/30/99)

(U) Machine C recorded the fact that a user had logged on, but not the actions of the user or the files that were down partitioned. To obtain this information, it would have been necessary to go to the CFS logs. (Omnibus 11/30/99) Identifying the files that had been down partitioned would not have been an easy task, according to [redacted] because the CFS log records millions of transactions per day. (Id.) [redacted] believed that it could have been done; however, [redacted] guessed that it could have taken "weeks or months" to complete and might have required two to three people to do it.[659] (Id.) According to [redacted] it would also have been possible to instruct the LANL system to begin to create a log of all the activities of a particular user. (Id.)

DOE b6 b7C

c. (U) LANL's NADIR System

(U) The LANL computer system also has a program, called Network Anomaly Detection and Intrusion Reporter ("NADIR"), to detect anomalies should there be an unusual number of transfers from the closed to the open system by a user. [redacted] 9/11/99; Omnibus 11/30/99) If this program is triggered by a high volume of transfers, it will generate a "NADIR" or "anomaly" report. According to SA [redacted] in the ordinary course, when such a report was generated, the computer security group would contact the user seeking an explanation for the transfers, and would then create a record of the resolution of the reported anomaly. The log of files transferred, which was maintained on the mainframe, could also be reviewed as part of the resolution of the anomaly

FBI b6 b7C

---

[659](U) [redacted] created the spreadsheets used in connection with Lee's detention hearing, which described all of his activities concerning the files charged in the Indictment. According to [redacted] the same information could have been compiled in 1996. [redacted] noted, however, that it took "some months" to compile the information in the detail they now have it. [redacted] 12/17/99)

DOE b6 b7C

report.[660] Occasionally, the system administrator notified [redacted] or [redacted] of the Office of Counterintelligence at LANL, apparently when the explanation of the anomaly was found insufficient. [redacted] 9/11/99)

DOE 66 67C

FBI 66 67C

(U) The NADIR system monitored activities on the open and secure ICN, including the supercomputers Sigma, Tao, and Theta, Machine C, and the CFS.[661] The NADIR system also monitored the system log, which recorded user log-ons, and the security log, which tracked file access, the number of times a file was accessed, and when different files were accessed. The NADIR system built a user profile for each ICN user based upon his past activities, and generated a report whenever a user's activities were anomalous based upon this profile of past activities. For example, NADIR monitored a user's hours of computing, and if that user began computing at unusual hours compared to his past hours, NADIR would generate a report. Similarly, if a user's number of downloads or transfers of files was anomalous based upon his history, NADIR would generate a report. Movement of files from the secure to the open CFS would not necessarily trigger a NADIR report, unless such activity, such as the quantity of files transferred or the time of day of the transfer, was anomalous in some way.[662] (Omnibus 11/30/99)

(U) In 1994, the CFS was modified to create an "air gap" between the open and secure systems, making it virtually impossible to transfer files directly between the two.

---

[660](U) According to [redacted] NADIR logs are maintained for two years. Reports from those logs, however, are kept back to October 1992. [redacted] did not know if the file names are recorded in the NADIR logs, but that information could be obtained from the CFS logs with the information that is in the NADIR reports. (Omnibus 11/30/99)

DOE 66 67C

[661](U) The NADIR system is maintained on a server that is part of the ICN. (Omnibus 11/30/99)

[662](U) If a NADIR report was generated for a user, the NADIR team had an investigator who would contact the user for an explanation of the anomaly. The explanation would then be entered onto a database. (Omnibus 11/30/99)

9/11/99) According to SA the fact that there would be this change in the system was widely publicized for several months before the system was changed. (Id.) As a result, there were a number of LANL computer users who were performing a high volume of transfers from the secure to open system, apparently trying to accomplish these before the new, considerably more difficult system for transferring files came into effect. (Id.) Consequently, there were, in the period before the new system was implemented, a high number of anomaly reports generated for each of these users. (Id.) According to a large number of NADIR reports were generated in "all of 1994 and a good chunk of 1993," when the LANL CFS system was being split. (Omnibus 11/30/99) One was generated for Wen Ho Lee.

