

Just Add Plaintiff: The Seventh Circuit's Recipe for Instant Liability Under the Computer Fraud and Abuse Act [*Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418 (7th Cir. 2006)]

Dan E. Lawrence*

I. INTRODUCTION

Judges have a unique position relative to the subject matter on which they rule. In a legal sense, the court's jurisdiction is narrowly defined; in a lay sense, it can be boundless. Judges are called upon to issue rulings of law and make findings of fact in technical subject matter without any specialized training.¹ Common sense tells us that a butcher should not evaluate the work of an electrician, nor should a computer programmer assess the surgical skills of a physician. Nonetheless, judges with no technical training are required to find facts and develop opinions, based on their own knowledge and whatever they can glean from expert testimony and other evidence, on matters that are typically the province of professionals with years of formal training. Those opinions then become binding law.

In *International Airport Centers, L.L.C. v. Citrin*,² the United States Court of Appeals for the Seventh Circuit found itself in such a position when it was called upon to evaluate a technical term in the

* B.A. 2003, University of Kansas; J.D. Candidate 2008, Washburn University School of Law. For more gifts than I can name, I would like to thank my wife, my brother, and my parents. Additionally, I would like to thank Prof. Aida Alaka for her assistance throughout the writing process.

1. An example currently in litigation is *SCO Group, Inc. v. IBM*. SCO Group (SCO) is a software company whose main products are UNIX-based operating systems called SCO UnixWare and SCO OpenServer. See The SCO Group, Inc., Products, <http://www.sco.com/products/unix/> (last visited Sept. 23, 2006). SCO claimed that IBM contributed SCO's intellectual property in the form of several hundred lines of computer code to the Linux project, an open source and freely distributed operating system consisting of millions of lines of code. See Amended Complaint at ¶ 150(e), *SCO Group, Inc. v. IBM*, No. 03-0294 (D. Utah July 22, 2003) (“[IBM contributed] protected source code and methods for incorporation into one or more Linux software releases, intended for transfer of ownership to the general public . . .”); see also David A. Wheeler, *More Than a Gigabuck: Estimating GNU/Linux's Size*, <http://www.dwheeler.com/sloc/redhat71-v1/redhat71sloc.html> (2002) (size of one version of the Linux operating system estimated at 30 million lines of code). Because SCO seeks to establish that its proprietary code is incorporated into Linux, litigation of the case may require examination and comparison of large quantities of complex code, a task normally reserved for programmers, computer engineers, and similar professionals. See Amended Complaint at ¶ 150(e), *SCO Group, Inc. v. IBM*, No. 03-0294. The court may therefore be required to make findings of fact on subject matter that most laypersons would consider highly technical (e.g., comparisons of code written in software development languages).

2. 440 F.3d 418 (7th Cir. 2006).

Computer Fraud and Abuse Act (CFAA).³ The Seventh Circuit ignored the guidance provided by other jurisdictions and developed its definition of “transmission” from the ground up, relying on its own judgment and what it deemed the colloquial meaning of the term.⁴

The resulting opinion is problematic in several ways. Most notably, it has the potential to extend liability under the CFAA to a class of actors outside Congress’s intended scope. Under the Seventh Circuit’s precedent, simply installing an operating system on a computer and then using the functionality present by default in that operating system could make an individual liable under the CFAA.⁵

II. CASE DESCRIPTION

Jacob Citrin was an employee and partial owner of International Airport Centers (IAC), a real estate investment firm.⁶ One of Citrin’s responsibilities was to locate properties that IAC might potentially purchase or invest in, record data about the properties on a company-owned laptop, and then help to acquire those properties.⁷

The event that set the litigation in motion was a change in the ownership of IAC. Previously a privately held, relatively small and consolidated organization, IAC sold a 50% ownership interest to one of its principal competitors, AMB Property Corporation (AMB).⁸ IAC also sold an additional 39% to Verizon Communications, but retained 11% for itself.⁹ Shortly after the company’s sale, Citrin resigned from his position as IAC’s Managing Director.¹⁰

IAC and Citrin disputed Citrin’s motivation for resigning.¹¹ Citrin claimed that he resigned because he was concerned about working for large organizations such as AMB and Verizon, and that he might face

3. 18 U.S.C. § 1030 (2000 & Supp. IV 2004) [hereinafter CFAA].

4. Courts that construed the element of transmission held that a transmission occurred when the code or software transmitted underwent some movement, whether by being physically shipped or by being transmitted electronically over a network. The Seventh Circuit found that a transmission occurred even when neither of these conditions was met. *See* discussion *infra* Part V.A.

5. As discussed in this comment, the Seventh Circuit construed the transmission element of 18 U.S.C. § 1030(a)(5)(A)(i) so that the act of installing any software, including an operating system, could satisfy the element. If the operating system was then used to permanently delete data, the “intentionally caus[ing] damage” element of § 1030(a)(5)(A)(i) would be fulfilled. If the computer on which these acts were performed qualified as a “protected computer” and the user accessed it “without authorization,” then all the ingredients for liability under § 1030(a)(5)(A)(i) would be met. *See infra* Part V.D.

6. Brief of Appellant at 4, *Int’l Airport Ctrs., L.L.C.*, 440 F.3d 418 (No. 05-1522).

7. *Int’l Airport Ctrs., L.L.C.*, 440 F.3d at 419.

8. AMB is a publicly held real estate development company more than twenty times the size of IAC. Brief of Appellee at 4-5, *Int’l Airport Ctrs., L.L.C.*, 440 F.3d 418 (No. 05-1522).

9. *Id.* at 5.

10. *Id.* at 9.

11. *Compare id.* (attributing Citrin’s decision to resign to his concerns about his new employers), *with* Brief of Appellant, *supra* note 6, at 5 (attributing Citrin’s decision to resign to his desire to enter into business for himself, in competition with his former employer and in violation of his employment agreement).

litigation from his new employers if he stayed.¹² Conversely, Citrin's former employers contend that he resigned to conduct his own business and compete with his former employer and its new owners in violation of the terms of his employment agreement.¹³ Regardless of his motivation, Citrin resigned and deleted data from his company-issued laptop before returning it.¹⁴ When Citrin removed the data from his laptop, he did not use the native delete functionality of the laptop's operating system.¹⁵ If he had done so, IAC could have recovered the data and determined what Citrin deleted.¹⁶ Instead, he installed the programs "Window Washer," "Ultra Destroy-It," and "Acronis Privacy Expert Suite," which were designed to render deleted data absolutely unrecoverable, and used these programs to delete data from his laptop.¹⁷

The litigants also contested the nature of the data deleted from Citrin's laptop.¹⁸ Citrin testified that he deleted personal information and pornography—testimony supported by the documents recovered from his laptop.¹⁹ Furthermore, a substantial number of IAC's spreadsheet and word-processing documents remained on the laptop when Citrin returned it, as well as 800 megabytes of IAC-related emails.²⁰ These facts alone, however, were not enough to convince IAC of Citrin's innocence.²¹ IAC found Citrin's story unconvincing and believed that he deleted evidence of his plan to compete with his former employer in violation of his employment agreement.²² IAC sued Citrin in the United States District Court for the Northern District of Illinois.²³

The district court dismissed the case for lack of subject matter ju-

12. Brief of Appellee, *supra* note 8, at 5, 9 (The sale agreement between IAC and AMB contractually obligated AMB to use litigation to enforce Citrin's noncompete if he chose to leave the company.).

13. Brief of Appellant, *supra* note 6, at 5.

14. *Int'l Airport Ctrs., L.L.C.*, 440 F.3d at 419.

