Notre Dame Law Review

Volume 94 | Issue 4 Article 10

6-2019

No Internet Does Not Mean No Protection Under the CFAA: Why Voting Machines Should Be Covered Under 18 U.S.C. § 1030

Jack Dahm
Notre Dame Law School

NOTES

NO INTERNET DOES NOT MEAN NO PROTECTION UNDER THE CFAA: WHY VOTING MACHINES SHOULD BE COVERED UNDER 18 U.S.C. § 1030

*Jack Dahm**

[T]hese [cyberattacks] are persistent, they are pervasive, and they are meant to undermine America's democracy on a daily basis, regardless of whether it is election time or not. Russian actors and others are exploring vulnerabilities in our critical infrastructure as well. . . . The warning signs are there, the system is blinking, and that is why I believe we are at a critical point.

—Dan Coats, Director of U.S. National Intelligence, July 13, 2018[1]

Introduction

The threat of cyberattacks to America's networks is ever increasing.[2] Dan Coats, the Director of U.S. National Intelligence, addressed this prob-

* Candidate for Juris Doctor, Notre Dame Law School, 2020; Bachelor of Science in Business, Miami University, 2015; Bachelor of Arts in English, Miami University, 2015. I would like to thank Professor Patricia Bellia for her guidance throughout the Note writing process. I would also like to thank the staff of the *Notre Dame Law Review* for their careful editing. Finally, a special thanks to Lainie Lynch, who is my greatest supporter in everything I do. All errors are my own.

1 Dan Coats, Dir. of Nat'l Intelligence, Address at Hudson Institute (July 13, 2018) [hereinafter Dan Coats Address]. For a transcript of the address, see *Transcript: Dan Coats Warns the Lights Are 'Blinking Red' on Russian Cyberattacks*, NPR (July 18, 2018), https://www.npr.org/2018/07/18/630164914/transcript-dan-coats-warns-of-continuing-russian-cyberattacks.

2 *See* Dan Coats Address, *supra* note 1; *see also* Grant Schneider, *President Trump Unveils America's First Cybersecurity Strategy in 15 Years*, White House (Sept. 20, 2018), https://www.whitehouse.gov/articles/president-trump-unveils-americas-first-cybersecurity-strategy-15-years/ (describing the "growing threats" by criminals, terrorists, and foreign adversaries to America's networks).

lem in a speech before the Hudson Institute[3] on July 13, 2018.[4] Coats recalled the months before September 2001, when then-current CIA Director George Tenet said, "the system was blinking red."[5] Coats then alerted the Hudson Institute, "I'm here to say the warning lights are blinking red again. Today, the digital infrastructure that serves this country is literally under attack."[6] Coats identified Russia as being "the most aggressive foreign actor—no question."[7] Russia has become a global force in cyber warfare.[8] So far, the biggest target of their attacks has been the 2016 U.S. election.[9]

Largely in response to Russia's cyberattacks and continued cyberthreats, the U.S. Attorney General established a Cyber-Digital Task Force within the Department of Justice (DOJ) in February 2018.[10] This newly created task force released its first public report on July 19, 2018.[11] Then–Attorney General Jeff Sessions announced the release of the report, while promising that "[a]t the Department of Justice, we take these threats seriously."[12] The report was designed to answer the following question: "How is the Department [of Justice] responding to cyber threats?"[13] The report begins by discussing the threat of foreign influence operations, described by the Task Force as "one of the most pressing cyber-enabled threats our Nation faces."[14] Specifically, the Task Force focuses on the dangerous threat of Russia to U.S. elections.[15]

---

3 A think tank and research center dedicated to nonpartisan analysis of U.S. and international economic, security, and political issues. *See generally* HUDSON INSTITUTE, https://www.hudson.org/about (last visited Feb. 22, 2019).

4 Dan Coats Address, *supra* note 1.

5 *Id.* (referring to intelligence communications identifying alarming activities that suggested a potential attack before 9/11).

6 *Id.*

7 *Id.*

8 Sophie Perryer, *A History of Russian Hacking*, NEW ECON. (Oct. 22, 2018), https://www.theneweconomy.com/technology/a-history-of-russian-hacking.

9 *Id.* (describing Russia's attempts to alter the outcome of the 2016 U.S. election through cyber hacking as "their biggest task yet"). Russia's cyber interference during the election included "systematic distribution of 'fake news' on social media sites, alleged financial contributions to Trump's campaign, and—the centerpiece of their interference—a phishing attack on Hillary Clinton's campaign." *Id.*

10 U.S. DEP'T OF JUSTICE, REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE (2018), https://www.justice.gov/ag/page/file/1076696/download [hereinafter DOJ CYBER DIGITAL REPORT].

11 Press Release, U.S. Dep't of Justice, Attorney General Sessions Announces Publication of Cyber-Digital Task Force Report (July 19, 2018), https://www.justice.gov/opa/pr/attorney-general-sessions-announces-publication-cyber-digital-task-force-report.