(U) (S/NF) In August 1993, Wen Ho Lee triggered a NADIR report for moving a large number of files. (Omnibus 11/30/99) The NADIR team's investigator, did not contact Lee for an explanation, however. (FBI 15838) characterized this incident as "common." (Id.) agreed that at the time preceding the CFS split, file movement in anticipation of the changes to the system was taken as a sufficient explanation for anomalous transfers of files from the secure to the open partition. (Omnibus 11/30/99) also noted that the NADIR system generates thousands of anomaly reports per year, and is the only investigator responsible for looking into all of them. just could not follow up on all of them. (FBI 15839)

(S/NF)

(LANL 001954 & 2054)

d. (U) LANL's help desk and Lee's questions

(U) LANL had a computer help desk which users could call for technical assistance. The questions and answers are entered on the computer system and maintained by the user name of the requester, so that it is possible to obtain a list of all questions and answers by a particular user.[663] 9/11/99; Omnibus 11/30/99) The

[663](U) The ICN help desk logged e-mail and oral requests for assistance from users. The X Division also had a help desk that maintained a log of all e-mail requests

listing of questions posed by Lee includes several that are significant to the criminal investigation.

(U)

(S) On March 2, 1998, the same day that Lee submitted a form to DOE regarding travel to Taiwan to vacation and to present a paper relating to Lagrangian codes (FBI 1275), a computer help desk inquiry shows that Lee asked "How to telnet to his machine from overseas." (FBI 13525) The "solution" entered on the help desk system states, "walk thru."[664] (Id.)

(U)

(S) On January 19, 1999, shortly after being interviewed by the FBI and the day before Lee began deleting the classified files he had transferred to the open CFS, a computer help desk inquiry shows that Lee asked "how to get from local workstation (X) to cfs?" (FBI 13525) Then on January 22, 1999, according to the April 8, 1999 EC, "Lee wanted to know why the 'deleted files . . . are not going away.' This request came just five days after Lee was first interviewed by the FBI." (FBI 01986; FBI 13525) On the same day, "Lee also wanted to know how to access the 'Gamma' computer from his Macintosh computer, which he had at his residence." (Id.)

b1 (S) [redacted] The file was opened and 19 classified files were removed from the TAR file. The file was re-TARed and stored back onto the open CFS. It was previously a classified file, but the modifications removed the classified material, and the unclassified file was saved back to the open CFS. (Detention Hearing 12/27/99 Tr. 64) On February 16, 1999, Lee made

---

DOE b6 b7C for assistance. According to [redacted] however, there were no references to requests for assistance by Wen Ho Lee on the X Division help desk system. (Omnibus 11/30/99)

(U)

"(S) According to an April 8, 1999 EC regarding Lee's help desk inquiries, "Lee asked the 'help desk' how he could access his network classified computer from overseas. He was told [that] he would not. The question is significant because he asked it just prior to a vacation he took to Taiwan." (FBI 01986)

another computer help desk inquiry: "wants to replace one file in a tar file on a tape."[665] (FBI 13525) Then on February 17, 1999, Lee made his "Final deletion of tar.File15. This was the next to last file deleted by [Lee] on the open CFS." (LANL 001989) According to SA [redacted] Lee had manipulated some of the tapes that the FBI recovered from his T Division office to delete the classified information from the tape. [redacted] 9/11/99)

FBI b6 b7C

c. (U) Electronic mail

(U) According to [redacted] everyone who had an account on the open and the secure X Division LAN had e-mail. X Division used a commercial, or "pop" client e-mail software package, such as Netscape or Microsoft Outlook Express, to access e-mail. Because the e-mail software was an "off-the-shelf" package, it did not contain any banner or notice that the e-mail may be monitored by LANL. To access the e-mail, however, an X Division user would have to have been logged onto the X Division LAN and therefore would have encountered the X Division banner. An X Division user's e-mail once read remained on the X Division e-mail server until the user did something with it. The user could store e-mail on the user's X Division home directory. The secure and open e-mail systems in X Division were completely separate from one another. (Omnibus 11/30/99)