15. *Id.*

16. *Id.*

17. Brief of Appellant, *supra* note 6, at 17; *see also* Acronis Privacy Expert Corporate Product Tour, <http://www.acronis.com/enterprise/products/privacyexpert/tour/> (last visited Sept. 23, 2006) (describing Acronis Privacy Expert's "secure data destruction" functionality); Ultra Destroy-It 2002 8.0 Review, <http://www.bluechillies.com/details/8912.html> (last visited Sept. 23, 2006) (describing Ultra Destroy-It's secure deletion functionality); Webroot Software, Window Washer, <http://www.webroot.com/consumer/products/windowwasher/> (last visited Sept. 23, 2006) (describing Window Washer's secure deletion functionality).

18. *Compare* Brief of Appellee, *supra* note 8, at 9 (describing the information deleted by Citrin as personal data belonging to him and his wife), *with* Brief of Appellant, *supra* note 6, at 5-6 (describing the information deleted by Citrin as evidence of his intent to compete with his former employer).

19. Some of the files that IAC determined Citrin deleted include [webcamteens\[1\].jpg](#), [gradedgirlbanner\[1\].gif](#), and [lostvirgin\[2\].htm](#). Brief of Appellant, *supra* note 6, at 18-19 n.8.

20. Brief of Appellee, *supra* note 8, at 9-10.

21. *Int'l Airports Ctrs., L.L.C. v. Citrin*, No. 03-8104, 2005 U.S. Dist. LEXIS 3905, at *2-3 (N.D. Ill. Jan. 31, 2005).

22. *See id.*

23. IAC argued that the district court had both diversity jurisdiction and federal question jurisdiction under 18 U.S.C. § 1030(a)(5)(A). *Id.* at *1-3. IAC also sought to extend supplemental jurisdiction to its state law claims of breach of fiduciary duty, conversion, misappropriation, and claims under the Illinois Trade Secrets Act and Illinois Computer Tampering Act. *Id.* at *2, *9.

risdiction.²⁴ Examining the legislative history of the CFAA, the court concluded that the main targets of the CFAA are hackers and authors of computer viruses and other malicious software.²⁵ Although the court acknowledged that the CFAA had been amended to make it more comprehensive and applicable to a broader class of offenders, the court did not find that Citrin's actions were within the scope of the statute.²⁶ Specifically, the court found that Citrin's installation of the software used to perform the secure deletion did not constitute a transmission under the CFAA.²⁷ The case was thus without a basis for federal subject matter jurisdiction and was dismissed.²⁸ IAC appealed the dismissal to the Seventh Circuit.²⁹

III. BACKGROUND

Congress passed the CFAA in 1984 to supplement existing mail and wire fraud laws, which were unsuited to deal with the new class of crimes made possible by computer technology.³⁰ Compared to its present state, the scope of the act was narrow.³¹ The act prohibited the acquisition of information related to national defense from a computer through unauthorized access if that information was subsequently used to harm the United States.³² It also criminalized unauthorized access to records of financial institutions and consumer reporting agencies, and extended protection to a broad category of machines that included any computer "operated for or on behalf of the Government of the United States."³³ Amendments to the CFAA have consistently expanded the scope of the act. This legislative trend, in combination with evidence of Congress's intent that the statute occupy the field of computer related crime, has led courts to construe the provisions of the CFAA broadly.³⁴

24. *Id.* at *9-10.

25. *Id.* at *4 (explaining that "the general purpose of the CFAA is to address the problem of computer crime, to protect computers and computer networks from access by hackers and to prevent the transmission of computer viruses or other harmful computer programs").

26. *Id.* at *4-5, *9.

27. *Id.* at *9. Additionally, the court found that the parties were not diverse because Citrin was a part owner of the plaintiffs' organization. *Id.* at *2.

28. *Id.* at *9-10.

29. *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418 (7th Cir. 2006).

30. David W. Garland & Linda B. Katz, *Computer Fraud and Abuse Act: Another Arrow in the Quiver of an Employer Faced with a Disloyal Employee - Part I*, METROPOLITAN CORP. COUNS., May 2006, at 5.

31. Dodd S. Griffith, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem*, 43 VAND. L. REV. 453, 460 (1990). Compare 18 U.S.C. § 1030 (1982 & Supp. II 1984) (prohibiting acquisition of defense information from a computer through unauthorized access if that information is then used to harm the United States, and criminalizing unauthorized access to the computers of financial institutions, consumer reporting agencies, and computers "operated for or on behalf of the Government of the United States"), with 18 U.S.C. § 1030 (2000 & Supp. IV 2004) (providing broad protection for private and government computers, and proscribing a more extensive range of behavior than previous versions of the act).

32. Griffith, *supra* note 31, at 460.

33. *Id.*; 18 U.S.C. § 1030 (1982 & Supp. II 1984).

34. See *Int'l Airport Ctrs., L.L.C. v. Citrin*, No. 03-8104, 2005 U.S. Dist. LEXIS 3905, at *4

Courts' broad construction of the CFAA has been bolstered by Congress's own frequent scope-broadening amendments to the CFAA.

A. The 1986 Amendments

The CFAA was amended for the first time in 1986.³⁵ The most significant effect of the 1986 amendments was the addition of 18 U.S.C. § 1030(a)(4)-(6), which extended the reach of the CFAA to three new categories of activity.³⁶ First, § 1030(a)(4) added a special injunction against fraudulent activity using a computer.³⁷ Second, § 1030(a)(5) extended the protection of the act to any "Federal interest computer"³⁸ and made it a violation to modify or destroy the information it contained, or to interfere with access to it by an authorized user.³⁹ Third, § 1030(a)(5) criminalized trafficking in computer passwords.⁴⁰ The CFAA was not amended again until 1994.⁴¹

B. The 1994 Amendments

As part of a comprehensive crime bill called "The Violent Crime Control and Law Enforcement Act of 1994," Congress amended the CFAA by replacing the phrase "Federal interest computer" with "computer used in interstate commerce or communications" and thereby ex-

(N.D. Ill. Jan. 31, 2005) (broadly stating the legislative intent of the CFAA as being "to address the problem of computer crime"); *see also* *United States v. Middleton*, 231 F.3d 1207, 1211 (9th Cir. 2000) (examining congressional intent as expressed by S. REP. NO. 104-357 in support of its broad construction of the term "individuals" to mean both persons and corporations for purposes of the CFAA); *Pac. Aerospace & Elecs., Inc. v. Taylor*, 295 F. Supp. 2d 1188, 1195 (E.D. Wash. 2003) (noting that "Congress has . . . continuously broadened the scope and coverage of the CFAA since its original enactment in 1984"); *In re AOL, Inc. Version 5.0 Software Litig.*, 168 F. Supp. 2d 1359, 1374 (S.D. Fla. 2001) (noting that "the CFAA has been increasingly broadened by Congress"); S. REP. NO. 104-357, at 5 (1996) (referring to the CFAA as *the answer to computer crimes of all types* "[T]he [CFAA] facilitates *addressing in a single statute the problem of computer crime* As computers continue to proliferate . . . and new forms of computer crimes emerge, Congress must remain vigilant to ensure that the [CFAA] . . . provides . . . the necessary legal framework to fight computer crime.") (emphasis added).

35. *See* 18 U.S.C. § 1030 (Supp. IV 1986).

36. Jeff Nemerofsky, *The Crime of "Interruption of Computer Services to Authorized Users" Have You Ever Heard of It?*, 6 RICH. J.L. & TECH. 23, ¶ 14 (2000), <http://www.richmond.edu/jolt/v6i5/article2.html>.

37. *Id.*

38. A "federal interest computer" is any computer

(A) exclusively [used by] a financial institution or the United States Government, or . . . used by or for a financial institution or the United States Government and the conduct constituting the offense affects the [Government or financial institution's use] of such computer; or

(B) which is one of two or more computers used in committing the offense, not all of which are located in the same State.

