PROSECUTING THE CIA: DOES THE COMPUTER FRAUD AND ABUSE ACT ALLOW FOR LIABILITY?♦

INTRODUCTION

In the computer security context, the term "hacker" is used to refer to someone who seeks weaknesses in a computer system or computer network.[1] Upon discovery, the hacker might exploit the weakness to gain unauthorized access to data. Unsurprisingly, few would expect the term to apply to the Central Intelligence Agency ("CIA"), an organization devoted in part to protecting against such unauthorized access. However, recent controversy involving the CIA and the Senate Select Committee on Intelligence ("SSCI") may indicate otherwise. In March of 2014, Senator Dianne Feinstein, chairperson of the SSCI, expressed fears that the CIA hacked into a standalone computer network used by SSCI staffers.[2] The hacking scandal dates back to January 2014,

[1] *See Hacker*, DICTIONARY.COM, http://dictionary.reference.com/browse/hacker (last visited Feb. 2, 2015).

[2] Luis Martinez, *Brennan Denies Claims CIA Hacked Senate Computers*, ABC NEWS (Mar. 11,

when the SSCI voted to initiate a comprehensive review of the CIA's notorious "Rendition, Detention, and Interrogation" program.[3] In the course of their investigation, SSCI staff members used the computer network to gain access to and investigate classified CIA documents containing information regarding the program.[4] Several CIA employees infiltrated the system when they discovered that the SSCI unintentionally gained accessed to an internal CIA memo, known as the Internal Panetta Review.[5] Significantly, the CIA's search may have violated the Computer Fraud and Abuse Act ("CFAA"). The CFAA is a computer trespass statute that prohibits intentional unauthorized access to computers, or hacking.[6] Although the Director of the CIA, John Brennan, initially denied any wrongdoing on behalf of the agency, the CIA Inspector General ("IG") recently released an investigative report stating that CIA officers improperly accessed or caused access to RDINet.[7] While the report does not expressly charge the CIA with violating the CFAA, an examination of the relevant case law and statutes reveals that the agency should be held criminally liable for hacking.

The CIA hacking scandal presents a novel set of facts and complex legal issues. For example, section (f) of the CFAA essentially provides blanket immunity for the CIA in the course of its intelligence duties.[8] Section (f) states that the CFAA does not prohibit law enforcement or intelligence agencies from engaging in "lawfully authorized" investigative activities.[9] If the CIA were to invoke section (f) in a case against the SSCI, a determination of immunity would ultimately turn on whether the CIA's actions were "lawfully authorized." Unfortunately, courts have never interpreted this section of the statute, nor decided what makes an activity "lawfully authorized." Nonetheless, this Note argues that the Fourth Amendment prohibits the CIA from invoking section (f) to validate the search. Other computer privacy statues with language similar to section (f) indicate that the term "lawfully

2014), http://abcnews.go.com/blogs/politics/2014/03/brennan-denies-claims-cia-hacked-senate-computers/.

3 *Id.*

4 *Id.*

5 Dianne Feinstein, *Statement on Intel Committee's CIA Detention, Interrogation Report*, DIANNE FEINSTEIN UNITED STATES SENATOR FOR CALIFORNIA (Mar. 11, 2014), http://www.feinstein.senate.gov/public/index.cfm/press-releases?ID=db84e844-01bb-4eb6-b318-31486374a895.

6 18 U.S.C. § 1030 (2012). The popular name "Computer Fraud and Abuse Act" was created in a 1986 amendment to 18 U.S.C. § 1030. *See* Pub. L. No. 99-474, 100 Stat. 1213, 1213 (1986). Section 1030 was initially created by the Comprehensive Crime Control Act of 1984. *See* Pub. L. No. 98-473, 98 Stat. 1976, 2190 (1984).

7 Feinstein, supra note 5; *Summary of Inspector General Report*, N.Y. TIMES (July 31, 2014), http://www.nytimes.com/interactive/2014/08/01/world/01cia-inspector-general-summary.html.

8 18 U.S.C. § 1030(f).

9 *Id.*

authorized" is limited in scope by the strictures of the Fourth Amendment, particularly the special needs doctrine.[10] Furthermore, the special needs doctrine, which provides an exception to the general requirement of individualized suspicion for searches, suggests that the CIA conducted an unreasonable search and violated the SSCI's reasonable expectation of privacy.[11]

Although section (f) does not exempt the CIA from liability, it is still unclear whether the CIA violated an express restriction of the CFAA. In order to establish liability under the statute, the government must prove that the CIA was "without authorization" to conduct the search.[12] However, the federal appellate courts are split on the definition of "without authorization."[13] The Ninth Circuit instructs that terms-of-service and other contractually based agreements, which provide acceptable-use policies for computers, are determinative of the issue of authorization.[14] The Fifth and Seventh Circuits hold that such agreements are non-determinative and that a user's actions cannot be deemed unauthorized merely for going beyond the scope intended by the provider.[15]

This Note explores whether the CIA can be held criminally liable under the CFAA for obtaining unauthorized access to RDINet. Two legal issues must be examined: (1) the scope of section (f)'s law enforcement exception; and (2) the definition of "without authorization" in the context of the CFAA. Part I of this Note traces the development of the CFAA, showing how the Act has evolved and explaining the rationale behind its many changes. Part II presents the particular facts of the CIA hacking scandal and the events leading up to its occurrence. Part III analyzes the necessary elements of proof in a potential suit against the CIA and examines the Fourth Amendment's relationship with the CFAA, particularly § 1030(f). Part IV further examines other portions of § 1030 to determine whether the CIA lacked authorization to conduct its search of RDINet. Lastly, Part V concludes that section (f) is limited by the strictures of the Fourth Amendment and asserts that the CIA lacked authorization to conduct its search.

---

10 *See* 18 U.S.C. §§ 2510–2522 (2012); 18 U.S.C. §§ 2701–2709, 2711–2712 (2012).

11 *See* New Jersey v. T.L.O., 469 U.S. 325 (1985). *See also* O'Connor v. Ortega, 480 U.S. 709 (1987).

12 18 U.S.C. § 1030(a)(1).

13 Molly Eichten, *The Computer Fraud and Abuse Act – A Survey of Recent Cases*, 66 BUS. LAW. 231, 232 (2010).

14 LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1129–30 (9th Cir. 2009); United States v. Nosal, 676 F.3d 854, 856 (9th Cir. 2012) (en banc).

15 Int'l Airport Centers, L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006); United States v. John, 597 F.3d 263 (5th Cir. 2010).