DOE b6, b7C

(U) According to [redacted] there is e-mail on both the secure and the open ICN; however, the secure e-mail system had very few users in 1996 and is still fairly low in use. There are no banners on the open or secure ICN e-mail systems. A user had only one open e-mail address, so that e-mail from X Division, from elsewhere in the lab, or from the Internet was all routed to the user's single open e-mail address. Similarly, users had only one secure e-mail address. LANL has had e-mail on the open ICN since the early 1980s. X Division did not have e-mail on its open LAN until the late 1980s or early 1990s. It was not necessary to have an account on the ICN in order to have an e-mail account at LANL. (Omnibus 11/30/99)

DOE b6 b7C

---

[665](U) According to SA [redacted] the help desk also has records of questions that were posed by Lee before 1996 that would have been helpful to the investigation. [redacted] 9/11/99)

FBI
b6
b7C

(U) According to SA [redacted] in his opinion it would not have advanced the investigation of Wen Ho Lee to have been able to search or monitor Lee's e-mail. None of what was discovered with respect to Lee's downloading of classified files would have been discovered through a search of Lee's e-mail. According to SA [redacted] Lee "didn't do what he did through e-mail." [redacted] 9/11/99)

C. (U) Legal Analysis

(U) It is settled that a government employee may have a reasonable expectation of privacy in the government workplace. O'Connor v. Ortega, 480 U.S. 709, 715-16 (1987). It appears, however, that when asked about searching Wen Ho Lee's computer in November 1996, the NSLU leapt from the unexceptionable premise that Lee *may* have had a reasonable expectation of privacy in his LANL computer, to the conclusion that he, in fact, *did* have one. Instead, this should have only been the beginning of the inquiry.

(U) The application of the Fourth Amendment depends upon whether the person invoking its protections can claim a reasonable expectation of privacy that has been invaded by government action. Smith v. Maryland, 442 U.S. 735, 740 (1979).

> (U) This inquiry . . . normally embraces two discrete questions. The first is whether the individual, by his conduct, has "exhibited an actual (subjective) expectation of privacy – whether . . . the individual has shown that "he seeks to preserve [something] as private." The second question is whether the individual's subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable'" – whether . . . the individual's expectation, viewed objectively, is "justifiable" under the circumstances.

Id. (citations omitted).

(U) The NSLU did not inquire, or advise the agents to inquire, whether a LANL employee such as Lee had a subjective expectation of privacy in the LANL computer systems he used, or whether, whatever expectation of privacy he may have had notwithstanding, it was justifiable under the circumstances. This was crucial. "Given

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, 480 U.S. at 718. Moreover, "[p]ublic employees' expectations of privacy in their offices, desks, and file cabinets, like similar expectations of employees in the private sector, may be reduced by virtue of actual office practices and procedures, or by legitimate regulation." Id. at 717.[666] Nor did the NSLU advise the agents to explore the computer architecture at LANL to ascertain whether, because of the nature of the computing environment, Lee had, in effect, "knowingly expose[d]" his computer activities,[667] or had "voluntarily turn[ed] over" information concerning his computer use to third parties.[668]

(U) In Smith v. Maryland, for example, the Court held that a telephone user could have no reasonable expectation of privacy in the numbers he dialed because he "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In doing so, petitioner assumed the risk that the company would reveal to police the numbers he dialed." 442 U.S. at 744.[669] The Court rejected the petitioner's contention that he had

---

[666](U) See also Schowengerdt v. General Dynamics Corp., 823 F.2d 1328, 1334 (9th Cir. 1987). "In the last analysis, the objective component of an employee's professed expectation of privacy must be assessed in the full context of the particular employment relation." Vega-Rodriguez v. Puerto Rico Telephone Co., 110 F.3d 174, 179 (1st Cir. 1997) (collecting cases).

[667](U) "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." Katz v. United States, 389 U.S. 347, 351 (1967).

[668](U) "This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." Smith, 442 U.S. at 741.

[669](U) See also United States v. Miller, 425 U.S. 435 (1976). In Miller, the Court held that a bank customer had no Fourth Amendment interest in checks, deposit slips and other information conveyed to his bank.

demonstrated an expectation of privacy by using "'the telephone in his house to the exclusion of all others.'" Id. at 743.

> (U) Regardless of his location, petitioner had to convey that number to the telephone company in precisely the same way if he wished to complete his call. The fact that he dialed the number on his home phone rather than on some other phone could make no conceivable difference, nor could any subscriber rationally think that it would.