18 U.S.C. § 1030(e)(2)(A)-(B) (Supp. IV 1986).

39. Nemerofsky, *supra* note 36, at ¶ 14. Hypothetically, a hacker or other malicious intruder might prevent an authorized user from accessing the data a computer contains in a number of ways. Data might be moved or hidden. A user's username and password could be changed, preventing that user from logging into his or her computer. Network activity could be disrupted to prevent or hinder access to remote resources on a company's local network or the Internet.

40. *Id.*

41. *See* 18 U.S.C. § 1030 (1994).

tended the CFAA to the limits of congressional power permitted by the commerce clause.⁴² Another significant change the 1994 amendments introduced was to remove the requirement that a liable party under the CFAA access a protected computer without authorization.⁴³ The result expanded the scope of the act dramatically by allowing it to cover a new class of offenders, which included authorized users of third-party computers who use their trusted status to perform malicious activities.⁴⁴ This amendment closed loopholes in the original CFAA, which had limited applicability in situations where an authorized user caused harm to a computer system.⁴⁵ This amendment also made it possible to use the CFAA to prosecute a defendant who used a third party to effectuate harm by, for example, giving a computer disk containing harmful code to an authorized user for installation on a computer system.⁴⁶ Despite these far-reaching changes, however, Congress revisited the CFAA with another series of changes two years later, in 1996.⁴⁷

C. The 1996 Amendments

A third series of changes to the CFAA was introduced in 1996.⁴⁸ The scope of the act was extended from any computer “used in interstate commerce or communications” to any “protected computer,” a phrase defined in the CFAA to include government-operated or affiliated machines, financial institution computers, and computers used in interstate commerce or communications.⁴⁹ The change corrected a flaw introduced by the 1994 amendments, which replaced “Federal interest computer” with “computer used in interstate commerce or communications” and incidentally weakened the CFAA’s protection for computers that belonged to the federal government or financial institutions, but were not involved in interstate commerce or communications.⁵⁰ Once

42. Nemerofsky, *supra* note 36, at ¶ 26.

43. *Id.*

44. Examples of such users would include bitter ex-employees seeking to harm their former employers, corporate saboteurs, and, in the words of the Seventh Circuit, “disgruntled programmers.” *Int’l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006).

45. See 18 U.S.C. § 1030(a)(5) (1994); see also The National Information Infrastructure Protection Act of 1996: Legislative Analysis, http://www.usdoj.gov/criminal/cybercrime/1030_anal.html (last visited Sept. 25, 2006) [hereinafter NIIPA Analysis].

46. See § 1030(a)(5) (1994); see also NIIPA Analysis, *supra* note 45.

47. See 18 U.S.C. § 1030 (Supp. II 1996).

48. See also NIIPA Analysis, *supra* note 45 (noting that the 1996 amendments contain “substantive amendments [to] the [CFAA] to specifically address new abuses that spring from the misuse of new technologies”).

49. § 1030(a)(5) (Supp. II 1996); see also NIIPA Analysis, *supra* note 45.

50. § 1030(a)(5) (1994); see also NIIPA Analysis, *supra* note 45. It is also possible that this change was prompted by the Supreme Court’s decision in *United States v. Lopez*, 514 U.S. 549 (1995), and that opinion’s effect in curtailing Congress’s formerly *carte blanche* power under the Commerce Clause. The first such exercise of power by the Supreme Court since the Great Depression, *Lopez* held that the authority granted to Congress to regulate interstate commerce extended only to activities having a substantial effect on interstate commerce. *Lopez*, 514 U.S. at 556. In *Lopez*, the court found that Congress’s authority to regulate interstate commerce did not allow it to

the amendments of 1996 passed, the CFAA was not amended again until Congress was spurred into action by the terrorist attacks of September 11, 2001.

D. *The USA PATRIOT Act*

Congress passed the USA PATRIOT Act⁵¹ (PATRIOT Act) in October 2001 and further expanded the CFAA.⁵² Section 202 of the PATRIOT Act added suspected violations of the CFAA to the list of felonies for which the Federal Bureau of Investigation (FBI) could conduct wiretap surveillance.⁵³ Though the FBI already had the authority to intercept electronic communications such as email,⁵⁴ section 217 of the PATRIOT Act gave the FBI the ability to exercise that authority without first seeking judicial approval.⁵⁵ After the passage of the PATRIOT Act, communications passing through a protected computer could be intercepted and monitored so long as the law enforcement agency conducting the monitoring met four easily satisfied requirements.⁵⁶

Aside from authorizing the FBI to conduct wiretap surveillance for suspected violations of the CFAA, the PATRIOT Act introduced a variety of other plaintiff- and prosecutor-friendly changes.⁵⁷ The PATRIOT Act increased the maximum prison sentences for first- and second-time offenders to ten years and twenty years respectively.⁵⁸ The mens rea requirement of the CFAA, which formerly required a prosecutor to prove that a defendant specifically intended to cause one of several pre-defined types of damage, was relaxed and is now satisfied by any general intent to cause damage.⁵⁹ The amendments also permit victims and plaintiffs to aggregate damages by combining multiple inci-

criminalize possession of a firearm within a school zone because of the attenuated link between possession of a firearm in a school zone and interstate commerce. *Id.*

51. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified in scattered sections of 18 U.S.C. and 50 U.S.C.).

52. See generally Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA PATRIOT Act of 2001, <http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm> (last visited Sept. 25, 2006) [hereinafter Field Guidance] (cataloging provisions of the USA PATRIOT Act that expand the CFAA).

53. *Id.*; see also 18 U.S.C. § 2516(1)(c) (Supp. I 2001).

54. Field Guidance, *supra* note 52; see also 18 U.S.C. § 2703(c) (Supp. I 2001).

55. Field Guidance, *supra* note 52; see also 18 U.S.C. § 2511(2)(i) (Supp. I 2001).

56. Field Guidance, *supra* note 52; see also § 2511(2)(i)(I)-(IV) (stating communications sent to, by, or through a protected computer may be intercepted by law enforcement officers provided that 1) the law enforcement officers obtain permission from the owner or operator of the computer; 2) the law enforcement officers are participating in an ongoing investigation; 3) the law enforcement officers reasonably believe that the contents of the intercepted communications relate to the ongoing investigation; and 4) the law enforcement officers intercept only those communications sent by individuals who are accessing the protected computer without authorization).

57. See Field Guidance, *supra* note 52.

58. *Id.*; see also 18 U.S.C. § 1030(c)(4) (Supp. I 2001).

59. Field Guidance, *supra* note 52; see also § 1030(a)(5)(A)-(B) (Supp. I 2001).

dents to reach the \$5,000 damage threshold at which a violator becomes culpable under the CFAA.⁶⁰ Additionally, the PATRIOT Act created a new offense for violators damaging computers used in the administration of justice, national security, or national defense, even if the damage did not exceed the \$5,000 threshold or meet the requirements for culpability under other provisions of the CFAA.⁶¹ The scope of the CFAA's protection was also extended to computers in foreign countries if those computers affect interstate commerce within the United States.⁶² Overall, the PATRIOT Act significantly bolstered the effectiveness of the CFAA as a prosecutor's tool.