I. BACKGROUND

A. *Enactment of the CFAA*

The early 1980s marked the dawn of the computer age as the development of the microchip made computers available to an unprecedented number of Americans.[16] Unfortunately, this new technology spurred a then unseen type of crime, namely cybercrime.[17] In response, Congress penned the original version of 18 U.S.C. § 1030, as growing concern emerged over the lack of criminal laws available to combat emerging computer crimes.[18] Section 1030 was included within the Comprehensive Crime Control Act of 1984 and established three new federal crimes.[19] These included computer misuse to obtain national security secrets, computer misuse to obtain personal financial records, and hacking into U.S. government computers.[20] More generally, the provisions prohibited "knowingly access[ing] a computer without authorization, or having accessed a computer with authorization, us[ing] the opportunity such access provides for purposes to which such authorization does not extend."[21] The legislative history indicates that Congress intended these provisions to provide a "clearer statement of proscribed activity" to "the law enforcement community, those who own and operate computers, as well as those who may be tempted to commit crimes by unauthorized access."[22] In essence, Congress tailored the statute to three specific government interests: national security, financial records, and government property.[23]

After the enactment of § 1030, Congress continued to investigate problems associated with computer crime to determine whether federal criminal laws required further revision.[24] This was done in response to heavy criticism for making the statute overly vague and too narrow in the range of potential issues it covered.[25] In 1986, only two years after

16 COMPUTER CRIME & INTELLECTUAL PROP. SECTION, CRIMINAL DIVISION, U.S. DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES 1 (2d ed. 2010), *available at* http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf.
17 *Id*.
18 *Id*.
19 *Id.*
20 Orin Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1564 (2010).
21 Comprehensive Crime Control Act of 1984 § 2102(a)(1)–(3), Pub. L. No. 98-473, 98 Stat. 1976.
22 H.R. Rep. No. 98-894, at 6 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3692.
23 Kerr, *supra* note 20, at 1564.
24 COMPUTER CRIME & INTELLECTUAL PROP., *supra* note 18.
25 *Id*.

the statute's original enactment, Congress significantly expanded the statute by passing Pub. L. No. 99-474, formally known as the Computer Fraud and Abuse Act ("CFAA").[26] In expanding the statute, Congress added three new prohibitions.[27] Section 1030(a)(4) prohibits unauthorized access to a computer with the intent to defraud, which is the traditional crime of wire fraud committed using a computer.[28] Section 1030(a)(5) prohibits accessing a computer without authorization and altering, damaging, or destroying information, thereby causing either $1,000 or more of aggregated loss or impairing a medical diagnosis, treatment, or care of one or more individuals.[29] Lastly, § 1030(a)(6) prohibits trafficking in computer passwords.[30]

B. *The CFAA Today*

Congress has amended the CFAA eight times since its enactment in 1986, increasing the breadth of computers covered with each amendment.[31] As it stands today, the CFAA prohibits unauthorized access to any "protected computer," which the statute defines as any computer "used in or affecting interstate or foreign commerce or communication."[32] The phrase "affecting interstate . . . commerce" signals congressional intent to cover as far as the Commerce Clause will allow.[33] Moreover, every computer around the world that can be regulated under the Commerce Clause is a "protected computer" covered by the CFAA.[34]

The modern version of the CFAA contains seven separate criminal provisions, three of which the CIA may have violated. Section (a)(1) prohibits exceeding authorized access or obtaining unauthorized access to computers containing information pertaining to national security.[35] Section (a)(2)(B) prohibits intentionally accessing a computer without authorization or exceeding authorized access and thereby obtaining information from any department or agency of the United States; or, under (a)(2)(C), information from any protected computer.[36] Section (a)(3) prohibits the intentional and unauthorized access of any nonpublic computer of a department or agency within the United States that is exclusively for the use of the United States government.[37]

---

[26] Kerr, *supra* note 20, at 1564.
[27] *Id.* at 1565.
[28] *Id.*
[29] *Id.*
[30] *Id.*
[31] COMPUTER CRIME & INTELLECTUAL PROP., *supra* note 18.
[32] 18 U.S.C. § 1030(e)(2)(B).
[33] Kerr, *supra* note 20, at 1570.
[34] *Id.*
[35] 18 U.S.C. § 1030(a)(1).
[36] § 1030(a)(2)(B)–(C).
[37] § 1030(a)(3).

While sections (a)(1) and (a)(3) are specific in scope, section (a)(2)(C) essentially regulates all forms of computer use.[38] Thus, criminal liability under the CFAA depends almost entirely on whether a prosecutor considers a particular activity to be authorized or unauthorized. Every criminal provision in the CFAA prohibits accessing a computer "without authorization," and three provisions prohibit "exceed[ing] authorized access" to a computer.[39] Despite the obvious importance of such terms, the statute provides little to no guidance on how to distinguish between authorized and unauthorized access.

C. *Defining Authorization*

Notwithstanding Congress's numerous attempts to further clarify and narrow the scope of the statute, the meaning of the statute's most important term, "authorization," remains exceedingly ambiguous. The CFAA defines "exceeds authorized access" as accessing a computer with authorization and using such access to obtain or alter information in the computer that the accesser is not entitled to so obtain or alter.[40] However, the CFAA does not define "without authorization," and courts differ on the meaning and scope of the phrase, as well as whether use (or misuse) of information even implicates the CFAA.[41] Moreover, the federal courts of appeal are split on the issue.[42] The two most prominent interpretations developed by the courts include the contract/agency approach and the code approach.[43] The Fourth and Ninth Circuits adhere to the code approach, which provides that once a user has authorization, he or she cannot be charged for accessing "without authorization" merely because his or her actions went beyond the scope intended by the provider.[44] However, the Fifth and Seventh Circuits follow the contract/agency approach, which holds that a violation of a contractual agreement constitutes "without authorization."[45] The U.S. Supreme Court has not yet addressed the issue nor granted certiorari in any case decided by the courts of appeal.[46]

In *LVRC Holdings LLC v. Brekka*, a civil case, an employee emailed himself confidential documents from his employer's computer with the intent to use the information to compete with the employer after his termination.[47] The employer brought a CFAA action against

[38] § 1030(a)(2)(c).
[39] *See* § 1030.
[40] *See* § 1030(e)(6).
[41] *See* Eichten, *supra* note 13, at 232.
[42] David A. Thaw, *Criminalizing Hacking, Not Dating: Reconstructing the CFAA Intent Requirement*, 103 J. CRIM. L. & CRIMINOLOGY 907, 909–10 (2013).
[43] *Id.* at 910.
[44] *Id.*
[45] *Id.*
[46] *Id.* at 909.
[47] *See Brekka*, 581 F.3d at 1129–30.

the employee, asserting that the employee acted "without authorization" at the moment he decided to use the computer contrary to the employer's interest.[48] However, the court rejected this argument and held that "without authorization" means "without permission."[49] Applying this new rule, the court held that the employee had authorization (*i.e.*, permission) to access the computer because his job required him to use the computer.[50]

The Ninth Circuit reinforced this rule in *United States v. Nosal*.[51] In *Nosal*, the defendant, a high-level executive at a large company that provided executive recruitment services, left to start a competing business.[52] After departing the company, Nosal and two of his former coworkers who remained at the company made a deal to provide Nosal with confidential information from the company's database in order to benefit the competing company.[53] Nosal and his former coworkers were charged with violating § 1030(a)(4), which prohibits unauthorized access to a computer to further a scheme to defraud.[54] While the defense argued that the Ninth Circuit does not contemplate misuse of information obtained through authorized access as a criminal violation, the district court initially denied Nosal's motion to dismiss the indictment.[55] However, following the Ninth Circuit's decision in *Brekka*, the district court reheard argument and granted the motion.[56] The Ninth Circuit Court of Appeals, sitting en banc, affirmed the district court's ruling.[57]