Id. Analogously, when Wen Ho Lee accessed the ICN by attaching his workstation to the port located in the lockbox on his office wall, and when he used the remote Machine C to down partition files or used the remote Machine Rho to save files onto its disks (because he had no such memory on his own workstation), he "voluntarily conveyed" information about his computer usage to the LANL systems and he "'exposed' that information to its equipment in the ordinary course of business," just as the telephone subscriber in Smith v. Maryland had.

(U) Thus, although the NSLU was apparently informed, incorrectly, that there was no banner on the LANL computer systems used by Wen Ho Lee, had a review been conducted of *additional* information concerning the "office practices and procedures" at LANL and the physical characteristics of the computer system itself, it would have been evident that Lee had no justifiable expectation of privacy, even in the absence of a banner. The factors supporting this conclusion include the following:

> **(U) All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business. . . . The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.**

425 U.S. at 442-43

1. (U) Since at least 1989, when Lee annually renewed his password for the secure ICN, he received documentation stating that the LANL computer systems were exclusively for official business;

2. (U) Lee was similarly told in connection with this annual password renewal that his computer files would be audited by the LANL security personnel as well as the computer personnel;

3. (U) Since at least 1991, Lee annually signed an X Division form stating that the X Division systems were to be used only for official business purposes;

4. (U) Lee was similarly told by the X Division form that DOE and LANL security policies required that his files be audited by security officers;

5. (U) The LANL Official Use Guidelines for Computing and Information Systems (which [redacted] had given to SA [redacted] in November 1996), widely-published in the LANL new bulletin, warned that LANL or the federal government might audit or access a user's computer system or data communications;

6. (U) This point was also made in the Safeguards and Security Manual, which was available on-line through Lee's computer;

7. (U) LANL computer users executed an on-line "Computer Security Responsibility Acknowledgment" that informed them that LANL computer systems were for official use only and that usage was subject to monitoring and auditing;[670]

---

[670](U) As discussed above, this Acknowledgment was not required of X Division users until some time in the December 1996 to April 1997 time frame.

8. (U) LANL personnel received regular briefings on computer security, which informed them that the computer security staff would monitor computer use;

9. (U) Since at least 1992, LANL regularly distributed booklets emphasizing that the computer systems were to be used only for official business;

10. (U) These booklets also notified LANL computer users that all users' files would subject to being audited;

11. (U) Users were not permitted to choose their own passwords to access the computer systems, but had them assigned for both the ICNs and the X Division LANs;

12. (U) The LANL system administrator could access a user's computer files without the need for the user's password, and this was widely known at LANL;

13. (U) Lee's office workstations had no memory capacity on which to store information, and all computer storage was maintained at a remote site to which Lee did not have access;

14. (U) Lee could not access the LANL systems without each day connecting his workstation to a port located in the wall of his office;

15. (U) To down partition files from the secure to the open CFS, Lee would have had to log onto Machine C, which, although accessible from his office workstation, was physically located at a remote location from his office and which was used by all other scientists at LANL to perform the same function;

16. (U) All worker machines through which Lee accessed classified files as part of his day-to-day job functions were at similarly remote locations and were similarly used by other scientists at LANL;

17 (U) Signs notified visitors to LANL that all containers and vehicles were subject to search, and searches of vehicles and containers were randomly and routinely conducted;

18. (U) Lee's X Division office door lock shared a common key with those of four other nearby offices;

19. (U) LANL is a nuclear weapons design facility subject to extensive security measures and requiring special clearances; and, finally,

20. (U) In 1994, all employees in Lee's division received a booklet explicitly stating that while using LANL computing and communication resources, "*you should have no expectation of privacy.*" (emphasis added)

(U) To be sure, those considering a warrantless search of Lee's computer, and of LANL systems accessed by him, still would have had to address the issue of whether, despite having no legitimate expectation against searches by his *employer*, Lee nevertheless might have had a justifiable expectation against searches by *law enforcement officers*.[671] From the foregoing litany of factors, however, Lee clearly did not have "a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy,'" Smith v. Maryland, 442 U.S. at 740, in the various LANL computer systems that he accessed from his office workstation, *regardless* of whether the search had been conducted by LANL personnel or by the FBI. See United States v. Taketa, 923 F.2d 665, 672 (9th Cir. 1991) (holding that warrantless search of defendant's office for evidence of criminal conduct was not "reasonable" under O'Connor, but noting that if the defendant had no reasonable expectation of privacy in his office "there was no fourth amendment violation regardless of the nature of the search"); Schowengerdt v. United States, 944 F.2d 483,