12 *Id.*

13 DOJ CYBER DIGITAL REPORT, *supra* note 10, at xi. This is one of the two foundational questions that were given to the Task Force by the Attorney General. The other question is: "And how can federal law enforcement more effectively accomplish its mission in this important and rapidly evolving area?" *Id.*

14 *Id.* This section makes up the first chapter of the report. *See id.* at 1–21.

15 *Id.* at 2. The report calls out Russia's "longstanding desire to undermine the U.S.-led liberal democratic order." *Id.* (quoting OFFICE OF THE DIR. OF NAT'L INTELLIGENCE,

After detailing the scope of this and other threats, the Task Force outlines the key prosecutorial tools available to the DOJ in combating cyberattacks.[16] The first tool, which this Note will discuss at length, is the Computer Fraud and Abuse Act (CFAA), codified at 18 U.S.C. § 1030.[17] The CFAA falls at the top of the Task Force's list because, as it mentions, "[the CFAA] remains the . . . principal tool for prosecuting computer crimes."[18] Many other scholars have described the CFAA as the cornerstone of computer fraud litigation.[19] The Task Force provides a simple definition of the CFAA, explaining how it "gives the owners of computers the right to control who may access their computers, take information from them, change how the computers work, or delete information on them."[20]

Later in the report, after emphasizing Russian interference with elections as the principal cyberthreat and the CFAA as the principal prosecution tool, the Task Force asserts that "[the CFAA] currently does not prohibit the act of hacking a voting machine in many common situations."[21] The Task Force plainly states that "the CFAA only prohibits hacking computers that are connected to the Internet (or that meet other narrow criteria for protection)."[22] However, the text of the CFAA does not explicitly require that hacked computers be connected to the internet, nor have the courts interpreted this as a requirement of the CFAA.[23] Though most of Russia's known cyberthreats have not been aimed directly at the voting machine devices themselves, the Task Force's assertion still raises a big question: Does the CFAA only apply to internet-connected devices?

This Note seeks to answer that question, ultimately concluding that internet connection is not required for a computer to reach protected status under the CFAA. Part I of this Note describes the background of the CFAA, specifically detailing the types of crime it was meant to punish, its definition of "computer," and its definition of "protected computer" (which builds on the definition of "computer" by providing the jurisdictional hook). Part II moves away from the Act's legislative history and discusses how courts have interpreted the CFAA over time. Part III applies the CFAA to the hacking of a voting machine (assumed to be without internet). Here, a voting machine is used as the vehicle for the analysis but much of the reasoning could apply

---

BACKGROUND TO "ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT U.S. ELECTIONS": THE ANALYTIC PROCESS AND CYBER INCIDENT ATTRIBUTION 1 (2017)).

16 *Id.* at 62.

17 *Id.*

18 *Id.*

19 *See, e.g.*, Shawn E. Tuma, "*What Does CFAA Mean and Why Should I Care?"–A Primer on the Computer Fraud and Abuse Act for Civil Litigators*, 63 S.C. L. REV. 141, 154 (2011) ("Practically speaking, the Computer Fraud and Abuse Act is the king of all computer fraud laws.").

20 DOJ CYBER DIGITAL REPORT, *supra* note 10, at 62.

21 *Id.* at 121.

22 *Id.*

23 *See* Orin Kerr (@OrinKerr), TWITTER (Aug. 29, 2018, 12:36 AM), https://twitter.com/OrinKerr/status/1034706398.

to other non-internet-connected devices. Part III argues that the hacking of a voting machine is certainly within the current-day scope of crimes meant to be punished by the CFAA, that voting machines fall within the Act's definition of "computer," and that voting machines probably fall within the definition of "protected computer." From there, the Conclusion explains why an amendment to expressly add voting machines to the definition of the CFAA would not be the best solution (especially since they are likely already protected). The Conclusion then analyzes the risks of the continuing expansion of the CFAA's scope and addresses the relative potential of Russia's cyberthreats to voting machines compared to their other election-related cyberthreats.

I. BACKGROUND ON THE CFAA

The CFAA is only thirty-two years old, having been passed in 1986 as an amendment to the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984.[24] The legislative history of the CFAA shows that Congress wanted "to provide a clear statement of proscribed activity . . . to the law enforcement community, those who own and operate computers and those tempted to commit crimes by unauthorized access."[25] Since 1986, Congress has amended the CFAA eight more times.[26] Each of these several amendments has "widened the depth and breadth of the Act by adding substantive offenses, lowering levels of scienter, or increasing penalties."[27] Congress will assuredly continue to amend the CFAA given the rapid increase in technology development. Because there have been so many changes to the CFAA, this Part does not offer a comprehensive review of all of the amendments, but it will highlight a few of the important changes and present the law as it stands today.