Both *Brekka* and *Nosal* are in direct contrast to *International Airport Centers, L.L.C. v. Citrin*, a 2006 Seventh Circuit decision.[58] In *International Airport*, the court held that an employee's authorization to access an employer's computer ended when the employee breached his duty of loyalty to the employer.[59] The court used agency principles and held that the defendant breached his duty of loyalty after deleting evidence that showed that he had started a competing company in violation of his employment contract.[60] Moreover, access is deemed unauthorized when the employee harms or acts contrary to the

[48] *Id.* at 1133.
[49] *Id.*
[50] *Id.*
[51] *Nosal*, 676 F.3d at 856.
[52] *Id.*
[53] *Id.*
[54] *Id.*
[55] *Id.*
[56] *Id.*
[57] *Id.* at 864.
[58] *Int'l Airport*, 440 F.3d at 418.
[59] *Id.* at 420.
[60] *Id.*

employer's interest.[61] Once an employee breaches his duty of loyalty to his employer, he no longer has authorization to access such information.[62]

In *United States v. John*, the government charged the defendant with violating the CFAA when, as a Citigroup employee, she used Citigroup computers to access information concerning customer accounts to incur fraudulent charges on Citigroup customer financial accounts.[63] John appealed her jury conviction on the grounds that the CFAA only prohibited unlawful acquisition of information, not unlawful use following authorized acquisition.[64] The Fifth Circuit rejected this interpretation, holding that access can be limited by purpose and that "[s]he was not authorized to access [customer] information for any and all purposes but [rather] for limited purposes."[65] The court noted the Ninth Circuit's concerns in *Brekka* regarding potential defendants lacking constitutionally required notice of changes in policy, reasoning alternatively that an "authorized computer user has reason to know that he or she is not authorized to access data or information in furtherance of a criminally fraudulent scheme."[66]

II. THE FACTS

On March 5, 2009, the SSCI voted to initiate a comprehensive review of the CIA Detention and Interrogation program.[67] Following the vote, the SSCI immediately requested that all relevant executive branch agencies, including the CIA, forward documents pertaining to the program to SSCI headquarters.[68] While the SSCI preferred that the CIA turn over all responsive documents to its office, the former Director of the CIA, Leon Panetta, proposed an alternative arrangement.[69] Panetta suggested that the CIA provide "internal emails, memos, and other documents pursuant to the committee's document requests at a secure location in Northern Virginia."[70] The SSCI agreed, subject to a number of conditions.[71] According to an exchange of letters in 2009 between the various heads of the CIA and the SSCI, the CIA agreed to "provide a stand-alone computer system with a network drive segregated from CIA networks for the committee that would only be accessed by information

[61] *Id.*
[62] *Id.* at 420–21.
[63] *John*, 597 F.3d at 263.
[64] *Id.* at 271.
[65] *Id.* at 272.
[66] *Id.* (internal quotation marks omitted).
[67] Feinstein, *supra* note 5.
[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] *Id.*

technology personnel at the CIA."[72] CIA IT personnel "would not be permitted to share information from the system with other [CIA employees], except as otherwise authorized by the committee."[73] According to a Senate staff member familiar with the database, the computer network contains the cables, spot reports, interrogation logs, and other details of the CIA's "black sites," a network of prisons around the world where captured Al-Qaeda operatives are questioned before being sent to Guantanamo Bay.[74]

In addition to demanding that any review of documents produced for the SSCI be held at a CIA facility, the CIA also insisted on conducting a multi-layered review of every responsive document before providing the document to the committee.[75] This ensured that the CIA did not mistakenly provide documents unrelated to the CIA's Detention and Interrogation Program or provide documents that the President of the United States could claim to be covered by executive privilege.[76]

In 2010, SSCI staff gained access to several draft versions of a document titled the "Internal Panetta Review" on RDINet.[77] CIA personnel wrote the Internal Panetta Review to summarize and analyze the materials provided to the SSCI on RDINet.[78] The documents comprising the Internal Panetta Review were no more highly classified than other information the SSCI received for its investigation—in fact, they appeared to be based on the same information already provided to the SSCI on RDINet.[79] It is still unknown whether the CIA intentionally provided the Internal Panetta Review to SSCI staff, or whether a whistleblower intentionally provided it.[80] While some of the documents within the Internal Panetta Review contained markings indicating that they were "privileged," the Senate Legal Counsel confirmed that Congress does not recognize such claims of privilege with respect to documents provided to Congress in the course of its oversight duties.[81] Moreover, the executive branch provided these documents "pursuant to an authorized congressional oversight investigation," leading the SSCI to believe that it had every right to review them.[82]

Shortly after identifying the Panetta Review documents, the CIA

[72] *Id.* (internal quotation marks omitted).
[73] *Id.* (internal quotation marks omitted).
[74] Eli Lake, *What's Inside CIA's 'Black Site' Database? And Were Senate Staffers Allowed to See?*, DAILY BEAST (Mar. 7, 2014), http://www.thedailybeast.com/articles/2014/03/07/what-s-inside-cia-s-black-site-database-and-were-senate-staffers-allowed-to-see.html.
[75] Feinstein, *supra* note 5.
[76] *Id.*
[77] *Id.*
[78] *Id.*
[79] *Id.*
[80] *Id.*
[81] Feinstein, *supra* note 5.
[82] *Id.*

removed access to the vast majority of the documents on RDINet.[83] However, the SSCI thought little of this as it was focused on reviewing other material. Two years later, the SSCI approved a 6300 page committee study of the CIA's Detention and Interrogation program and sent the study to the executive branch for comment.[84] While the CIA agreed with some of the study's findings, it disputed several important parts.[85] Coincidentally, the CIA-disputed findings were acknowledged in the Panetta Review documents.[86] In an effort to corroborate this information, the SSCI transported a printed portion of the few Panetta Review documents still on RDINet to a designated SSCI office space in the Hart Senate Office Building.[87] In late 2013, Senator Dianne Feinstein requested that the CIA provide a final and complete version of the Internal Panetta Review to the committee.[88] Shortly thereafter, CIA Director Brennan requested an emergency meeting to inform the committee that CIA personnel conducted a search of the committee computers at the offsite facility.[89] This investigation involved not only a search of documents provided to the committee by the CIA, but also a search of the "stand alone" and "walled-off" committee network drive containing the committee's own internal work product and communications.[90] According to Brennan, the computer search was conducted in response to indications that some members of the committee staff might already have access to the Internal Panetta Review.[91]

III. ARGUMENT

A. *Framing The Issues*

In order to ascertain whether the CIA is liable for hacking under the CFAA, it is necessary to determine who controlled access rights to the accessed network (i.e., who owned or operated the network).[92] According to the agreement between the CIA and SSCI, the SSCI and its staff had exclusive access to RDINet, with the exception of CIA IT

[83] *Id.*
[84] *Id.*
[85] *Id.*
[86] *Id.*
[87] Feinstein, *supra* note 5.
[88] *Id.*
[89] *Id.*
[90] *Id.*
[91] *Id.*
[92] Orin Kerr, *Did the CIA Violate the Computer Fraud and Abuse Act by Accessing Intelligence Committee Computers?*, LAWFARE (Mar. 12, 2014), http://www.lawfareblog.com/2014/03/did-the-cia-violate-the-computer-fraud-and-abuse-act-by-accessing-intelligence-committee-computers/.

