

FBI
b6
b7c

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.⁶⁷⁰

(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.)

DOE
b6
b7c

(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)

OOE
b6
b7c

FBI
b6
b7c

(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

OOE
b6
b7c

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.)

~~TOP SECRET~~ [REDACTED]

"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/NT) 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]

b1

[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)

(S/RD/NT) [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] [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] (12/15/99) SSA [REDACTED] thought that Lee would have had to go to the vault. (Id.) That is what he was told by LANL scientists in

~~TOP SECRET~~ [REDACTED]

(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]

DOE
FBI
b6, b7c

[REDACTED] They would simulate this weapon on a computer to test it."⁶²⁶ (FBI 00803)

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)

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.

FBI
b6, b7c

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.)

10E
b6
b7C

(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

FBI
b6
b7C

(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.⁶²

[REDACTED] 12/20/99)

DOE
b6, b7C

FBI
b6
b7C

(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. 61

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

(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)

FBI
b6, b7C

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

[REDACTED] (Id.)

b1

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.

FBI
b6
b7C

(U) SA [REDACTED] notes show that he had a meeting with SSA [REDACTED] on April 29, 1997 regarding the FISA application. (AQI 05367) Among the targets of surveillance, SA [REDACTED] had listed "home computer" and "office computer." (Id.) Next to this last item, SA [REDACTED] 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 [REDACTED] was zeroing in on a crucial investigative step.

(U)

(S/NF) In fact, on May 6, 1997, SA [REDACTED] interviewed [REDACTED] and learned that Wen Ho Lee was "quite sophisticated on a mainframe computer . . . [but] less sophisticated regarding a personal computer."⁶²⁹ (FBI 00891) SA [REDACTED] and [REDACTED] 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

DOE
b6
b7C

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

~~TOP SECRET~~ [REDACTED]

FBI
b6
b7c

download from the LANI, 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)

DOE
b6, b7c

(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

DOE
b6, b7c

⁶³⁰(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.

DOE
b6, b7c

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."

b1

~~TOP SECRET~~ [REDACTED]

~~TOP SECRET~~ [REDACTED]

FBI
b6
b7C

(U) It is baffling that SA [REDACTED] and [REDACTED] Lee's X Division [REDACTED] 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 [REDACTED] 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

DOE
b6
b7C

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

⁶³²(U) [REDACTED] recalled SA [REDACTED] asking about the computer equipment used by Wen Ho Lee. He recalled providing SA [REDACTED] with a list of Lee's equipment. [REDACTED] did not recall if [REDACTED] knew at the time why SA [REDACTED] wanted this information. [REDACTED] did not think that he ever asked. [REDACTED] did not recall a discussion of searching or monitoring Lee's computer in the 1997 or 1998 time frame. [REDACTED] could not recall ever talking to SA [REDACTED] about searching Lee's computer. In fact, [REDACTED] did not recall talking to anyone about searching Lee's computer before March 1999. [REDACTED] believed that [REDACTED] 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] could not be certain of this, however. [REDACTED] 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 [REDACTED] 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)

~~TOP SECRET~~ [REDACTED]

(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.

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

FBI
b6
b7C

(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
b6
b7C

(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
b6
b7c

DOE
b6
b7c

(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 "IA 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
b6
b7c

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
b6, b7c

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
b6
b7c

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
b6, b7c

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. [REDACTED] 9/13/99; [REDACTED] 9/7/99)

DOE
b6
b7c

9. (S//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]

[REDACTED] (AQI 01795) As

(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.

(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

~~TOP SECRET~~ [REDACTED]

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]

[REDACTED]

(S/RD/NF) [REDACTED]

[REDACTED]

(AQI 01667)

~~TOP SECRET~~ [REDACTED]

(S/NP) As an indication of the importance of [REDACTED]

b1

[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.

DOE
b6, b7c

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

DOE
FBI
b6
b7c

(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.⁶⁰ [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.⁶¹ (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.⁶² (Id.)

⁶⁰(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)

⁶¹(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)

⁶²(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,

~~TOP SECRET~~ [REDACTED]

DOE
FBI

b6

b7C

(U) According to [REDACTED] SA [REDACTED] already knew about the on-line acknowledgment of computer monitoring,⁶³ 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.⁶⁴ (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.)

⁶³ (U) [REDACTED] referred to this on-line acknowledgment as a "waiver" [REDACTED] 9/13/99), as have other witnesses and reports.

⁶⁴ (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] [REDACTED] 3/10/00)

~~TOP SECRET~~ [REDACTED]

(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

~~TOP SECRET~~ [REDACTED]

Lee transferred them in 1993 and 1994 until they were deleted by Lee in 1999.⁶⁴
(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:

00E
b6
b7C

(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] [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] [REDACTED] who provided [REDACTED] with the "Rules of Use" forms, containing an express consent to monitoring, signed by Lee.⁶⁵ (FBI 00209)

FBI
b6
b7C

⁶⁵(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)

(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]

~~TOP SECRET~~ [REDACTED]

~~TOP SECRET~~ [REDACTED]

(U) [REDACTED] predecessor was [REDACTED] the person whom, in December 1996, X Division [REDACTED] suggested that SA [REDACTED] contact for assistance with [REDACTED].⁶⁴⁷ As discussed above, according to [REDACTED] 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.⁶⁴⁸ (Omnibus 11/30/99) [REDACTED] the "Rules of Use" forms, which were specific to X Division. Had [REDACTED] been asked by the FBI about searching or monitoring Wen Ho Lee's computer, or if [REDACTED] 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 [REDACTED] 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 [REDACTED] in November 1996. (FBI 00211) When interviewed by the FBI on May 10, 1999, [REDACTED] said that [REDACTED] had confirmed that Wen Ho Lee "is listed in [REDACTED] computer as one of the employees who did go through the online training process." (Id.) When interviewed by the AGRT, however, [REDACTED] did not recall either being asked to verify that Wen Ho Lee had registered or ascertaining that Lee had registered. [REDACTED] 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 [REDACTED] 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)

⁶⁴⁷(U) According to Lee, he never met SA [REDACTED] until the Senate Governmental Affairs Committee hearings into the handling of the investigation. (Omnibus 11/30/99)

⁶⁴⁸(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.