---

[671](U) Cf. Mancusi v. DeForte, 392 U.S. 364, 369 (1968) (defendant who shared office with other union officers "still could reasonably have expected that only those persons and their personal or business guests would enter the office, and that records would not be touched except with their permission or that of union higher-ups"); but see O'Connor, 480 U.S. at 731 (Scalia, J. concurring) ("The identity of the searcher (police v. employer) is relevant not to whether Fourth Amendment protections apply, but only to whether the search of a protected area is reasonable.").

488 (9th Cir. 1991) (warrantless search of Naval employee's office by Special Agent for the Naval Investigative Service upheld on the grounds that the "operational realities" of the workplace precluded an objectively reasonable expectation of privacy); see also United States v. Simons, 206 F.3d 392 (4th Cir. 2000) (remote searches of defendant's computer did not violate his Fourth Amendment rights in light of agency's Internet policy that limited use to "official government business only" and warned that agency would "audit, inspect, and/or monitor" use).[672]

---

[672](U) It should be noted that it is clear from O'Connor v. Ortega and its progeny that *DOE* could have searched Lee's computer, *even if* he had a reasonable expectation of privacy, at any time after DOE had "reasonable grounds for suspecting that the search [would] turn up evidence that [Lee was] guilty of work-related misconduct." O'Connor, 480 U.S. at 726. Presumably, this would have been at some time during the conduct of DOE's administrative inquiry. An examination of Lee's directories and files at that time would have been "reasonably related to the objectives of the search and not excessively intrusive in light of the nature of the misconduct." Id. (citation and internal marks omitted). Also, Title III would have permitted DOE to monitor Lee's computer activities as "necessarily incident . . . to the protection of the rights or property of" DOE. 18 U.S.C. § 2511(2)(a)(i).

DOE FBI b6 b7C

(U) The reason given by a number of DOE personnel for refraining from taking such investigative steps has been that Executive Order 12333 prohibited DOE from taking any investigative measures once the matter had been turned over to the FBI. (See, e.g., [redacted] 9/13/99 [redacted] 9/7/99) This reason would not obtain during the administrative inquiry, however, since the referral to the FBI had not yet been made. Executive Order 12333 does provide that, other than the FBI, agencies within the intelligence community, such as the intelligence element of DOE, are not authorized to conduct physical searches in the United States. Exec. Order No. 12333, § 2.4(b), 46 Fed. Reg. 59941 (1981). Also, DOE Order No. 5670.3 (1992), promulgated pursuant to Executive Order 12333, provides:

> (U) When an inquiry or administrative investigation provides reason to believe that there may be a basis for an espionage investigation, the matter will be immediately referred to the [FBI]. This Order does not authorize any DOE or contractor

employees to conduct espionage investigations or any other criminal investigations.

Id., 1992 WL 754373.

(U)

(S) Because it is not within the scope of the AGRT's mission, we have not explored whether there may be other orders or regulations that deal directly with the effect of Executive Order 12333 upon an agency's ability to conduct searches of the kind contemplated by O'Connor. On the whole, however, neither Executive Order 12333, nor the related DOE order quoted above, appear to apply to *work-related*, O'Connor searches, as opposed to searches conducted for intelligence or counterintelligence purposes. This interpretation is bolstered by the 1992 Memorandum of Understanding ("MOU") between the FBI and DOE, which was apparently applicable during the investigation. (FBI 01240) While requiring DOE to coordinate with the FBI, the MOU otherwise leaves DOE free to deal with work-related issues:

> (U)
> (S) This MOU is not intended to affect DOE's authority to conduct administrative investigations or inquiries related to DOE personnel or facilities. While the DOE may take appropriate administrative, disciplinary or other action *at any time* in connection with a DOE employee whose activities are reported to the FBI, DOE will coordinate with the FBI in advance of any intended action, to avoid prejudicing any ongoing or planned FBI investigative effort or criminal prosecution.