personnel.[93] However, CIA IT employees could not share information on RDINet with other CIA personnel.[94] Thus, while the CIA technically created and owned the system, the SSCI functioned as its primary operator.[95] Further complicating the matter is the lack of case law on how to resolve conflicting claims of control between owners and operators.[96] According to Orin Kerr, an expert on computer crime law, the "[c]ourts haven't even been clear that it's the owner/operator who controls access generally; the statute [18 U.S.C. § 1030] assumes this and the cases reflect it, but courts haven't been clear on the point because it hasn't come up."[97]

Second, even if the SSCI qualified as the network's primary operator, the CIA's method of access may not have violated any specific provision of the CFAA. If the barrier preventing CIA access was a code-based restriction, such as a password, then the issue of authorization is fairly clear. Section 1030(a)(6) expressly restricts bypassing password-protected computers without authorization.[98] However, if the barrier were merely a contractual agreement, then the circuit split would be implicated. According to the CIA IG's report, five agency employees, two attorneys, and three IT staff members improperly accessed the SSCI majority shared staff drives on RDINet.[99] Since CIA IT staff members were implicated in violating the access restriction, the most probable theory of liability rests on establishing a violation of the contractual agreement. Moreover, no CIA personnel other than the IT staff were permitted access to the system.[100] Thus, one can only assume that the three IT staff members shared information stored on the system with other CIA personnel.

Third, even if the SSCI controlled access rights and the CIA breached an access restriction, the CIA's access of RDINet may not have been intentionally unauthorized if the CIA indeed thought that it had rights to access the network.[101] The circumstances surrounding the hacking scandal indicate that the CIA conducted its search after learning that the SSCI was mistakenly granted access to the Internal Panetta Review.[102] Moreover, § 1030(f) provides that the CFAA "does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a

93 *Id.*
94 Feinstein, *supra* note 5.
95 *See* Kerr, *supra* note 92.
96 *Id.*
97 *Id.*
98 18 U.S.C. § 1030(a)(6) (2012).
99 *Summary of Inspector General Report*, *supra* note 7.
100 Feinstein, *supra* note 5.
101 Kerr, *supra* note 92.
102 Feinstein, *supra* note 5.

political subdivision of a State, or of an intelligence agency of the United States."[103] According to several CIA officials, the CIA gained lawful authorization under section (f) to conduct the search after learning that the SSCI had obtained access to the Internal Panetta Review.[104] In other words, the "CIA legitimately believed that a classified internal document had come to be in the possession of [the SSCI] by unknown means," which constituted "a legitimate basis to conduct a security inquiry."[105] However, no court has ever interpreted this section of the statute, nor for that matter what makes an activity "lawfully authorized."

B. *Examining Different Hypotheticals*

The theories of liability upon which the government would rely in a hypothetical prosecution of the CIA for hacking are purely conjectural and have never been argued in court. Likewise, the legal implications that accompany this factual scenario are vast and complex. Most significantly, the CIA's involvement in this case implicates section (f) of the CFAA, complicating matters even further. As mentioned previously, section (f) provides that the CFAA does not prohibit lawfully authorized investigative activities of any law enforcement or intelligence agency of the United States.[106] Thus, in order to provide context and to understand how the CFAA generally functions in more ordinary hacking scenarios, an examination of various CFAA hypotheticals involving different parties is instructive.

Assessing the implications of an ordinary citizen hacking into RDINet provides a logical starting point. The first step in the analysis is to determine whether access of the system by an ordinary citizen would be unauthorized. Since the SSCI had exclusive access to RDINet (with the exception of CIA IT personnel), if an ordinary citizen were to access the network, his or her access would undoubtedly be unauthorized. Moreover, the only way in which an ordinary citizen could gain access to the system would be by hacking — i.e., by bypassing CIA security measures installed to prevent outside access. This is expressly prohibited by the CFAA.[107] The next step is to determine what specific provision or provisions of the CFAA the ordinary citizen would violate. The documents stored on RDINet contained information concerning the CIA's Detention and Interrogation program,[108] and such information

103 18 U.S.C. § 1030(f).
104 Lake, *supra* note 74.
105 Chris Donesa, *SSCI v. CIA – Three Key Questions*, LAWFARE (Mar. 12, 2014, 9:00 AM), http://www.lawfareblog.com/2014/03/ssci-v-cia-three-key-questions/.
106 § 1030(f).
107 *See* § 1030.
108 Feinstein, *supra* note 5.

pertains to national security.[109] Section (a)(1) forbids anyone from knowingly accessing, without authorization, information relating to national defense or foreign relations.[110] Thus, the ordinary citizen could be prosecuted under section (a)(1) of the CFAA.[111] Additionally, the information obtained is stored on computers under the supervision of either the CIA or the SSCI, both of which are considered "departments or agencies of the United States."[112] Section (a)(2)(B) expressly prohibits intentionally accessing a computer without authorization and thereby obtaining information from any department or agency of the United States.[113] Lastly, the computers comprising RDINet fall within the CFAA's definition of "protected computers."[114] Thus, the ordinary citizen could be held liable under section (a)(2)(C) of the statute as well.[115]

The next logical scenario involves examining how the CFAA would be applied if the CIA, or for that matter any law enforcement agency, gained unauthorized access to the computer of an ordinary citizen. First and foremost, this scenario presents a very different set of circumstances. The accessed computer in this case is not government-owned and most likely does not contain information pertaining to national defense, foreign relations, nor any department or agency of the government. Therefore, no theory of liability exists with respect to sections (a)(1),[116] (a)(2)(a) or (b),[117] nor (a)(3).[118] The only theory of liability the ordinary citizen might prevail on would be to argue that his or her computer is a "protected computer" as defined under the statute.[119] However, even if such argument could be made successfully, the CIA or other law enforcement agency could likely invoke immunity under section (f) of the statute, depending on its reasons for conducting the search.[120] Section 1030 does not prohibit any "lawfully authorized investigative . . . or intelligence activity of a law enforcement agency of the United States . . . or of an intelligence agency of the United States."[121] Thus, liability would ultimately turn on whether or not the search was lawfully authorized.