A. The Substantive Crime: 18 U.S.C. § 1030(a)

The CFAA is meant to prevent "fraud and related activity in connection with computers."[28] The requisite mens rea for the crime is "intentionally,"[29] thus the Act is meant to punish only the most culpable actors. The actual substance of the crime has evolved with time as Congress has continually

24 Tuma, *supra* note 19, at 155.

25 *Id.* (quoting S. REP. NO. 104-357, at 3 (1996)).

26 Matthew Kapitanyan, *Beyond* WarGames*: How the Computer Fraud and Abuse Act Should Be Interpreted in the Employment Context*, 7 I/S: J.L. & POL'Y FOR INFO. SOC'Y 405, 414 (2012). The five most substantial amendments include the Computer Fraud and Abuse Act of 1986, the Violent Crime Control and Law Enforcement Act of 1994, the Economic Espionage Act of 1996, the USA Patriot Act of 2001, and the Identity Theft Enforcement and Restitution Act of 2008. *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1564–71 (2010).

27 Kapitanyan, *supra* note 26, at 415 (citing Reid Skibell, Note, *Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act*, 18 BERKELEY TECH. L.J. 909, 911 (2003)).

28 Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030 (2012).

amended the Act and technology has substantially changed.[30] The amendment process started with the CFAA itself when it expanded the scope of the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, which was strictly designed to protect information, records, and computers used by the U.S. government.[31] The 1986 amendment did not remove the language of the original statute, but simply expanded its scope. Therefore, portions of the Act still reflect its original, more narrow intent from back in 1984.[32] Today, far beyond preventing only the hacking of computers belonging to the U.S. government, the Act prevents the hacking of "any protected computer,"[33] a definition that will be further discussed in Sections II.B and II.C.

While the Act has broadened to cover the hacking of more types of computers, it has remained fairly consistent in defining what it means to hack a computer (though the courts have interpreted this definition of hacking in different ways).[34] A hacking worthy of punishment under the CFAA involves a person who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information."[35] The key words from this definition, which have triggered much legal argument, are "without authorization or exceeds authorized access." Congress attempted to aid the courts in understanding these words by providing a definition of "exceeds authorized access," which reads: "[T]o access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[36] However, this definition is rather circular and does not provide additional context beyond the text of the phrase itself. On top of that, Congress has never defined "without authorization." Therefore, it has largely been up to the courts to answer the following questions: What does it mean to access a computer without authorization? What does it mean to exceed authorized access? The courts' answers to these questions bear important weight, as they directly influence the scope of the substantive crime.

It is worth briefly noting the varying degrees of punishment for offenses committed under the CFAA. Based on the severity of the offense, a criminal defendant might receive a fine under the title of the Act, a prison sentence

29 *Id.* Initially, the mens rea had been "knowingly." *See* Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, § 2, 100 Stat. 1213, 1213–16 (1986) (codified as amended at 18 U.S.C. § 1030 (2012)).

30 Patricia L. Bellia, *A Code-Based Approach to Unauthorized Access Under the Computer Fraud and Abuse Act*, 84 GEO. WASH. L. REV. 1442, 1442 (2016).

31 *Id.* at 1443.

32 For example, 18 U.S.C. § 1030(a)(1) specifically refers to hacking of information "that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations." 18 U.S.C. § 1030(a)(1) (2012).

33 *Id.* § 1030(a)(2)(C).

34 *See infra* Section II.A.

35 18 U.S.C. § 1030(a)(2).

36 *Id.* § 1030(e)(6).

ranging from not more than one year to not more than twenty years, or possibly both a fine and prison sentence.[37] The upward bound of twenty years in prison illustrates the gravity of potential offenses committed under the Act. The full punishment scheme is laid out in subsection (c) of the Act.[38] Initially, the CFAA was only a criminal statute, but Congress later expanded it to allow for recovery of civil damages as well.[39]

B. The Definition of "Computer": 18 U.S.C. § 1030(e)(1)

While the meaning of the phrase "without authorization or exceeds authorized access" greatly influences what actions are considered criminal under the Act, there can be no criminal action under the CFAA without the involvement of a computer. Again, this statute was conceived back in the 1980s, when computers were very different from what they are now. Aside from the enormous advancements with regard to the traditional computer, the breadth of computer-like devices has extraordinarily widened and continues to do so with time. Thus, determining "what is a computer," is not as easy as it might seem. Here is how Congress currently defines "computer" under the CFAA:

> [A]n electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.[40]

The wordiness of this definition reflects the difficulty of defining a current-day (and future-day) computer. Given the vast range of computer-like devices, Congress chose to offer examples of what a computer is not. The examples provide concrete clarification, as they allow lawyers and judges to materially distinguish between a "maybe computer" and the explicit "not computers" put forth by Congress.