(FBI 01243) (emphasis added)

(U) An interpretation of Executive Order 12333 that permits work-related searches is more consistent with the purpose of the order, which according to its preamble is that "[a]ll reasonable and lawful means must be used to ensure that the United States will receive the best intelligence available." This is not to suggest that DOE could act as an alter ego of the FBI to conduct searches for the benefit of a criminal or FCI investigation. Rather, when there are valid reasons to be concerned about an

(U) The FBI also would have had to consider the implications of the wire tap statute, 18 U.S.C. §§ 2510-22 ("Title III"), and the Electronic Communications Privacy Act, 18 U.S.C. §§ 2701-11 ("ECPA").[673] In this regard, however, the factors discussed above regarding an absence of an expectation of privacy would also establish that Wen Ho Lee had expressly or impliedly consented to the interception of his electronic communications, within the meaning of 18 U.S.C. § 2511(2)(c) under Title III. United States v. Workman, 80 F.3d 688, 693 (2d Cir. 1996); United States v. Lanoue, 71 F.3d. 966, 981 (1st Cir. 1995).[674] In addition, since LANL is not a provider of electronic communication services "to the public," ECPA's prohibitions on the disclosure of the contents of electronic communications, 18 U.S.C. § 2702(a), do not apply to it. Andersen Consulting LLP v. UOP, 991 F. Supp. 1041 (N.D. Ill. 1998).

---

employee's continued employment or unsupervised access to classified information, Executive Order 12333 should not be read to prohibit the kind of work-related searches that the Supreme Court has plainly said the Constitution permits. Of course, whatever evidence DOE lawfully obtained as a result of a search *conducted for that work-related purpose* could be shared with the FBI. United States v. Simons, 206 F.3d 392 (4th Cir. 2000); United States v. Johnson, 16 F.3d 69, 74 (5th Cir. 1994). See also Gossmeyer v. McDonald, 128 F.3d 481, 492 (7th Cir. 1997) (presence of outside law enforcement officials and the possibility of the search leading to criminal charges did not inevitably convert search into a criminal search requiring probable cause and a warrant).

[673](U) This assumes, for argument, that Wen Ho Lee's activities on the LANL computer system, such as his accessing of files on the CFS or his instructions to worker machines on the ICN, such as Machine Rho or Machine C, would meet the definition of "electronic communication," contained in 18 U.S.C. § 2510(12), which generally "means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." It is not clear, however, that Lee's activities while using the LANL computer systems would have amounted to "electronic communication."

[674](U) Congress intended the consent provisions of Title III to be construed broadly. United States v. Amen, 831 F.2d 373, 378 (2d Cir. 1987); Griggs-Ryan v. Smith, 904 F.2d 112, 116 (1st Cir. 1990).

(U) Even if the FBI remained concerned that these factors were insufficient to conduct a full search of Wen Ho Lee's computer files or a "real time" monitoring of his computer activities,[675] the FBI should have considered whether the LANL computer systems might yield information to which Lee could have no reasonable expectation of privacy and to which Title III and ECPA would not apply. The various logs maintained by the LANL computer systems would have provided fertile ground.[676] For example, the logs on Machine C, which simply recorded when it was accessed and by whom, are little different from the X Division entry and exit logs, which the FBI obtained through a voluntary production by LANL. The FBI might have queried the NADIR logs to see if Lee was responsible for an unusually large number of transfers from the closed to the open systems had taken place. It might have examined the CFS logs to see what files Lee had transferred. Under the circumstances listed above, Lee would have no Fourth

---

[675](U) Only contemporaneous monitoring of Lee's computer usage would implicate Title III's prohibitions on intercepting electronic communications. See, e.g., Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457, 460-63 (5th Cir. 1994); Bohach v. City of Reno, 932 F. Supp. 1232, 1235-36 (D. Nev. 1996).