109 *Id.*
110 § 1030(a)(1).
111 *Id.*
112 § 1030(e)(7).
113 § 1030(a)(2)(B).
114 § 1030(e)(2)(B).
115 § 1030(a)(2)(C).
116 § 1030(a)(1).
117 § 1030(a)(2)(A)–(B).
118 § 1030(a)(3).
119 § 1030(e)(2)(B).
120 § 1030(f).
121 *Id.*

C. *The Wiretap Act And The Electronic Communications Privacy Act*

Although the courts have never interpreted section (f) of the CFAA, other federal privacy statues with similar law enforcement exceptions to the one found in section (f), particularly the Wiretap Act and the Electronic Communications Privacy Act ("ECPA"), indicate that the meaning of the phrase "lawfully authorized" must comply with the terms of the Fourth Amendment.[122] A brief history of the Fourth Amendment and the influence it wielded in the crafting of these statutes demonstrates why. The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[123] It provides that these rights shall not be violated, and no warrants shall issue, but upon probable cause.[124] In *Katz v. United States*, the U.S. Supreme Court held that this language prevents the government from infringing upon a reasonable expectation of privacy in one's communications, whether oral, written, or electronic, without prior judicial authorization based on a showing of probable cause.[125] As Justice Harlan explained, the requirement is two-fold.[126] In order to maintain a reasonable expectation of privacy over their person, houses, papers, or effects, he or she must have exhibited an actual, subjective expectation of privacy, and the expectation must be one that society is prepared to recognize as reasonable.[127] Only with a warrant based upon probable cause can the government invade one's reasonable expectation of privacy.[128]

The Court expounded upon the procedures law enforcement officials must follow in obtaining a warrant in *Berger v. New York*.[129] The Court specified the Fourth Amendment's particularity requirement while examining the validity of a New York eavesdrop statute, N.Y. Code Crim. Proc. § 813-a.[130] Section 813-a authorized New York courts to issue "ex parte order[s] for eavesdropping upon oath or affirmation of a district attorney, or of the attorney-general or of an officer above the rank of sergeant of any police department of the state."[131] The statute required that the oath provide reasonable grounds to believe that evidence of a crime may be obtained.[132] Additionally, it mandated that the oath accurately describe the person or persons being eavesdropped

122 *See* 18 U.S.C. §§ 2510–2522 (2012); 18 U.S.C. §§ 2701–2709, 2711–2712 (2012).
123 U.S. CONST. amend. IV.
124 *Id.*
125 *See* Katz v. United States, 389 U.S. 347 (1967).
126 *See id.* at 361 (Harlan, J., concurring).
127 *Id.*
128 *See id.* at 362.
129 *See* Berger v. New York, 388 U.S. 41 (1967).
130 *See id.*
131 *Id.* at 54 (internal quotation marks omitted).
132 *Id.*

on, and specifically identify the telephone number involved.[133] However, the Court held that the statute violated the particularity requirement of the Fourth Amendment, which commands that a warrant issue not only upon probable cause, but also "particularly describ[e] the place to be searched, and the persons or things to be seized."[134] Section 813-a merely stated that "a warrant may issue on reasonable grounds to believe that evidence of crime may be obtained via [an] eavesdrop."[135] The statute laid down no requirement for particularity in the warrant, such as what specific crime had been or was being committed, the place to be searched, or the persons or things to be seized, as specifically required by the Fourth Amendment.[136] The Court noted that the need for particularity is especially great when seeking judicial authorization for eavesdropping.[137]

In response to *Katz* and *Berger*, Congress set up procedures for law enforcement officials to obtain judicial authorization for wiretapping and eavesdropping.[138] Enacted as Title III of the Omnibus Crime Control and Safe Streets Act ("Title III," often referred to as the "Wiretap Act"), the procedures are codified as amended at 18 U.S.C. §§ 2510–2522.[139] Congress extended the reach of these provisions to electronic communications in 1986 via the ECPA.[140] Moreover, § 2511 of the Wiretap Act provides that it is unlawful for anyone to intentionally intercept any wire or electronic communication.[141] However, § 2518 of the Act authorizes courts to issue special orders permitting law enforcement officials to intercept the contents of such communications.[142] Unlike section (f) of the CFAA, which merely states that lawfully authorized investigative activities by intelligence agencies are not prohibited,[143] the Wiretap Act requires that each application for an order authorizing such interception be supported upon oath or affirmation to a judge and state the applicant's authority to make such application.[144] Significantly, each order authorizing or approving

133 *Id.*
134 *Id.* at 55 (citations omitted).
135 *Id.* at 55-56.
136 *See id.* at 58.
137 *Id.* at 60.
138 *See* 18 U.S.C. §§ 2510–2522 (2012).
139 *Id.*
140 18 U.S.C. §§ 2701–2712 (2012).
141 18 U.S.C § 2511.
142 18 U.S.C. § 2518.
143 18 U.S.C. § 1030(f) (2012).
144 § 2518(3) (a judge may issue an order so long as he or she determines that: "(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter; (b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception; (c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous; [and] (d) except as provided in

such interception must "specify—(a) the identity of the person, if known, whose communications are to be intercepted; (b) the nature and location of the communication facilities as to which, or the place where, authority to intercept is granted; [and] (c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates."[145] The statute also contains an exception allowing certain high-level officials in the U.S. Department of Justice to proceed with an interception if an "emergency situation" requires that communications be acquired before a court order "can, with due diligence, be obtained."[146] This provision requires that the government apply for a full Title III order within forty-eight hours.[147]

Similarly, § 2701 of the ECPA prohibits "intentionally access[ing] without authorization a facility through which an electronic communication service is provided. . . and thereby obtain[ing]. . . authorized access to a wire or electronic communication while it is in electronic storage in such system. However, section 2703(a) provides a limited exception.[148] It states that a governmental entity may require a provider of an electronic communication service to disclose the contents of an electronic communication pursuant to a warrant using the procedures described in the Federal Rules of Criminal Procedure.[149]

In light of the Supreme Court's decisions in *Katz* and *Berger*, along with the general warrant procedures Congress employed in the law enforcement exceptions to the Wiretap Act and the ECPA, section (f) of the CFAA must be interpreted to comport with the Fourth Amendment. In other words, when Congress stipulated that section (f) does not prohibit any lawfully authorized investigative activity of a law enforcement or intelligence agency of the United States, it did not intend to exempt such law enforcement or intelligence agencies from complying with the Fourth Amendment. To suggest otherwise would contradict decades of Supreme Court precedent, and essentially permit law enforcement officials to engage in warrantless invasions of individuals' personal computers. Seeing as the information available on one's personal computer is much more voluminous and revealing in comparison to the types of communications described in the Wiretap Act and the ECPA, the Fourth Amendment must apply with equal if not more force to the CFAA.

subsection (11), there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.").

145 *Id.* § 2518(4)(a)–(c).

146 *See id.* § 2518(7).

147 *Id.*

148 18 U.S.C. § 2703(a) (2009).