E. Case Law Interpreting the Element of Transmission

Congress did not define the element of transmission, leaving courts to develop their own interpretations.⁶³ Courts interpreting transmission and other elements of the CFAA have typically expanded its scope.⁶⁴ For instance, the Central District of California considered the element of transmission in *North Texas Preventive Imaging v. Eisenberg*.⁶⁵ There, the defendant developed and sold software used by the plaintiff.⁶⁶ The plaintiff decided that the software did not suit its needs and sought to cancel its contract with the defendant, as well as recover more than \$160,000 in licensing fees that it paid to the defendant.⁶⁷ In the ensuing conflict, the plaintiff learned that if the dispute was not resolved by the deadline specified by the defendant, the software system would be disabled.⁶⁸

The plaintiff also discovered that the defendant introduced a disabling mechanism into the software even before litigation commenced.⁶⁹ Prior to the dispute, the defendant customarily shipped update disks to the plaintiff on a regular basis.⁷⁰ It is not clear whether the update disks contained software updates, but it is clear that the disks contained a type

60. Field Guidance, *supra* note 52; *see also* § 1030(a)(5)(B)(i) (Supp. I 2001).

61. Field Guidance, *supra* note 52; *see also* § 1030(a)(5)(B)(v) (Supp. I 2001).

62. Field Guidance, *supra* note 52; *see also* § 1030(e)(2)(B) (Supp. I 2001).

63. *See* CFAA *supra* note 3 (defining many of the terms used in the CFAA, but omitting a definition of "transmission" or its root).

64. *See, e.g.,* Shurgard Storage Ctrs. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000) (finding that an employee's authorized access to his employer's computers is revoked at the moment he develops a subjective intent inconsistent with the duty of loyalty to the employer); YourNetDating, L.L.C. v. Mitchell, 88 F. Supp. 2d 870, 872 (N.D. Ill. 2000) (holding that damage to intangible goodwill can satisfy the damage requirement under the CFAA); Shaw v. Toshiba Am. Info. Sys., 91 F. Supp. 2d 926, 935 (E.D. Tex. 1999) (holding that the element of transmission under 18 U.S.C. § 1030(a)(5)(A)(i) is satisfied by shipment and delivery of hardware containing code).

65. No. SA CV 96-71 AHS, 1996 U.S. Dist. LEXIS 19990 (C.D. Cal. Aug. 19, 1996).

66. *Id.* at *3-4.

67. *Id.* at *5.

68. *Id.* at *6.

69. *Id.*

70. *Id.*

of software called a time bomb, which would disable the software sold to the plaintiff if it was not regularly updated using the floppy disks sent by the defendant.⁷¹ The plaintiff brought suit under the CFAA, claiming that the defendant's practice of shipping update disks containing disabling code violated § 1030(A)(5)(a).⁷²

The court struggled with the application of the CFAA to the facts of the case because no unauthorized party physically accessed the computer on which the time bomb was installed.⁷³ The defendant manufactured and shipped the disks, but an authorized party employed by the plaintiff received and installed them.⁷⁴ Intervention by a third party thus interrupted and attenuated the chain of transmission.⁷⁵ Ultimately, the court found that the shipment of the floppy disks containing the malicious software constituted a transmission so long as the defendant intended harm.⁷⁶

In yet another case, the District Court of New Jersey considered the definition of the element of transmission in *Gomar Manufacturing Co. v. Novelli*.⁷⁷ The facts of *Gomar* were similar to those of *North Texas Preventive Imaging*. The plaintiff in *Gomar* purchased a computer-controlled laminating machine from the defendant that contained a time bomb similar to the software in *North Texas Preventive Imaging*.⁷⁸ When the relationship between the parties broke down and the plaintiff stopped making payments, the time bomb caused the machine

71. *Id.* "Time bomb" within the context of *North Texas Preventive Imaging* referred to a code or program that "detonates" at a pre-set time and date, disabling itself or another application. *Id.*

72. *Id.* at *7-8. The content of this section has since been amended so that it is possible for an individual to violate it without having made a transmission; however, at the time of the lawsuit, transmission was key to the section:

[Whoever] through means of a computer used in interstate commerce or communications, knowingly causes the transmission of a program, information, code, or command to a computer or computer system if—

- (i) the person causing the transmission intends that such transmission will—
 - (I) damage, or cause damage to, a computer, computer system, network, information, data, or program; or
 - (II) withhold or deny, or cause the withholding or denial, of the use of a computer, computer services, system or network, information, data or program; and
- (ii) the transmission of the harmful component of the program, information, code, or command—
 - (I) occurred without the authorization of the persons or entities who own or are responsible for the computer system receiving the program, information, code, or command; and
 - (II)(aa) causes loss or damage to one or more other persons of value aggregating \$ 1,000 or more during any 1-year period; or (bb) modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals . . . [shall be punished as provided in subsection (c) of this section].

18 U.S.C. § 1030(a)(5) (1994) (emphasis added).

73. *N. Tex. Preventive Imaging*, 1996 U.S. Dist. LEXIS 19990, at *10-11.

74. *See id.* at *6.

75. *Id.*

76. *Id.* at *16.

77. No. 96-4000, 1998 U.S. Dist. LEXIS 23452 (D.N.J. Apr. 13, 1998).

78. *Id.* at *3-4.

to stop working, and the plaintiff was unable to make deliveries and fulfill other contractual obligations.⁷⁹ The court held that the shipment of the machine from defendant to plaintiff, along with the pre-installed malicious code, was a transmission.⁸⁰

The District Court for the Eastern District of Texas considered the meaning of transmission a year later in *Shaw v. Toshiba American Information Systems*.⁸¹ The plaintiffs were various members of a class and the defendant was Toshiba American Information Systems (Toshiba), a computer hardware manufacturer that distributed a component containing faulty code.⁸² The plaintiffs alleged that the defendant violated § 1030(a)(5), and that the shipment and distribution of the hardware containing the faulty code satisfied the element of transmission.⁸³

Toshiba moved for summary judgment, arguing that the shipment and distribution of the hardware containing the faulty code did not constitute a transmission under § 1030(a)(5), because a transmission required an electronic conveyance of data between two or more computers.⁸⁴ In its analysis, the court found that the 1996 amendments to the CFAA removed the requirement for computer-to-computer transmission by excising the phrase “through means of a computer used in interstate commerce or communications.”⁸⁵

The court also rejected Toshiba’s argument that the CFAA was only intended to cover acts by hackers, explaining that “this Court does not see a blanket exemption for manufacturers in [the CFAA]; nor does it see the term ‘hacking’ anywhere in this statute.”⁸⁶ In keeping with the trend set by the California and New Jersey courts, the Texas court held that either an electronic transfer or a marketplace transfer may satisfy the element of transmission, if the thing transmitted undergoes some substantial movement or travel through space.⁸⁷ Seven years later, courts still struggle to define transmission. The Seventh Circuit is the latest to consider the issue.

79. *Id.* at *4-5.

80. *See Shaw v. Toshiba Am. Info. Sys.*, 91 F. Supp. 2d 926, 934 (E.D. Tex. 1999) (recounting the discussion of transmission from *Gomar Mfg. Co. v. Novelli*, C.A. No. 96-4000 (D.N.J. Jan. 28, 1998)).

81. 91 F. Supp. 2d 926 (E.D. Tex. 1999).

82. *Id.* at 928.

83. *Id.* at 932.

84. *Id.*

85. *Id.* at 934 n.15 (explaining that “[i]n 1996 Congress amended subsection 1030(a)(5)(A) by deleting . . . ‘through means of a computer used in interstate commerce or communications.’ . . . [the Court] notes in passing that Congress[s] deletion of this qualifying phrase arguably removed the need for *computer-to-computer* ‘transmission’”).

86. *Id.* at 936.

87. *Id.*

F. *The CFAA and Secure Deletion Software*

It is possible that the CFAA was initially intended to target worms, viruses, trojan horses, and other malicious software.⁸⁸ Notwithstanding its originally intended targets, the act has since been applied to other, innocuous categories of software, including software used to generate unsolicited emails;⁸⁹ software used to collect usage statistics from users of a web site;⁹⁰ and automated software, called a “bot,” used to collect information from the pages of a group of related web sites.⁹¹ The application of the CFAA in *International Airport Centers* to the secure deletion software used by Citrin is therefore nothing new in this respect.