But on the whole, the definition of "computer" is broad and unlikely to be at issue. In fact, the Seventh Circuit Committee on Federal Criminal Jury Instructions anticipated that "in most cases, it will be unnecessary to instruct the jury on the meaning of the term 'computer.'"[41] Legal scholars seem to agree. In a 2010 law review article, Professor Orin Kerr said that this broad construction allows for nearly every computer to be protected under the Act, to the point where a protected computer can include "coffeemakers, microwave ovens, watches, telephones, children's toys, MP3 players, refrigerators, heating and air-conditioning units, radios, alarm clocks, televisions, and DVD

37 *Id.* § 1030(c).

38 *See id.*

39 Tuma, *supra* note 19, at 155.

40 18 U.S.C. § 1030(e)(1).

41 PATTERN CRIMINAL JURY INSTRUCTIONS OF THE SEVENTH CIRCUIT 384 (COMM. ON FED. CRIMINAL JURY INSTRUCTION OF THE SEVENTH CIRCUIT 2012).

players, in addition to more traditional computers like laptops or desktop computers."[42] Because all of these devices contain microchips and electronic storage devices, they are likely to satisfy the definition.[43]

C. The Definition of "Protected Computer": 18 U.S.C. § 1030(e)(2)

Meeting the definition of "computer" does not end the analysis. With the passage of the Economic Espionage Act in 1996, Congress added the requirement that the computer also be "protected."[44] There are two categories of "protected computers." The first category includes computers involving a financial institution or the United States government.[45] Whether a computer is protected under this first category is fairly straightforward. The second category includes computers that are used in or affect interstate or foreign commerce or communication.[46] The section of the Act that gives effect to this second category of protected computers reads: "[U]sed in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States."[47]

Initially, the second category only covered computers *used in* interstate or foreign commerce, and not those *affecting* such commerce.[48] When Congress first added the "protected computer" category to the Act as part of the Economic Espionage Act in 1996, the Senate Judiciary Committee said, "[it] is intended to protect against the interstate or foreign theft of information by computer."[49] In 2008, Congress added the phrase "affecting interstate commerce" to align the CFAA's jurisdiction with the breadth of the Commerce Clause.[50] In other words, the phrase "affecting interstate commerce" is meant to invoke Congress's full sphere of power under the Commerce Clause of the Constitution. Essentially, the Constitution does not give Congress the right to regulate computers, but it does provide Congress with the ability to regulate interstate or foreign commerce.[51] In this scenario, by requiring that computers affect interstate or foreign commerce in order to

42 Kerr, *supra* note 26, at 1577–78.

43 *Id.*

44 Economic Espionage Act of 1996, § 201, Pub. L. No. 104-294, 110 Stat. 3488, 3491 (codified as amended at 18 U.S.C. § 1030)).

45 18 U.S.C. § 1030(e)(2)(A).

46 *Id.* § 1030(e)(2)(B).

47 *Id.*

48 Economic Espionage Act of 1996 § 201.

49 William A. Hall, Jr., *The Ninth Circuit's Deficient Examination of the Legislative History of the Computer Fraud and Abuse Act in* United States v. Nosal, 84 GEO. WASH. L. REV. 1523, 1539–40 (2016) (emphasis omitted) (citing S. REP. NO. 104-357, at 7 (1996)).

50 Tiffany Curtiss, Comment, *Computer Fraud and Abuse Act Enforcement: Cruel, Unusual, and Due for Reform*, 91 WASH. L. REV. 1813, 1818 (2016).

51 U.S. CONST. art. I, § 8, cl. 3. (stating that the United States Congress shall have power "[t]o regulate Commerce with foreign Nations, and among the several States, and with the Indian tribes").

be protected, Congress was able to use the commerce power to regulate this area of the law.

The Supreme Court greatly expanded the scope of "affecting commerce" when it decided *Wickard v. Filburn* in 1942.[52] This case involved a statute passed by Congress under the commerce power, which limited wheat production for farmers based on their total farm acreage.[53] Ohio farmer Roscoe Filburn harvested 239 wheat bushels in excess of his limit under the statute, though he intended to use the extra wheat for home consumption.[54] Having exceeded his quota, Filburn sought to enjoin enforcement of the marketing penalty that he faced under the statute.[55] Filburn argued that Congress's regulation of wheat production for home consumption exceeded the scope of its power under the Commerce Clause.[56] But ultimately, Justice Jackson said that an activity may "be reached by Congress if it exerts a substantial economic effect on interstate commerce, and this irrespective of whether such effect is what might at some earlier time have been defined as 'direct' or 'indirect.'"[57]

More recently, and largely relying on the reasoning from *Wickard*, the Supreme Court upheld this "indirect effects" interpretation of the commerce power in *Gonzales v. Raich*.[58] *Gonzales* involved a statute passed by Congress under the commerce power, which limited the use of marijuana.[59] Respondents Raich and Monson sought injunctive and declaratory relief prohibiting enforcement of the law as applied to personal medical marijuana use.[60] Justice Stevens, writing for the majority, explained how the respondents' usage of homegrown medical marijuana could still affect the broader interstate marijuana market, just as Filburn's extra wheat for homegrown consumption posed indirect effects on interstate commerce.[61] Specifically, Stevens wrote, "While the diversion of homegrown wheat tended to frustrate the federal interest in stabilizing prices by regulating the volume of commercial transactions in the interstate market, the diversion of homegrown marijuana tends to frustrate the federal interest in eliminating commercial transactions in the interstate market in their entirety."[62]