149 *Id.*

D. *The Fourth Amendment and The CFAA*

The restrictions the Fourth Amendment places upon law enforcement officials in enforcing the Wiretap Act and the ECPA clearly apply to law enforcement officials enforcing the CFAA. However, the circumstances surrounding the CIA's search require an unconventional Fourth Amendment analysis. First, the CIA did not search a private citizen's computer.[150] Rather, it searched a congressional committee's computer network.[151] The text of the Fourth Amendment merely states that persons, not congressional bodies such as the SSCI, are protected against unreasonable searches and seizures.[152] The question then arises whether the SSCI, as a congressional body, can assert that it had a reasonable expectation of privacy in its deliberations concerning the CIA's detention and interrogation program. Second, the CIA did not conduct its search in the pursuit of criminal law enforcement.[153] Accordingly, the search falls under the Fourth Amendment's special needs doctrine.[154] Reasonableness in relation to the special needs doctrine is judged differently than traditional Fourth Amendment searches.[155]

Although the Fourth Amendment is principally directed at curbing governmental abuse of its criminal law enforcement power with regard to investigating the activities of private citizens, the strictures of the Fourth Amendment also apply to the conduct of governmental officials outside of the criminal law context.[156] Thus, the Amendment's prohibition on unreasonable searches is not limited to operations conducted by the police.[157] The Court has often characterized the Fourth Amendment's strictures as "restraints imposed upon governmental action–that is, upon the activities of sovereign authority."[158] Moreover, the Amendment's fundamental purpose is to protect the privacy and security of individuals against arbitrary invasions by government officials.[159] As the court noted in *New Jersey v. T.L.O.*, "[b]ecause the individual's interest in privacy and personal security suffers whether the government's motivation is to investigate violations of criminal laws or breaches of other statutory or regulatory standards, it would be anomalous to say that the individual and his private property are fully protected by the Fourth Amendment only when the individual is

150 Feinstein, *supra* note 5.
151 *Id.*
152 U.S. CONST. amend. IV.
153 Feinstein, *supra* note 5.
154 *See* New Jersey v. T.L.O., 469 U.S. 325 (1985).
155 *See id.* at 341–42.
156 *See id.* at 334–35.
157 *Id.* at 335.
158 *Id.* (internal quotation marks omitted).
159 *Id.*

suspected of criminal behavior."[160]

For example, in *O'Connor v. Ortega*, a state-employed physician alleged that hospital officials investigating workplace misconduct had violated his Fourth Amendment rights by conducting a warrantless search of his office and seizing personal items from his desk and filing cabinet.[161] The entire court agreed with the general principle that "individuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer."[162] Moreover, the Court explained that because "some government offices may be so open to fellow employees or the public that no expectation of privacy is reasonable," a court must consider the operational realities of the workplace in order to determine whether an employee's Fourth Amendment rights are implicated.[163] Personal work spaces seldom operate as "private enclave[s] free from entry by supervisors, other employees, and business and personal invitees."[164] Rather, fellow employees and other visitors typically enter offices throughout the workday for conferences and other work-related reasons.[165] Thus, according to the Court, whether an employee has a reasonable expectation of privacy must be assessed "on a case-by-case basis," in light of whether his or her office is so accessible to fellow colleagues or the general public that no expectation of privacy is reasonable.[166]

Comparing the facts of *Ortega* to the present case, one could conclude that SSCI committee members are not CIA employees.[167] Nevertheless, the CIA's relationship with the SSCI is sufficiently analogous to constrain the CIA in the same manner that the Court constrained the hospital officials in *Ortega*. The searching parties in both cases maintained supervisory roles.[168] The public officials in *Ortega* managed the daily operations of the hospital, while the CIA administered the functioning of RDINet.[169] In other words, both oversaw the administration of their respective workplaces. So, the same rationale the court applied in *Ortega* to recognizing a state-employed physician's reasonable expectation of privacy over his workplace should be employed in the case of the SSCI.[170]

Applying the plurality's rationale in *Ortega*, a court would likely find that SSCI staff had a reasonable expectation of privacy in its

160 *Id.* at 335 (internal quotation marks omitted).
161 O'Connor v. Ortega, 480 U.S. 709 (1987).
162 *Id.* at 717.
163 *Id.* at 718.
164 *Id.* at 717.
165 *Id.*
166 *Id.* at 718.
167 *See id.* at 717–18; Feinstein, *supra* note 5.
168 *See Ortega*, 480 U.S. at 717–18; Feinstein, *supra* note 5.
169 *See Ortega*, 480 U.S. at 717–18; Feinstein, *supra* note 5.
170 *See Ortega*, 480 U.S. at 717–18; Feinstein, *supra* note 5.

documents stored on RDINet. RDINet contained separate electronic shared drives for use by several entities, including the SSCI Majority and Minority staff members and CIA personnel supporting the review and redaction of documents provided to the SSCI review team.[171] Following review of relevant documents by the RDI team, responsive documents were then made available to SSCI staff members on their shared drives.[172] While CIA IT personnel had access to RDINet, their access was restricted to their respective drives.[173] These facts indicate that the SSCI sought to preserve the documents on its drive as private. In other words, the SSCI exhibited an actual, subjective expectation of privacy. It is very likely that society would deem this expectation objectively reasonable, as documents stored on a Senate-maintained network drive are generally considered private.[174]

However, determining that the SSCI had a reasonable expectation of privacy over its drive on RDINet is not determinative of whether the CIA's search violated the SSCI's Fourth Amendment rights. As the Court declared in *T.L.O.*, "[t]o hold that the Fourth Amendment applies to searches conducted by [public employers] is only to begin the inquiry into the standards governing such searches. . . . [W]hat is reasonable depends on the context within which a search takes place."[175] To determine the appropriate standard of reasonableness in a particular class of searches, one must balance "the nature and quality of the intrusion on [an] individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion."[176] In *Ortega*, the court balanced "the invasion of the [physician's] legitimate expectations of privacy against the government's need for supervision, control, and the efficient operation of the workplace."[177] Furthermore, after balancing the interests, the Court agreed that special needs, beyond the need for law enforcement, render the warrant and probable cause requirement impracticable for government employers.[178] The Court reasoned that imposing such requirements would interfere with the completion of the government's work in a prompt and efficient manner, and seriously disrupt its routine conduct of business.[179] Ultimately these requirements would impose intolerable burdens on public employers, as the delay they would impose "in correcting the employee misconduct . . . [would] be

171 Feinstein, *supra* note 5.
172 *Id.*
173 *Id.*
174 *See id.*
175 *T.L.O.*, 469 U.S. at 337.
176 United States v. Place, 462 U.S. 696, 703 (1983).
177 *See Ortega*, 480 U.S. at 719–20.
178 *Id.* at 725.
179 *Id.*

translated into tangible and often irreparable damage to the agency's work, and ultimately to the public interest."[180]

Although the balancing of the interests is slightly different in the case of the CIA and the SSCI, the result is arguably the same. In supervising the operation of RDINet, the CIA had two principal interests. The first involved ensuring that the SSCI received documents pertaining to the CIA's detention and interrogation program in a prompt and efficient manner.[181] The second involved ensuring that the SSCI was not mistakenly provided access to documents unrelated to the CIA's Detention and Interrogation program.[182] Balancing these interests against the SSCI's legitimate expectation of privacy in its drive on RDINet suggests that imposing warrant and probable cause requirements would unduly burden the CIA. For instance, if the CIA unintentionally uploaded a sensitive or classified document to RDINet not meant for the SSCI, imposing warrant and probable cause requirements could prevent the CIA from quickly removing the document from the system. This could irreparably damage the CIA's work and severely harm the public interest.

Nevertheless, "[d]etermining the reasonableness of any search involves a twofold inquiry: first, one must consider whether the . . . action was justified at its inception; second, one must determine whether the search as actually conducted was reasonably related in scope to the circumstances which justified the interference in the first place."[183] Likewise, reasonableness inquiries regarding the conduct of searches must take into account the nature of the parties involved and the events leading up to the search.[184] Here, the CIA, an executive agency, conducted its search when it believed the SSCI, a legislative committee, had obtained the Internal Panetta Review and failed to return it.[185] The SSCI's failure to promptly return the Internal Panetta Review indicates that the search was justified at its inception.[186]

However, the nature of the parties involved and the events leading up the search require an uncharacteristic reasonableness inquiry.