There is a significant difference, however, between *International Airport Centers* and prior cases in which the CFAA was used to prosecute an unlawful use of legitimate software. In the instant case, secure deletion software of the type used by Citrin is the native functionality of some operating systems.⁹² Macintosh OS X, for example, is a recently released version of an operating system that incorporates a “Secure Empty Trash” feature that offers secure deletion functionality.⁹³ Similarly, the “shred” command available in the Unix and Linux operating systems can be used to securely delete files.⁹⁴ Commercial and shareware versions of secure deletion software are also widely available for other operating systems, such as Windows, where secure deletion functionality is not present by default.⁹⁵ Secure deletion software is thus widely used and widely sought.

It is easy to understand computer users’ desire for secure deletion software and to understand the motivation that leads software developers, such as Macintosh, to provide such software. The delete functionality present on operating systems that do not have secure deletion capa-

88. A trojan horse is a program that appears to serve a useful purpose, but performs other, often malicious, functions. Wikipedia, Trojan Horse (computing), [http://en.wikipedia.org/wiki/Trojan_horse_\(computing\)](http://en.wikipedia.org/wiki/Trojan_horse_(computing)) (last visited Sept. 25, 2006); Findlaw’s Modern Practice – Technology Glossary for Lawyers, <http://practice.findlaw.com/glossary.html> (last visited Sept. 25, 2006). A computer virus is a self-replicating program that propagates itself among computers, often inflicting damage in the process. Wikipedia, Computer Virus, http://en.wikipedia.org/wiki/Computer_virus (last visited Sept. 25, 2006); WordNet Search 2.1, <http://wordnet.princeton.edu/perl/webwn?s=virus> (last visited Sept. 25, 2006). Similar to a virus, a worm propagates itself among networked computers, but inflicts damage by consuming bandwidth and affecting network performance. Wikipedia, Computer Worm, http://en.wikipedia.org/wiki/Computer_worm (last visited Sept. 25, 2006); WordNet Search 2.1, <http://wordnet.princeton.edu/perl/webwn?s=worm> (last visited Sept. 25, 2006).

89. AOL, Inc. v. CN Prods., Inc., 272 B.R. 879 (E.D. Va. 2002).

90. *In re Pharmatrak, Inc. Privacy Litig.*, 329 F.3d 9 (1st Cir. 2003).

91. *EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58, 60 (1st Cir. 2003).

92. See, e.g., Mac Zealots: Complete Mac Security, Part 3, <http://maczealots.com/tutorials/security/3/> (last visited Sept. 25, 2006) (describing the “Secure Empty Trash” feature of Mac OS X, which provides secure deletion functionality).

93. Apple: Mac OS X, <http://www.apple.com/macosx/> (last visited Sept. 25, 2006); Mac Zealots: Complete Mac Security, Part 3, <http://maczealots.com/tutorials/security/3/> (last visited Sept. 25, 2006).

94. See Shred – Linux Command – Unix Command, http://linux.about.com/library/cmd/blcmd11_shred.htm (last visited Sept. 25, 2006).

95. For example, Eraser is such a tool. Online Privacy and Email Server Manufacturers – Heidi Computers Limited, <http://www.heidi.ie> (last visited Sept. 25, 2006).

bility, and which is used by default even on those operating systems that do, is fundamentally inadequate as a means of protecting a user's privacy. When it is used to delete a file, the default delete functionality of Windows and most other operating systems simply removes the reference to the file that allows the operating system to locate it.⁹⁶ The operating system then treats the disk space containing the file's data as free space, which means that it will eventually be overwritten with new data as the need for the space arises.⁹⁷ Depending on the amount of unallocated space available elsewhere on the disk and the computer's degree of use, a substantial amount of time could pass before this occurs.⁹⁸ For that entire time, other commercially available software can be used to "undelete" the data and recover it.⁹⁹

Any computer user can testify that one of the reasons for deleting data is to make sensitive information unavailable to others. It is therefore not surprising that other software is readily available to address the shortcomings inherent in most operating systems' default deletion functionality. Nor is it surprising that some companies have incorporated the feature into the native functionality of the operating systems they produce, given that secure deletion software is so widely sought by users.¹⁰⁰ Although no data is available regarding the degree and frequency with which software providing secure deletion functionality is used, it is reasonable to infer that it is used frequently.¹⁰¹ Thus, the category of software characterized by the Seventh Circuit as being comprised of "destructive program[s]" is used by a substantial, perhaps even growing, segment of the population.¹⁰²

IV. COURT'S DECISION

In *International Airport Centers*, the Seventh Circuit's opinion fo-

96. See Wikipedia, File Wiping, http://en.wikipedia.org/wiki/Secure_file_deletion (last visited Sept. 25, 2006) [hereinafter File Wiping]; CNet, How to Remove Personal Files Before you Ditch your Old PC, <http://www.cnet.com.au/desktops/pcs/0,39029439,40062001,00.htm> (last visited Sept. 25, 2006) [hereinafter Remove Files]; How To: Data Recovery, <http://www.tech-pro.net/how-to-data-recovery.html> (last visited Sept. 25, 2006) [hereinafter Data Recovery].

97. See File Wiping, *supra* note 96.

98. See *id.*; Data Recovery, *supra* note 96.

99. See File Wiping, *supra* note 96; See Remove Files, *supra* note 96; Data Recovery, *supra* note 96.

100. See You Can't Empty the Trash or Move a file to the Trash in Mac OS X, <http://docs.info.apple.com/article.html?artnum=106272> (last visited Sept. 25, 2006) ("In Mac OS X 10.3 Panther or later, you can securely delete items by choosing Secure Empty Trash from the Finder menu."); Wikipedia, Shredding, <http://en.wikipedia.org/wiki/Shred#Computers> (last visited Sept. 25, 2006) ("[S]ome versions of [Mac OS] offer a 'secure delete' command, such as the 'Secure Empty Trash' command.").

101. The rationale for this inference is obvious. Secure deletion functionality has been incorporated into the default functionality of Mac OS X. Furthermore, multiple third-party tools offering this functionality are commercially available. Free tools offering the same functionality are also available. It may be inferred that the authors of these applications produced them after recognizing a real demand for this functionality.

102. *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006).

cused on defining transmission. Early in its discussion of this element, the court appeared willing to view pressing a key on a computer's keyboard as a transmission.¹⁰³ The court acknowledged, however, that this "might be stretching the statute too far."¹⁰⁴

The opinion soon revealed how far the court was willing to "stretch[] the statute."¹⁰⁵ The lower court's decision examined the means by which software was delivered to the target machine to determine whether the required element of transmission was satisfied.¹⁰⁶ Conversely, the Seventh Circuit disposed of the issue immediately by announcing that it did not know how Citrin installed the software he used, and that it did not care because it "[didn't] see what difference [it could] make."¹⁰⁷ The court then explained that the software's installation method was immaterial to the element of transmission.¹⁰⁸ What really mattered, according to the court, was whether the program passed over a wire:

[W]e don't see what difference the precise mode of transmission can make. . . . The only difference [between downloading from the internet and installation from a disk] is that the disk is inserted manually before the program on it is transmitted electronically to the computer. The difference vanishes if the disk drive into which the disk is inserted is an external drive, connected to the computer by a wire, just as the computer is connected to the Internet by a telephone cable or a broadband cable or wirelessly.¹⁰⁹

Therefore, if at some point the object of transmission passed over a wire on its way to the computer, then the element of transmission is satisfied for purposes of the CFAA.¹¹⁰ The element is satisfied even if the wire over which the program passes is the cable connecting an external storage device to the computer.¹¹¹

The Seventh Circuit's treatment of the element of transmission is consistent with the position proposed by IAC, but not that of the district court below. The district court's reading of *North Texas Preventive Imaging* and *Shaw* led it to conclude that those courts "recognized that 'transmission' includes the element of a shipment or delivery of a code or program."¹¹² IAC, however, argued that the correct reading of these

103. *Id.* at 419.