52 317 U.S. 111 (1942).
53 *Id.* at 114.
54 *Id.*
55 *Id.*
56 *Id.* at 114–15.
57 *Id.* at 125.
58 545 U.S. 1 (2005).
59 *Id.* at 14.
60 *Id.* at 6–7.
61 *Id.* at 19.
62 *Id.*

II. The Courts' Interpretations of the CFAA

While a substantial number of courts have applied the CFAA, the Supreme Court has yet to do so.[63] This has led to uncertainty in the law, especially with regard to the reach of the substantive crime. This Part provides a brief analysis of how the U.S. courts of appeals have interpreted the scope of "without authorization or exceeds authorized access." Thereafter, this Part discusses how the U.S. courts of appeals have interpreted the definition of "computer" over time. This Part concludes by showing how U.S. courts of appeals have interpreted the reach of "affecting interstate or foreign commerce," one of the controlling phrases in determining whether a computer is protected under the Act.

A. The Circuit Split Regarding 18 U.S.C. § 1030(a): "Without Authorization"

The circuit split regarding the meaning of "without authorization" has been the subject of many journal articles,[64] given the divisiveness of the varying interpretations and the resulting friction that this divide has created for legal practitioners and the lower courts. Putting it bluntly, Professor Orin Kerr has said that "[n]o one knows what it means to 'access' a computer . . . or when access becomes 'unauthorized.'"[65] This Note does not produce an exhaustive review of the circuit split but simply provides a brief explanation of the different circuits' viewpoints and justifications. Looking at the split from a sweeping perspective, there are two circuits in particular that have issued decisions that lie on polar ends of the spectrum: the Seventh Circuit in *International Airport Centers, LLC v. Citrin*[66] and the Ninth Circuit in *United States v. Nosal*.[67] In these decisions, the Seventh Circuit employed a broad interpretation[68] while the Ninth Circuit took a narrower approach.[69]

This Section will first discuss *Citrin*, as it was decided six years before *Nosal*. In *Citrin*, the Seventh Circuit held that an employee's authorization to access his employer's computer terminates when he breaches his duty of loy-

63 Tuma, *supra* note 19, at 154.

64 *See, e.g.*, Laura Bernescu, Note, *When Is a Hack Not a Hack: Addressing the CFAA's Applicability to the Internet Service Context*, 2013 U. Chi. L.F. 633; Ryan E. Dosh, Comment, *The Computer Fraud and Abuse Act: As Conflict Rages on, The* United States v. Nosal *Ruling Provides Employers Clear Guidance*, 47 Loy. L.A. L. Rev. 901 (2014); Justin Precht, Comment, *The Computer Fraud and Abuse Act or the Modern Criminal at Work: The Dangers of Facebook from Your Cubicle*, 82 U. Cin. L. Rev. 359 (2013).

65 Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1596 (2003).

66 440 F.3d 418 (7th Cir. 2006).

67 676 F.3d 854 (9th Cir. 2012) (en banc).

68 *See Citrin*, 440 F.3d at 420. The Seventh Circuit has been relatively joined by the First, Fifth, and Eleventh Circuits, all of which have also employed broader interpretations. Precht, *supra* note 64, at 362.

69 *See Nosal*, 676 F.3d at 864. The Fourth Circuit has also taken a narrow approach. Precht, *supra* note 64, at 362.

alty to his employer.[70] This case arose when Jacob Citrin engaged in improper conduct by taking his employer's marketing data, deleting the employer's copy of the data, resigning from that employer, and starting his own company.[71] Exacerbating the impropriety of Citrin's conduct, he not only deleted the employer's data, but he also made sure it was unrecoverable.[72] Against these facts, the court applied an agency theory.[73] The court reasoned that, once Citrin breached his duty of loyalty by acting against his employer's interest, his authorization to access the employer's data had terminated.[74] Thus, Citrin had accessed the employer's computer "without authorization" when he took and deleted the data, therefore violating the CFAA.[75]

The Ninth Circuit chose not to follow the reasoning of *Citrin*.[76] In *Nosal*, the Ninth Circuit decided that the CFAA does not cover employee hackers or insiders who take data from their employers in violation of a computer-use policy.[77] Similar to Citrin, David Nosal decided to leave his company and start a competing business.[78] However, rather than take data from his previous employer before leaving, Nosal hacked the data after he quit through inside contacts he still had at the firm.[79] These inside contacts all had authorized access to the employer's database, but disclosing confidential information from the database was against the company's computer-use policy.[80] The government argued that violating an employer's computer-use policy constitutes "exceed[ing their] authorized access," but the court disagreed.[81] Relying on the rule of lenity, the court held that this sort of broad interpretation would "'delegate to prosecutors and juries the inherently legislative task of determining what type of . . . activities are so morally reprehensible that they should be punished as crimes' and would 'subject individuals to the risk of arbitrary or discriminatory prosecution and conviction.'"[82] Ultimately, the court concluded that the phrase "exceeds authorized access"

70 *Citrin*, 440 F.3d at 420–21.