---

180 *Id.* at 724.

181 *See* Feinstein, *supra* note 5.

182 *See id.*

183 *Ortega*, 480 U.S. at 726 (quoting New Jersey v. T.L.O., 469 U.S. 325 (1985)).

184 *See T.L.O.*, 469 U.S. at 337 (Court held that public school officials could search students without a warrant provided there existed "*reasonable grounds* for suspecting that [a] search will turn up evidence that a student violated . . . the laws or rules of the school." So long as a search does not excessively intrude on the student in light of his or her age, sex, and the nature of the infraction, the search remains reasonable).

185 *See* Feinstein, *supra* note 5.

186 *See Ortega*, 480 U.S. at 726 ("Ordinarily, a search of an employee's office by a supervisor will be 'justified at its inception' when there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct, or that the search is necessary for a noninvestigatory work-related purpose such as to retrieve a needed file").

Moreover, the CIA and the SSCI come from different branches of government, and the search occurred in response to a congressional investigation relating to alleged abuse of executive branch authority.[187] Such circumstances suggest that any assessment of reasonableness in this case must account for the attendant separation of powers principles inherent in this inter-branch dispute.[188]

E. *Separation of Powers*

Although the Constitution does not explicitly give Congress the power to investigate in the performance of its oversight duties, the Supreme Court has said that "[t]he power of Congress to conduct investigations is inherent in the legislative process."[189] The Court has also recognized that:

> [This] power is broad. It encompasses inquiries concerning the administration of existing laws as well as proposed or possibly needed statutes. It includes surveys of defects in our social, economic or political system for the purpose of enabling the Congress to remedy them. It comprehends probes into departments of the Federal Government to expose corruption, inefficiency or waste.[190]

In *Barenblatt v. United States*, Justice Harlan wrote that "[t]he scope of the power of inquiry . . . is as penetrating and far reaching as the potential power to enact and appropriate [funds] under the Constitution."[191]

The modern congressional oversight structure emerged in the mid 1970s after information came to light regarding several covert CIA operations of which Congress had been entirely unaware.[192] In the summer of 1974 Congress learned of the CIA's alleged role in the assassination plot of Chilean President Salvador Allende, as well as its support to rebels opposing the communist regime in Angola.[193] In December of that same year Congress learned that the CIA "undertook aggressive programs to collect information on groups and individuals in this country opposed to the war in Vietnam."[194] "Following these disclosures both Houses of Congress [voted to] create[] special

187 Feinstein, *supra* note 5.
188 *Id*. *See also* U.S. Const. art. I–III.
189 Watkins v. United States, 354 U.S. 178, 187 (1957).
190 *Id.*
191 Barenblatt v. United States, 360 U.S. 109, 111 (1959).
192 L. Britt Snider, *Congressional Oversight of Intelligence: Some Reflections on the Last 25 Years*, DUKE UNIV. SCH. OF LAW, CTR. FOR LAW, ETHICS, AND NAT'L SEC. 1 (2004), https://web.law.duke.edu/lens/downloads/snider.pdf.
193 *Id.*
194 *Id.*

investigating committees," known as the Church and Pike committees, to investigate the inner workings of the CIA and other intelligence agencies.[195] Their findings revealed that the existing congressional oversight structure had failed.[196] Little was known in terms of "what the Agency was doing with taxpayers' money."[197] Congress had essentially "left the Agency to its own devices, trusting that its work was important and necessary."[198] Consequently, the Church and Pike committees recommended instituting permanent Senate and House select committees on intelligence to monitor and oversee the CIA.[199]

In creating these new committees, "Congress, above all, sought to achieve awareness" of the CIA's activities.[200] For example, the Senate resolution that created the SSCI stated that it was "'the sense of the Senate' that the committee be kept 'fully and currently informed with respect to intelligence activities' and that the heads of intelligence agencies 'should furnish any information or documentation in the possession, custody, or control' of the agency when requested by the committee."[201] In the years following their creation, the House and Senate committees have "recognized no limit on their right to obtain information or documentation from the Intelligence Community."[202] They were, however, "willing to accept limitations and conditions on their access (so long as they got it) when they knew that particularly sensitive information was at issue."[203]

When analyzing the CIA's search in the context of these oversight norms, it is apparent that the search violated the chief principle upon which the SSCI was founded, namely, achieving awareness of the CIA's daily operations and objectives. The search directly interfered with the SSCI's investigation of the CIA's detention and interrogation program, and ultimately prevented Congress from informing itself on the inner workings of the CIA.[204] On a more fundamental level, the search contravened the system of checks and balances embodied within the Constitution.[205] The CIA essentially took the law into its own hands. According to Senator Feinstein, the CIA's actions "may have undermined the constitutional framework essential to effective

195 *Id.*
196 L. Britt Snider, *Congressional Oversight of Intelligence: Some Reflections on the Last 25 Years*, DUKE UNIV. SCH. OF LAW, CTR. FOR LAW, ETHICS, AND NAT'L SEC. 1 (2004), https://web.law.duke.edu/lens/downloads/snider.pdf.
197 *Id.* at 2.
198 *Id.*
199 *Id.* at 3.
200 *Id.* at 5.
201 *Id.*
202 *Id.*
203 *Id.*
204 Feinstein, *supra* note 5.
205 *See generally* U.S. CONST. art. I–III.

congressional oversight of intelligence activities or any other government function."[206] Several other SSCI committee members have echoed Senator Feinstein's concerns. Senator Saxby Chambliss of Georgia, "generally a staunch ally of the intelligence community," remarked that "this is a serious situation and there are serious violations."[207] Senator Chambliss "called for [] C.I.A. employees to be 'dealt with harshly.'"[208] Senator Mark Udall also demanded John Brennan's resignation.[209] Both senators accused "the C.I.A. [of] unconstitutionally sp[ying] on Congress by hacking into the Senate Intelligence Committee computers."[210] According to Udall, "[t]his grave misconduct not only is illegal but it violates the U.S. Constitution's requirement of separation of powers."[211] Senator Feinstein went so far as to label the search a "defining moment in the committee's history," stating that "how the matter [is] resolved will show whether the Intelligence Committee can be effective in monitoring and investigating our nation's intelligence activities, or whether our work can be thwarted by those we oversee."[212] In all, the CIA's violation of traditional separation of powers principles confirms that the CIA conducted an unreasonable Fourth Amendment search. Thus, the CIA cannot assert that it had lawful authorization to conduct the search under § 1030(f) of the CFAA.