104. *Id.*

105. *Id.*

106. *Int'l Airport Ctrs., L.L.C. v. Citrin*, No. 03-8104, 2005 U.S. Dist. LEXIS 3905, at *7 (N.D. Ill. Jan. 31, 2005).

107. *Int'l Airport Ctrs., L.L.C.*, 440 F.3d at 419.

108. *Id.*

109. *Id.* at 419-20.

110. *Id.*

111. If transmission occurs when data passes over the cable connecting an external drive to a computer, it is reasonable to infer that a transmission will also occur when data passes over the cable connecting an external storage device, such as an external hard drive or a flash drive attached by a dongle. *See id.*

112. *Int'l Airport Ctrs., L.L.C. v. Citrin*, No. 03-8104, 2005 U.S. Dist. LEXIS 3905, at *7 (N.D. Ill. Jan. 31, 2005).

cases was not that shipment and delivery are essential components of a transmission, but that “shipment and delivery” is simply one of the multiple ways the element of transmission may be satisfied.¹¹³ Therefore, a shipment or delivery may constitute a transmission, but not every transmission necessarily includes a shipment or delivery.¹¹⁴ Similarly, the Seventh Circuit found a transmission even in the absence of a shipment or delivery.¹¹⁵

The Seventh Circuit and both parties supported their positions with references to congressional intent. Section 1030(a)(5)(A)(ii) extends liability under the CFAA to any individual who “intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage.”¹¹⁶ The Seventh Circuit saw this as evidence of Congress’s intent to extend the reach of the act to cover “disgruntled programmers.”¹¹⁷ Arguing the same point, IAC relied on Senate Report excerpts explaining that the scope of the CFAA extends to malicious insiders like Citrin.¹¹⁸ Attempting to counter IAC and put himself beyond the scope of the CFAA, Citrin responded that the purpose of the statute was to combat computer viruses and other malicious software, not to prosecute disloyal employees.¹¹⁹ Furthermore, Citrin argued that his use of specialized software to delete files was fundamentally indistinguishable from using a computer’s delete key, and that such a commonplace act did not violate the CFAA.¹²⁰

Although IAC did not raise the issue, the court also found that Citrin violated § 1030(a)(5)(A)(ii) because he “intentionally accesse[d] a protected computer without authorization, and as a result of such conduct, recklessly cause[d] damage.”¹²¹ According to the court, Citrin’s authorization to use the laptop computer in his possession ceased as soon as he developed interests adverse to those of his employer.¹²² Consequently, his access to the hardware in his possession was “without authorization.”¹²³

The court acknowledged that “the [CFAA] distinguishes between ‘without authorization’ and ‘exceeding authorized access,’” and that the latter might seem a more apt description of Citrin’s actions.¹²⁴ It maintained, however, that because Citrin’s authority to use the laptop in

113. See Brief of Appellant, *supra* note 6, at 12-13.

114. See *id.*

115. *Int’l Airport Ctrs., L.L.C.*, 440 F.3d at 419.

116. 18 U.S.C. § 1030(a)(5)(A)(ii) (Supp. IV 2004).

117. *Int’l Airport Ctrs., L.L.C.*, 440 F.3d at 420.

118. Brief of Appellant, *supra* note 6, at 15.

119. See Brief of Appellee, *supra* note 8, at 17.

120. *Id.* at 18.

121. *Int’l Airport Ctrs., L.L.C.*, 440 F.3d at 420.

122. *Id.*

123. *Id.*

124. *Id.*

question was suspended when he developed the intent to compete with his former employer, his actions should be considered to be “without authorization” rather than “exceeding authorized access.”¹²⁵ Therefore, the court concluded, Citrin was properly liable under § 1030(a)(5)(A)(ii).

In closing, the court addressed a contract-based defense Citrin raised: his employment contract authorized him to destroy data on the laptop before returning it to his employer after his employment ceased.¹²⁶ Citrin argued that his contract therefore authorized his destruction of the data on the laptop.¹²⁷ The court found Citrin’s argument unconvincing, as it did not think that the intent of the clause Citrin relied upon was to allow him to destroy data that IAC would want and of which it did not have duplicates.¹²⁸

V. COMMENTARY

In *International Airport Centers, L.L.C. v. Citrin*, the Seventh Circuit held that the transmission element of § 1030(a)(5)(A)(i) was satisfied by the installation of software from a floppy disk onto a computer without requiring any movement or shipment of the software.¹²⁹ The Seventh Circuit’s opinion deserves a close examination for several reasons. First, the decision ignores the well-reasoned trend established by other courts that have construed the element of transmission. Second, the court could have reversed the district court without construing the element of transmission so broadly. Third, the court’s decision created precedent that unreasonably extends the scope of the CFAA beyond what it likely anticipated. Finally, the court construed the element of transmission so broadly that whenever a defendant installs software or copies code to a computer, the element of transmission is satisfied.

A. *The Court’s Disregard for Persuasive Authority*

As the district court noted, there are few cases construing the element of transmission, and none of these are binding authority in the Seventh Circuit.¹³⁰ In spite of this, *International Airport Centers* seems inconsistent with the emerging trend.

Prior to *International Airport Centers*, courts construing the element of transmission held that in the absence of an electronic conveyance of data, transmission for purposes of § 1030(a)(5)(A)(i) required

125. *Id.* at 421.

126. *Id.*

127. *Id.*

128. *Id.*

129. See discussion *supra* Part IV.

130. *Int’l Airport Ctrs., L.L.C. v. Citrin*, No. 03-8104, 2005 U.S. Dist. LEXIS 3905, at *5-6 (N.D. Ill. Jan. 31, 2005).

shipment or travel.¹³¹ In *Gomar*, the court found that a transmission occurred when code that had been developed to be recklessly or intentionally harmful was physically shipped on a disk.¹³² Similarly, in *Shaw*, the court found that a transmission occurred because hardware containing harmful code was shipped and delivered to consumers throughout the country.¹³³ Finally, in *North Texas Preventive Imaging*, a transmission occurred because the defendant shipped software containing malicious code to a third party consumer.¹³⁴

These cases are not binding authority in the Seventh Circuit, and their facts and those of *International Airport Centers* are dissimilar. Nonetheless, these cases do reflect that the Seventh Circuit's opinion deviated from the established trend in construction of the element of transmission. The opinions in *North Texas Preventive Imaging*, *Gomar*, and *Shaw* are consistent with basic rules of statutory interpretation concerning the plain meaning of statutory language.¹³⁵ Specifically, when interpreting a statute, "‘fidelity to the plain meaning of the text is not boundless.’ However, departure from the plain meaning of the text is not casually undertaken. If [a court] ‘finds [a statute] unambiguous, judicial inquiry is complete, except in rare and exceptional circumstances.’"¹³⁶ The *North Texas Preventive Imaging*, *Gomar*, and *Shaw* courts construed the element of transmission broadly but did not depart from the plain meaning of the word, which implies a movement of the code, program, or command from one place to another.¹³⁷ The Seventh Circuit's construction of the element of transmission violated that rule.¹³⁸

The court justified its broad construction of the element of transmission as being consistent with Congress's intent that the CFAA reach

131. See discussion *supra* Part III.E.

132. See *Shaw v. Toshiba Am. Info. Sys., Inc.*, 91 F. Supp. 2d 926, 935 (examining the holding of *Gomar*, C.A. No. 96-4000 (D.N.J. Jan. 28, 1998), which explains that transmission includes loading destructive code onto a manufacturing machine, then shipping that machine). *Id.* at 936 (explaining that transmission includes shipment of computer hardware containing destructive code); *N. Tex. Preventive Imaging v. Eisenberg*, No. SA CV 96-71 AHS, 1996 U.S. Dist. LEXIS 19990, at *16 (C.D. Cal. Aug. 19, 1996) (explaining that transmission includes loading destructive code onto a floppy disk, then shipping that disk).