71 Complaint at 4–5, *Citrin*, 440 F.3d 418 (No. 03C-8104).

72 *Citrin*, 440 F.3d at 419.

73 *Id.* at 420–21. Agency law imposes a duty of loyalty that employees owe to their employers. *Id.* at 420.

74 *Id.* Judge Posner, who wrote the opinion, explained that Citrin's only basis of authority over the laptop had been based on his employment relationship. *Id.* at 421.

75 *Id.* at 420.

76 *See* United States v. Nosal, 676 F.3d 854, 862 (9th Cir. 2012) (en banc).

77 *Id.* at 863 ("We therefore respectfully decline to follow our sister circuits and urge them to reconsider instead.").

78 *Id.* at 856.

79 *Id.*

80 *Id.* at 856 n.1 (in addition to the policy, "[t]he opening screen of the database also included the warning: 'This product is intended to be used by Korn/Ferry employees for work on Korn/Ferry business only.'").

81 *Id.* at 857.

82 *Id.* at 862 (omission in original) (quoting United States v. Kozminski, 487 U.S. 931, 949 (1988)).

in the CFAA does not extend to violations of an employer's computer-use policy.[83]

When Nosal violated his company's computer-use policy, he breached his duty of loyalty by acting against his employer's interest. Under the *Citrin* school of thought, this breach should have revoked his authorization.[84] But as Judge Kozinski pointed out in *Nosal*, "[i]f Congress meant to expand the scope of criminal liability to everyone who uses a computer in violation of computer use restrictions [that] may well include everyone who uses a computer."[85] For example, a company's computer-use policy might include a term like "this computer is for business use only." Therefore, if an employee were to check a personal Facebook or Twitter account—or anything personal, for that matter—that would be a violation of the use policy. But could that sort of violation reasonably be considered an offense under the CFAA, a federal criminal statute? This concern drove the Ninth Circuit to its narrower approach.

B. The Circuit Courts' Interpretations of "Computer" Under 18 U.S.C. § 1030(e)(1)

Congress answered "what is a computer" by drafting 18 U.S.C. § 1030(e)(1). Now, in recent years, the courts have had to answer "is this a computer" upon hearing cases that bring claims under the CFAA. In contrast from their analysis of "authorization," the circuit courts have tended to use similar reasoning in analyzing various computer-like devices under the text of § 1030(e)(1).

In 2005, the Seventh Circuit held that a computer-based radio system for police, fire, ambulance, and other emergency communications (referred to as "Smartnet II") was a "computer" under § 1030(e)(1) in *United States v. Mitra*.[86] The case resulted from a radio transmission, sent by the defendant, which interfered with nineteen other communication channels and thereby stopped the flow of information among public-safety officials.[87] The defendant argued that he could not possibly be convicted under the CFAA, as the Act is meant to punish crimes like "invad[ing] a bank's system to steal financial information, or eras[ing] data on an ex-employer's system."[88] Essentially, his point was that Congress could not have intended the Act to punish a transmission sent over public radio.[89] The court rejected this argument, explaining that "[l]egislation is an objective text approved in constitutionally

83 *Id.* at 863.

84 *See* Int'l Airport Ctrs. LLC v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006).

85 *Nosal*, 676 F.3d at 857 (Judge Kozinski further explaining that if Congress had intended this, "we would expect it to use language better suited to that purpose").

86 405 F.3d 492, 493, 497 (7th Cir. 2005).

87 *Id.* at 493. The damage caused by the defendant was the resulting threat to public health and safety, given that the ability of emergency servicemen to communicate was impaired. *Id.*

88 *Id.* at 495 (citing United States v. Lloyd, 269 F.3d 228 (3d Cir. 2001)).