~~TOP SECRET~~ [REDACTED]

FBI

b6

b7c

DOE

b6

b7c

~~TOP SECRET~~ [REDACTED]

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

~~TOP SECRET~~ [REDACTED]

~~TOP SECRET~~ [REDACTED]

mentioned the "Rules of Use" forms, which [REDACTED] knew to have been signed by everyone in X Division. ⁶⁹ [REDACTED] (12/21/99)

DOE
FBI
b6
b7c

(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. ⁶⁹ [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

⁶⁹(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]. [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.

⁶⁹(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.

~~TOP SECRET~~ [REDACTED]

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

~~TOP SECRET~~ [REDACTED]

the users were to disconnect the workstation from the port.⁶³³ 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.⁶³⁴ 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.⁶³⁵ (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

⁶³³(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.

⁶³⁴(U) The X Division secure and open LANs were physically separate systems.

⁶³⁵(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.

~~TOP SECRET~~ [REDACTED]

~~TOP SECRET~~ [REDACTED]

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 ^{DOE} _{66,67C} 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

~~TOP SECRET~~ [REDACTED]

~~TOP SECRET~~ [REDACTED]

Doc
b6
b7c
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 existed 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)

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.

DOE
b6
b7c

(U)
⁶⁵⁷(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)

~~TOP SECRET~~ [REDACTED]

(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)

DOE
b6
b7C

(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.⁶⁹ (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.)

c. (U) LANL's NADIR System

FBI
b6
b7C

(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

DOE
b6
b7C

⁶⁹(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)

report.⁶⁰ 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)

FBI
b6
b7C

DOE
b6
b7C

(U) The NADIR system monitored activities on the open and secure ICN, including the supercomputers Sigma, Tao, and Theta, Machine C, and the CFS.⁶¹ 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.⁶² (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.

⁶⁰(U) According to [REDACTED]

[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
b6
b7C

⁶¹(U) The NADIR system is maintained on a server that is part of the ICN. (Omnibus 11/30/99)

⁶²(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)

FBI
b6
b7C

~~TOP SECRET~~ [REDACTED]

[REDACTED] 9/11/99) According to SA [REDACTED] 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 [REDACTED] 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.

00E
b6
b7C

(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, [REDACTED] did not contact Lee for an explanation, however. (FBI 15838) [REDACTED] characterized this incident as "common." (Id.) [REDACTED] 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) [REDACTED] also noted that the NADIR system generates thousands of anomaly reports per year, and [REDACTED] is the only investigator responsible for looking into all of them. [REDACTED] just could not follow up on all of them. (FBI 15839)

(S/NF)

[REDACTED]
[REDACTED] (LANL 001954 & 2054)

b1

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. ⁶⁰³ [REDACTED] 9/11/99; Omnibus 11/30/99) The

FBI
b6
b7C

⁶⁰³(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

~~TOP SECRET~~ [REDACTED]

~~TOP SECRET~~ [REDACTED]

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." (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)

~~TOP SECRET~~ [REDACTED]

~~TOP SECRET~~ [REDACTED]

another computer help desk inquiry: "wants to replace one file in a tar file on a tape."⁶⁶
(FBI 13525) Then on February 17, 1999, Lee made his "Final deletion of tar file 15.
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

⁶⁶(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)

~~TOP SECRET~~ [REDACTED]

~~TOP SECRET~~ [REDACTED]

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

~~TOP SECRET~~ [REDACTED]

~~TOP SECRET~~ [REDACTED]

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.

~~TOP SECRET~~ [REDACTED]

~~TOP SECRET~~ [REDACTED]

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 download 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

~~TOP SECRET~~ [REDACTED]

~~TOP SECRET~~ [REDACTED]

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;
- DOE
b6
b7C 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; FBI
b6
b7C
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.

~~TOP SECRET~~ [REDACTED]

~~TOP SECRET~~ [REDACTED]

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;

~~TOP SECRET~~ [REDACTED]

~~TOP SECRET~~ [REDACTED]

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.").

~~TOP SECRET~~ [REDACTED]

~~TOP SECRET~~ [REDACTED]

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).

(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

~~TOP SECRET~~ [REDACTED]

DOE
FBI
b6
b7C

~~TOP SECRET~~ [REDACTED]

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

~~TOP SECRET~~ [REDACTED]

~~TOP SECRET~~ [REDACTED]

(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 Gossmeier 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).

~~TOP SECRET~~ [REDACTED]

~~TOP SECRET~~ [REDACTED]

(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").

~~TOP SECRET~~ [REDACTED]

~~TOP SECRET~~ [REDACTED]

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

~~TOP SECRET~~ [REDACTED]

~~TOP SECRET~~ [REDACTED]

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,

b1 | [REDACTED]

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).

~~TOP SECRET~~ [REDACTED]