133. *Shaw*, 91 F. Supp. 2d at 936.

134. *N. Tex. Preventive Imaging*, 1996 U.S. Dist. LEXIS 19990, at *16.

135. See discussion *supra* Part III.E.

136. *Shaw*, 91 F. Supp. 2d at 931 (internal citations omitted) (quoting Toshiba's Motion for Summary Judgment at 14, *Shaw*, 91 F. Supp. 2d 926, (No. 1:99-CV-0120) and *Garcia v. U.S.*, 469 U.S. 70, 75 (1978) respectively).

137. The root verb of "transmission," transmit, is defined in relevant part as "to transfer from one person or place to another . . . to cause or allow to spread abroad . . . to cause . . . to pass through space or a medium." THE MERRIAM-WEBSTER DICTIONARY 769 (1994).

138. The Seventh Circuit held that the element of transmission was satisfied by the passage of software from the floppy disk drive (presumably a CD-ROM, as few companies now distribute software on 3.5" floppies and few late-model laptops even have 3.5" disk drives) of Citrin's laptop to the computer's more central components. *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 419-20 (7th Cir. 2006). In the Seventh Circuit's analysis from *International Airport Centers*, a transmission thus occurred when the code traveled no more than a few inches.

all types of computer criminals, regardless of whether they launch their attacks from inside or outside of a victim's organization.¹³⁹ Congressional intent, however, was fulfilled by applying the plain language of the statute.¹⁴⁰ This is demonstrated by the court's own opinion, in which it found that Citrin's conduct fit within the scope of § 1030(A)(5)(a)(ii) as expressed by the plain language of that subsection.¹⁴¹ The court could have brought Citrin within the scope of the CFAA's plain language and thereby fulfilled congressional intent without delving into § 1030(A)(5)(a)(i) and the accompanying discussion of transmission.

B. *Gratuitous Construction*

There seems to be a congressional mandate that courts interpret the CFAA broadly. In meetings of the Subcommittee on Technology and the Law of the Committee on the Judiciary, the committee chair, Senator Patrick Leahy, acknowledged that the CFAA regulated an area that is always changing because of rapidly evolving technology.¹⁴² Within a very short time, he said, the courts might face problems and cases that arise within the statute's subject matter but are not obviously within the scope of its plain language: "You know, this is an area that changes all the time. Answers we have today may well be different a year or so from now. The questions, I am sure, will be different."¹⁴³ Senator Leahy concluded by explaining that the CFAA should be construed broadly to accommodate new varieties of computer-related crime, and to compensate for Congress's inability to predict them.¹⁴⁴

There is also evidence that when the legislature crafted the CFAA, it intended the statute to occupy the field of computer crime. For example, the 1994 and 1996 amendments expanded the CFAA's scope from attackers outside of protected computer networks to include internal attackers, such as disgruntled employees who "exceed[] authorized access."¹⁴⁵ These amendments also expanded the scope of the statute

139. See *id.* at 420 (referring to Congress's intent that the CFAA reach the authors of worms and viruses, and other attacks that "come mainly from the outside," as well as internal attacks, such as those launched by "disgruntled programmers").

140. *Id.*

141. *Id.*

142. See, e.g., *The Impact of Computer Viruses and Other Forms of Computer Sabotage or Exploitation on Computer Information Systems and Networks: Hearing Before the Subcomm. on Technology and the Law of the Comm. on the Judiciary*, 101st Cong. 12 (1989) (statement of Sen. Patrick Leahy, Chairman, S. Comm. on the Judiciary).

143. *Id.*

144. *Id.* at 34.

On the day that we pass a law, we are, in effect, taking a snapshot of what we know that day. But however we draw it, somebody is going to sit down and say, well, look, I am just going to create a variation not covered by the statute. I am not sure all of us, putting our best minds together, could come up with every variation on a law that might get enacted some time this year to cover some new variation next year.

Id. at 34.

145. 18 U.S.C. § 1030(a)(2) (Supp. II 1996).

from protecting only Federal interest computers to the more comprehensive “protected computer.”¹⁴⁶ Courts have interpreted this and similar language as tacit congressional approval to broadly construe the CFAA.¹⁴⁷

The Seventh Circuit reasoned that its broad construction of the element of transmission was consistent with congressional intent.¹⁴⁸ The court’s own opinion, however, suggests that its interpretation of the element of transmission was extraneous.¹⁴⁹ As the court noted, Citrin’s conduct also violated other sections of the CFAA.¹⁵⁰ Therefore, federal jurisdiction could have been justified, and the Seventh Circuit could have reversed the decision of the lower court, without the extraneous flourish regarding the meaning and scope of transmission.¹⁵¹

C. Future Repercussions

The Seventh Circuit’s application of § 1030(a)(5)(A)(i) to secure deletion software sets a precedent that may criminalize the actions of a large group of otherwise innocent computer users. Applying the logic of the Seventh Circuit, a user who installed Macintosh OS X on a computer and used its native functionality could face prosecution under § 1030(a)(5)(A)(i).¹⁵² The installation of the operating system would satisfy the element of transmission, and the use of its secure deletion functionality to remove data would satisfy the element of damage.¹⁵³ Damage for the purposes of § 1030(a)(5)(A)(i) must be caused intentionally, but the statute’s mens rea requirement would be satisfied so long as the user employed the secure deletion software purposefully, which would be true in almost all situations.¹⁵⁴

For all users of secure deletion software, *International Airport Centers* is a potential recipe for a 10-year prison term. The only ingre-

146. 18 U.S.C. § 1030(a)(5)(A) (Supp. IV 2004). Protected computers include government-operated or affiliated machines, financial institution computers, and computers used in interstate commerce or communications. *Id.*

147. See discussion *supra* Part III.E.

148. See discussion *supra* Part IV.

149. See *Int’l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006) (finding that Citrin violated two sections of the CFAA, either of which would have permitted the Seventh Circuit to reverse the decision of the district court).

150. *Id.*

151. The District Court for the Northern District of Illinois dismissed IAC’s claims due to a lack of subject matter jurisdiction. *Int’l Airport Ctrs., L.L.C. v. Citrin*, No. 03-8104, 2005 U.S. Dist. LEXIS 3905, at *9 (N.D. Ill. Jan. 31, 2005). The Seventh Circuit’s finding that Citrin violated § 1030(a)(5)(A)(ii) provided grounds for reversal.

152. The appellant’s brief demonstrates its ignorance of this fact. The brief argues that this situation—opening the door to liability for people who use functionality inherently present on their computers—will specifically not happen. Brief of Appellant, *supra* note 6, at 9-10.

153. 18 U.S.C. § 1030(e)(8) (Supp. IV 2004). (“[T]he term ‘damage’ means any impairment to the integrity or availability of data, a program, a system, or information . . .”).