89 *Id.*

prescribed ways; its scope is not limited by the cerebrations of those who voted for or signed it into law."[90] The court sharply focused on the language of § 1030(e)(1) and ultimately declared that a computer-based radio system is a "computer" under the language set forth by Congress.[91] The court pointed out that, based on this analysis, the effective scope of the Act will continue to expand as more devices acquire built-in intelligence.[92] With regard to this issue of expanding scope, the court said, "[it] might prompt Congress to amend the statute but [it] does not authorize the judiciary to give the existing version less coverage than its language portends."[93]

Six years later, in 2011, the Eighth Circuit decided *United States v. Kramer*, which involved a criminal claim where the CFAA definition of "computer" was at issue.[94] In writing for the court, Judge Wollman began his opinion by referring to a quote from Steve Wozniak, cofounder of Apple, in which Wozniak said "Everything has a computer in it nowadays."[95] Wollman then got to the heart of the issue: "[I]s an ordinary cellular phone—used only to place calls and send text messages—a computer?"[96] Neil Kramer, the defendant, specifically argued that the the CFAA definition of computer "should apply only when a device is used to access the Internet."[97] The court disagreed.[98] In justifying its position, the court relied on the exceedingly broad language of § 1030(e)(1) and asserted that its definition "captures any device that makes use of a[n] electronic data processor, examples of which are legion."[99] The court then outright stated, "there is nothing in the statutory definition that purports to exclude devices because they lack a connection to the Internet."[100] In rounding out its analysis, the court mentioned that it found few similarities when comparing an automated typewriter and a handheld calculator (which are explicitly deemed "not computers" in § 1030(e)(1)) to a modern cellular phone with an electronic processor.[101]

Both the Seventh and Eighth Circuits have broadly interpreted the definition of "computer."[102] It is worth noting that in both of these cases, the

90 *Id.* The court points out that Congress "has so many brains with so many different objectives that it is almost facetious to impute a joint goal or purpose to the collectivity." *Id.*

91 *Id.* at 497.

92 *Id.* at 495.

93 *Id.*

94 United States v. Kramer, 631 F.3d 900, 901 (8th Cir. 2011).

95 *Id.* (citing Mark Milian, *Apple's Steve Wozniak: 'We've Lost a Lot of Control,'* CNN (Dec. 8, 2010), http://www.cnn.com/2010/TECH/innovation/12/08/steve.wozniak.computers/index.html).

96 *Id.*

97 *Id.* at 902.

98 *Id.*

99 *Id.* (citing Kerr, *supra* note 26, at 1577).

100 *Id.* at 903.

101 *Id.* at 902. The court also acknowledged that a "basic" cellular phone might not be colloquially considered a computer, but that they must consider it a "computer" based on the definition of the Act, by which they were bound. *Id.*

102 *See id.*; United States v. Mitra, 405 F.3d 492, 495 (7th Cir. 2005).

device at issue was used for communication (i.e., a cell phone for texting and calling and a radio for transmitting messages). However, the courts did not argue that the devices' communication abilities were close enough to internet-like communication, thereby making the devices similar enough to traditional computers. Instead, the courts placed more emphasis on the devices' electronic data-processing abilities. This would seem to suggest that, when deciding what is a "computer," the ability of a device to electronically process data is far more determinative than the ability of a device to communicate with other devices (especially considering that this argument was not even mentioned).

C. The Circuit Courts' Interpretations of "Protected Computer" Under 18 U.S.C. § 1030(e)(2)(B)

The text of 18 U.S.C. § 1030(e)(2)(B) draws on Congress's commerce power, which is expressly enumerated in the Constitution.[103] The Constitution allows for Congress to regulate commerce in three different ways: (1) with foreign nations, (2) among the several states, and (3) with the Indian tribes.[104] In enacting the CFAA, Congress relied on the first two ways, as § 1030(e)(2)(B) contains the phrase "which is used in or affecting *interstate* or *foreign* commerce."[105] Throughout history, Congress has used these magic words to trigger the commerce power and enact all sorts of regulation.[106] It has then been up to the courts to determine whether the substance of the regulation actually affects interstate or foreign commerce, just as the Supreme Court did in *Wickard* and *Gonzales*.[107] Both the Seventh and Eighth Circuits have heard constitutional arguments with regard to the CFAA, where the defendants have argued that the computer system at issue did not affect interstate commerce enough for it to be within Congress's reach.

The defendant in *Mitra* (discussed above) challenged the CFAA on constitutional grounds before the Seventh Circuit, arguing that the radio communication system at issue was beyond the reach of the commerce power.[108] Again, in this case, the court did not respond well to the crux of Rajib Mitra's argument, which rested on his belief that "Congress [could not] have contemplated such breadth."[109] The court remained steadfast in its firm approach to interpret the *text* of the law, rather than "the cerebrations of those who voted for or signed it into law."[110] Turning to the radio communication system's effect on commerce, the system was not connected to the

103 *See* U.S. CONST. art. I, § 8, cl. 3.

104 *Id.*

105 18 U.S.C. § 1030(e)(2)(B) (2012) (emphases added).

106 The first Commerce Clause case before the Court was *Gibbons v. Ogden*, 22 U.S. (9 Wheat.) 1 (1824). Most recently, the Court analyzed the scope of the commerce power in *National Federation of Independent Business v. Sebelius*, 567 U.S. 519 (2012).

107 *See supra* Section I.C.