[676](U) Even assuming that the accessing or transferring of computer files by a LANL computer user constitutes an "electronic communication," the logs on the ICN and various worker machines do not "intercept" such communications because they do not acquire the "contents" of the "electronic communication." The logs merely record information concerning what files were accessed and when and what actions were performed. "Intercept" is defined in Title III as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4) "Contents" under Title III "includes any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8). See In re United States, 36 F. Supp. 2d 430, 432 (D. Mass. 1999) (distinguishing computer "user activity logs" from contents); see also, Bohach v. City of Reno, 932 F. Supp. At 1236 (storage of alphanumeric message by city's computer system was not an "intercept"; even if it was an intercept, there was implied consent "for one who sends a message using a computer surely understands that the message will pass through the computer").

Amendment interests in this information.[677] Cf. Smith v. Maryland, 442 U.S. 735 (no reasonable expectation of privacy in telephone numbers dialed through telephone company); United States v. Miller, 425 U.S. 435 (no reasonable expectation of privacy in checks, deposit slips, and other information conveyed to bank). See also United States v. Simons, 29 F. Supp. 2d 324, 328 (E.D. Va. 1998) (court questioned whether a review of computer firewall logs "even constituted a search"), aff'd in part, remanded in part on other grounds, 206 F.3d 392 (4th Cir. 2000).

(U) It is unnecessary, however, to wonder in the abstract whether the foregoing list would have sufficed to dispel any reasonable expectation of privacy as to some or all of the information available concerning Lee's computer usage. It is obvious beyond cavil that had the agents in the field been advised by the NSLU to pursue an inquiry into what expectation of privacy a LANL computer user might have had, the "Rules of Use" waiver signed by Wen Ho Lee on April 19, 1995 would certainly have been discovered, as would the banners on all worker machines on both the open and secure ICNs and on the open and secure X Division LANs. These waivers and banners obviously would have supported a warrantless search of Wen Ho Lee's computer directories and files.[678]

---

[677](U) ECPA should not be read to reach the anomalous result that a private provider is allowed to voluntarily disclose to a governmental entity the contents of electronic communications, 18 U.S.C. § 2702 (a), but not "other information" pertaining to a subscriber, 18 U.S.C. § 2703(c). Cf. United States v. Auler, 539 F.2d 642, 646 n.9 (7th Cir. 1976) (since Title III permitted telephone company to intercept the contents of defendant's calls, use of less intrusive pen register or tone detecting device was "surely permissible"). In any event, Wen Ho Lee would likely be deemed to have consented to the disclosure to the government of the "other information" protected by § 2703(c). Moreover, this sort of historical "transactional information" can be obtained with a national security letter under 18 U.S.C. § 2709. Finally, to the extent that the FBI may have been concerned about the effect of § 2703(c), it could have sought an order under 18 U.S.C. § 2703(d), although this would have required the FBI to state that the "other information" was "relevant and material to an ongoing criminal investigation."

[678](U) According to Scott Charney, former Chief of the Computer Crime Section, had he been asked in 1996, he would have advised the FBI to "take everything" on the strength of the "Rules of Use" waivers, including the searching of Wen Ho Lee's

American Postal Workers Union v. United States Postal Service, 871 F.2d 556, 557 (6th Cir. 1989) (no Fourth Amendment interests in lockers violated by "search . . . to discover illegal drugs . . . , weapons, . . . or other contraband" where employees had signed Notice and Waiver Provision upon receipt of the locker acknowledging that lockers were for official use only and were subject to random inspection); United States v. Simons, 206 F.3d at 398.[679]

(S/NF) Finally, it must be emphasized that had the FBI gained access to the LANL computer logs *alone* – even without gaining access to the *contents* of the files – they were themselves so indicative of ongoing improper intelligence-gathering activity involving sensitive national secrets that, combined with the other information that the FBI already had concerning Lee, a FISA order would have been a foregone conclusion. This is particularly so given what the FBI now knows from having reviewed those logs, [redacted]

b1

---

computer files, and would also have approved the real time monitoring of his computer use, at least for a period of time. (Charney 9/2/99)

[679](U) Lee's "Rules of Use" waiver also would permit "real time" monitoring of his computer use, under the consent exception to Title III, 18 U.S.C. § 2511(2)(c). So, too, would the banners, as an implied consent. United States v. Workman, 80 F.3d 688, 693 (2d Cir. 1996); United States v. Lanoue, 71 F.3d. 966, 981 (1st Cir. 1995).