154. *Id.* § 1030(a)(5)(A)(i) (“*knowingly* causes the transmission of a program, information, code, or command, and as a result of such conduct, *intentionally* causes damage without authorization, to a protected computer”) (emphasis added).

dient missing is a party willing to bring suit. The ramifications of the court's decision are especially ironic given that the Seventh Circuit acknowledged the need for a relatively high degree of care, as the CFAA provides not only civil, but criminal penalties.¹⁵⁵ One can only assume that the Seventh Circuit did not intend these consequences, but rather that they are the result of the court's unfamiliarity with the relevant technology. Evidence of such inexperience permeates the appellant's entire brief, and the court presumably adopted this faulty understanding.¹⁵⁶ After all, one of the judges said during oral argument "[d]estroying a person's data—that's as bad as you can do to a computer."¹⁵⁷ Language in Judge Posner's opinion also suggests a fundamental lack of understanding on the part of the court regarding the technology at issue. For example, the court refers to the secure deletion tool Citrin used as a "destructive program," and at no point in the opinion does the court acknowledge that the software Citrin used is a legitimate tool with a useful purpose.¹⁵⁸

It is also possible that the Seventh Circuit is not so inexperienced as *International Airport Centers* may suggest. *International Airport Centers* may instead be a results-oriented opinion, and its drastic expansion of the CFAA's scope may be precisely the effect the court intended.¹⁵⁹ The use of such tactics by results-oriented judges is not, after all, unprecedented.¹⁶⁰

D. Rendering Transmission Superfluous by Broad Construction

A fundamental rule of statutory construction is that a court should

155. *Int'l Airport Ctrs., L.L.C.*, 440 F.3d at 419 ("Pressing a delete or erase key . . . transmits a command, but it might be stretching the statute too far (especially since it provides criminal as well as civil sanctions for its violation) to consider any typing . . . to be a form of 'transmission' just because it transmits a command . . .").

156. Brief of Appellant, *supra* note 6, at 10 (arguing that Citrin's use of secure deletion software is not the equivalent of using an operating system's native deletion functionality).

157. CNet, Police Blotter: Ex-Employee Faces Suit Over File Deletion, http://news.com.com/Police+blotter+Ex-employee+faces+suit+over+file+deletion/2100-1030_3-6048449.html (last visited Sept. 25, 2006).

158. *Int'l Airport Ctrs., L.L.C.*, 440 F.3d at 420.

159. The discussion of congressional intent that immediately follows the court's broad construction of transmission suggests that this may be the case. The court broadly construed transmission, and then proceeded to explain its belief that this sort of broad construction is appropriate for the CFAA. *See id.* (explaining that "if the [CFAA] is to reach the disgruntled programmer, which Congress intended . . . it can't make any difference that the destructive program comes on a physical medium, such as a floppy disk or CD").

160. An example is the recent case of *People v. Hill*, 715 N.W.2d 301 (Mich. Ct. App. 2006). In *Hill*, the defendant, Bryan Hill, obtained child pornography from the Internet and created CD-ROM disks containing copies of the same pornographic images. *Id.* at 304-05. Applying the relevant statute, the court found that Hill could be charged with not only the lesser crime of possessing child pornography, which carried a maximum penalty of four years imprisonment, but also the crime of *producing* child pornography. *Id.* at 307. The decision is noteworthy because the statutory language under which Hill was convicted had been previously understood to refer to offenders who actually engaged in the filming, photographing, or facilitating of pornographic acts involving minors. *See, e.g., People v. Riggs*, 604 N.W.2d 68, 69 (Mich. Ct. App. 1999).

not construe a part of a statute or interpret it in such a way that one of the elements of the statute becomes superfluous.¹⁶¹ Doing so effectively excises the construed element from the statute and is an exercise of authority that should be reserved for the legislature.¹⁶² Yet, this was the result of the Seventh Circuit's construction of the element of transmission. According to the court, transmission encompasses both installation of a program when a "disk is inserted manually" and also by transmission over a network, as via an "Internet download."¹⁶³ The opinion further states that "the only difference [between these modes of transmission] is that the disk is inserted manually before the program on it is transmitted electronically to the computer."¹⁶⁴ A reasonable reading of this language is that a transmission can occur even within the computer itself. For instance, when the contents of a floppy disk, CD-ROM, or other media are transferred between the disk drive and the computer's motherboard to which they are attached, a transmission occurs according to the Seventh Circuit.

The Seventh Circuit's definition of transmission appears to cover almost every method by which data is typically transferred to a computer. As the Seventh Circuit found, the element of transmission is fulfilled when a party installs software onto a computer from a form of removable storage, such as a floppy disk or CD-ROM, as Citrin did.¹⁶⁵ The court's opinion also made it clear that a transmission will occur when code or commands are transmitted to a computer from the Internet via a wired or wireless connection.¹⁶⁶ If a party successfully conveys data to a computer from some source other than a mouse and keyboard, the element of transmission will be satisfied.

Transmission is not the only element required by § 1030(a)(5)(A)(i), so the Seventh Circuit's opinion will not provide plaintiffs and prosecutors with a way to ensure a conviction or fix liability every time § 1030(a)(5)(A)(i) is applied.¹⁶⁷ It will, however, give plaintiffs and prosecutors an advantage when litigating § 1030(a)(5)(A)(i), as the transmission element will be irrefutably satisfied in almost all cases. Defendants will find that fighting a lawsuit or charges brought against them under § 1030(a)(5)(A)(i) is more difficult because there will be

161. See *State v. Sedillos*, 112 P.3d 854, 859 (Kan. 2005); *San Antonio v. Marin*, 19 S.W.3d 438, 441 (Tex. App. 2000).

162. Compare U.S. CONST. art. I, § 8, cl.1, 18 ("The Congress shall have power . . . [t]o make all Laws . . . necessary and proper for carrying into Execution the foregoing Powers, and all other Powers vested by this Constitution in the Government of the United States, or in any Department or Officer thereof."), with U.S. CONST. art. III (enumerating the jurisdiction and powers of the judiciary branch of the United States government, which do not include the power to make or modify laws).

163. *Int'l Airport Ctrs., L.L.C.*, 440 F.3d at 419.

164. *Id.*

165. *Id.* at 419-20.

166. *Id.*

167. 18 U.S.C. § 1030(a)(5)(A)(i) (Supp IV 2004) (elements include not only transmission, but also intentional damage).

one less element that the plaintiff or prosecution must prove. The CFAA may be used to impose both civil and criminal penalties, with a maximum sentence of ten years for first time offenders.¹⁶⁸ The Seventh Circuit should not unilaterally place the defendants to whom the CFAA is applied at such a disadvantage.

VI. CONCLUSION

In *International Airport Centers*, the United States Court of Appeals for the Seventh Circuit disregarded all persuasive authority construing the element of transmission in 18 U.S.C. § 1030(a)(5)(A)(i), and crafted its own definition from the ground up. Judicial construction and congressional intent indicate that the CFAA as a whole is to be construed broadly; in *International Airport Centers*, however, the court construed the element of transmission so broadly that it will always be met when data is transmitted to a computer by any means other than a keyboard or mouse. The Seventh Circuit thus effectively excised the element from the statute, placing CFAA defendants at a disadvantage.

Another consequence of the court's decision will be to extend liability under the CFAA to a new class of actors. Using the new definition of transmission set forth by the Seventh Circuit, the simple act of installing an operating system and using its default functionality may create civil liability and impose a criminal penalty of up to ten years imprisonment. The decision resulted from the court's lack of understanding of the relevant technology involved in the case.

Ultimately, the Seventh Circuit's decision in *International Airport Centers* is puzzling. To a certain extent, the court's error may be the result of its understandably imperfect and ad hoc understanding of technical subject matter—the result of a legal professional trying to squeeze into the shoes of an IT professional. Other parts of the opinion, however, are not so easily understood. The court exercised power that plainly was not within its authority, and did so without any apparent explanation. Nonetheless, the decision is now binding authority in the Seventh Circuit. One can only hope that the decision's application is limited until it is eventually overturned.

168. *Id.* § 1030(c)(4)(A).