IV. AUTHORIZATION

The fact that section (f) is inapplicable in this case does not automatically render the CIA liable for its actions.[213] It still must be determined whether the CIA lacked authorization to access RDINet under the CFAA's other provisions.[214] The question of access is perhaps the most difficult hurdle the prosecution would face in attempting to hold the CIA liable under the CFAA. "The structure of the CFAA presumes that there is a computer owner or operator who controls access rights to each computer, much like an owner/operator controls access rights to physical property."[215] However, in the case of the CIA and the SSCI, there is no clear operator or owner. The CIA owned the machines, whereas the SSCI operated them. Under the framework of the

206 Feinstein, *supra* note 5.
207 Mark Mazzetti and Carl Hulse, *Inquiry by C.I.A. Affirms It Spied on Senate Panel*, N.Y. TIMES (July 31, 2014), *available at* http://www.nytimes.com/2014/08/01/world/senate-intelligence-commitee-cia-interrogation-report.html.
208 *Id.*
209 *Id.*
210 *Id.*
211 *Id.*
212 *Id.*
213 18 U.S.C. § 1030 (2012).
214 *Id*.
215 Kerr, *supra* note 92.

CFAA, each party has a legitimate claim that it retained superior access rights over RDINet. While Orin Kerr, a nationally recognized scholar of computer crime law, indicated that "the CIA probably has a better claim to controlling access than the Committee, as it is both the owner of the machine and maintains some residual rights to have IT people access the computers," he admitted that this was just his "instinct."[216]

Assuming the SSCI controlled access rights to RDINet, whether the CIA could be held liable turns on what standard a court would use to determine the issue of authorization. For example, both the Fifth and Seventh Circuits have held that violations of contractual like agreements and misuse of accessed information fall within the CFAA's definition of "without authorization."[217] Their decisions support the notion that the CIA was without authorization to access RDINet in the manner revealed in the CIA Inspector General's Report. Moreover, the terms of the agreement between the SSCI and the CIA provided that CIA IT personnel could access RDINet solely for IT reasons, and that the information they accessed could not be shared with any other CIA employees.[218] The CIA Inspector General's Report revealed that CIA IT personnel improperly accessed SSCI staff files and records on RDINet.[219] More particularly, CIA IT personnel conducted a search of the stand-alone and walled-off committee drive containing the committee's own internal work product.[220] In other words, they accessed RDINet for non-IT related reasons. This constitutes a violation of the CIA's agreement with the SSCI, and in turn indicates that the CIA lacked authorization to conduct the search.

On the other hand, both *Brekka* and *Nosal* support the proposition that the CIA's actions were authorized under the CFAA.[221] Both decisions embrace the code approach to authorization, which provides that once a user has authorization, he or she cannot be charged for accessing "without authorization" merely because his or her actions went beyond the scope intended by the provider.[222] As mentioned prior, the agreement between the CIA and the SSCI provided that CIA IT personnel would access RDINet solely for IT reasons.[223] This included reviewing and uploading documents to the SSCI's drive on RDINet.[224] Additionally, the agreement prohibited CIA IT staff from sharing any

216 *Id.*
217 18 U.S.C. § 1030 (2012). *See* Int'l Airport Ctrs., L.L.C., v. Citrin, 440 F.3d at 418; United States v. John, 597 F.3d at 263.
218 Feinstein, *supra* note 5.
219 *Summary of CIA Inspector General Report*, *supra* note 7.
220 *Id.*
221 *See Brekka*, 581 F.3d at 1127; *Nosal*, 676 F.3d at 856.
222 *Id.*
223 Feinstein, *supra* note 5.
224 *Id.*

information they accessed on RDINet with other CIA employees.[225] Nevertheless, such agreements have no bearing on the element of authorization. According to the Seventh and Eleventh Circuits, "without authorization" is merely defined as without permission.[226] Seeing as CIA IT staff had permission to access RDINet, the fact that their actions went beyond the scope of the agreement is of no consequence.[227]

Despite the lack of a uniform definition of "without authorization," the separation of powers issues inherent within this dispute suggest that the contract/agency approach is better equipped to resolve the issue as opposed to the code approach. Moreover, the underlying rationale supporting the code approach is inapplicable in the case of the CIA. The code approach implies, among other things, that unauthorized access must be interpreted so as to give "sufficient notice of what is criminal."[228] If the CFAA is interpreted to prohibit accessing a computer for reasons not intended by the provider, computer users lack sufficient notice of what constitutes valid computer use.[229] For example, in the employer-employee context, an employee could be held liable for merely accessing his employer's computer for personal reasons.[230] While these policy concerns are valid, they should not dictate the outcome of this case. The CIA surely did not lack notice that its actions violated basic separation of powers principles. Similarly to the defendants in *John*, the CIA had reason to know that it did not have authorization to access the SSCI's computer network in the manner that it did.[231] For these reasons, the CIA should be deemed to have lacked authorization under the CFAA to conduct the search at issue.

CONCLUSION

In sum, § 1030(f) of the CFAA does not support the proposition that the CIA had lawful authorization to conduct a search of the SSCI's drive on RDINet. As demonstrated by other computer privacy statutes, section (f) must be interpreted to comport with the Fourth Amendment. Although the Fourth Amendment is predominantly aimed at preventing against governmental abuse of its criminal law enforcement power, the special needs doctrine provides that the strictures of the Fourth Amendment apply outside of the criminal law context. Accordingly, the SSCI possessed a reasonable expectation of privacy over their drive on RDINet, which the CIA then violated when it accessed SSCI work

225 *Id.*
226 *See Brekka*, 581 F.3d 1127; *Nosal*, 676 F.3d 854.
227 Feinstein, *supra* note 5; *see Brekka*, 581 F.3d 1127; *Nosal*, 676 F.3d 854.
228 Kerr, *supra* note 20, at 1586.
229 *Id.*
230 *Id.*
231 *Id. See also John*, 597 F.3d at 263.

product. While the CIA had a reasonable suspicion to suspect that the SSCI had mistakenly obtained the Internal Panetta Review, separation of powers principles indicate that the conduct of CIA intrusion failed to match the level of suspicion. In other words, the CIA acted unreasonably in conducting its search.

Nevertheless, the fact that section (f) does not authorize the CIA's search says nothing about their potential liability with regard to the CFAA's other provisions. The vagueness of the CFAA with respect to defining access rights in terms of the owner/operator framework suggests that the CIA may have a legitimate claim that it retained superior access rights to those of the SSCI. Furthermore, case law interpreting the CFAA is divided with respect to the definition of without authorization. Any successful prosecution would thus be dependent upon the case falling within either the Fifth or Seventh Circuit's jurisdiction. However, no matter what court the case arises in, the CIA would be hard-pressed to legitimately defend its actions when considering the separation of powers principles it violated in conducting the search. The rationale behind the code approach simply does not support the proposition that the CIA had authorization to conduct its search of RDINet.

*Sam Taterka**

* Associate Editor, CARDOZO ARTS & ENT. L.J. Vol. 34, J.D. Candidate, Benjamin N. Cardozo School of Law (2016); B.A., Political Science, *cum laude*, The George Washington University (2007). Thank you to Professors Brett Frischmann and Kyron Huigens for their guidance, editing and helpful comments throughout the process and to the Vol. 33 and 34 *Cardozo Arts & Entertainment Law Journal* Boards for their suggestions and encouragement. I am especially thankful for my parents, James and Toni, my brothers, Ben and Charlie, and Katie O'Brien. I could not have written this without their unwavering love and support.