108 United States v. Mitra, 405 F.3d 492, 495 (7th Cir. 2005).

109 *Id.*

110 *Id.*

internet, but it was networked in another way. As the court explained, "[t]he system operated on [a] spectrum licensed by the FCC."[111] The court concluded that, for this reason, Mitra's interference with the system affected interstate "communication."[112] Still, Mitra contended that his interference had no effect on any radio system in any other state.[113] Responding to this point, the court clarified the framework of the Commerce Clause analysis, explaining how, with regard to the CFAA, it is not the actor who must affect interstate commerce but the computer itself.[114] And after *Wickard* and *Gonzales*, it is settled that "[o]nce the computer is used in interstate commerce, Congress has the power to protect it from a local hammer blow, or from a local data packet that sends it haywire."[115] Mitra attempted to push his case one step further by hypothetically conceding that the radio communication system was a "protected computer," but arguing that to punish him would violate his due process rights because he was not put on reasonable notice of the Act's breadth.[116] But the court promptly shut down this position, explaining that the Act was applied to him as written and that "[t]here is no constitutional obstacle to enforcing broad but clear statutes."[117]

Although the defendant in *Kramer* did not make constitutional arguments in his case,[118] the Eighth Circuit heard this same sort of pushback from a defendant in another case, *United States v. Trotter*.[119] In *Trotter*, which came before the court in 2007, the defendant argued that a nonprofit organization's computer network did not affect interstate commerce enough for Congress to regulate it.[120] John Trotter pled guilty to his charge of intentionally causing damage to a protected computer without authorization, but he reserved his right to challenge the constitutionality of the CFAA as applied to him.[121] As background, Trotter interfered with the Salvation

111 *Id.* at 496.

112 *Id.* Note that the Seventh Circuit explicitly chose to call out the effect on "communication" rather than "commerce" (likely because the spectrum involved here was licensed by the Federal Communications Commission). *See id.* Also, the text of 18 U.S.C. § 1030(e)(2)(B) does mention both "commerce" and "communication," though all activities that affect interstate "communication" probably affect interstate "commerce."

113 *See id.*

114 *See id.*

115 *Id.*(emphasis omitted).

116 *Id.* The court clarifies the holdings from other cases, which have said that "a court may not apply a clear criminal statute in a way that a reader could not anticipate, or put a vague criminal statute to a new and unexpected use." *Id.*

117 *Id.* However, Professor Orin Kerr has argued that perhaps the CFAA should be rendered void for vagueness, which is in part due to its overbreadth, which is only expanding. *See generally* Kerr, *supra* note 26. Therefore, it is possible that Mitra's argument could have had merit, perhaps if it had been framed another way or presented in front of a different U.S. court of appeals.

118 *See supra* notes 94–101 and accompanying text.

119 478 F.3d 918 (8th Cir. 2007) (per curiam).

120 *Id.* at 919.

121 *Id.* Therefore, the constitutionality of the Act as applied was the sole issue on appeal. *See id.*

Army's computer network in all sorts of ways after the Salvation Army fired him.[122] He was not very sneaky about it; around the time of the hackings, several Salvation Army employees received pop-up messages saying "Trotter was here."[123] While Trotter admitted to his conduct, he complained, similar to Mitra, that "[n]early all computers [these] days are used someway in interstate commerce through the [I]nternet or private networks."[124] Given this, he thought the Act could not "possibly be so broad as to cover the computer network of a not-for-profit organization like the Salvation Army."[125] The court rejected this argument, largely relying on the fact that the computers were connected to the internet, which Trotter himself admitted.[126] Essentially, the computers' connection to the internet was determinative on this issue, as it made the computers "part of 'a system that is inexorably intertwined with interstate commerce' and thus properly within the realm of Congress's Commerce Clause power."[127] Before making its ruling, the court also pointed out that the nature of the attacked organization (here, the Salvation Army as a not-for-profit entity) and the location of the attack (likely all within Missouri) had no bearing on whether the computers affected interstate commerce.[128] In other words, it is the computers themselves that must affect interstate (or foreign) commerce—not the actor, the victim, or the attack.

Neither the Seventh Circuit nor the Eighth Circuit responded well to the defendants' arguments with regard to overbreadth. Both Mitra and Trotter thought it would be unfair to import nontraditional computer systems (i.e., a radio communication system and a nonprofit's computer system) into the definition of "protected computer." However, both of their arguments hinged on what the legislature would have intended, rather than the text of the law, which caused them to fail. Trotter's case was especially uncompelling because the Salvation Army computer system was connected to the internet—which the Eighth Circuit found to definitively implicate interstate commerce. Mitra also faced an uphill battle because a federal government agency (the FCC) licensed the communication spectrum for the radio system, and the text of § 1030(e)(2)(B) explicitly mentions an effect on interstate or foreign commerce *or communication*. Ultimately, it would seem that any computer that affects communication would also affect commerce, though that would make the word "communication" surplusage in this provision. Although it is unclear why Congress included both "commerce" and "communication" in the definition, including both words is unlikely to have any legal implication given the breadth of the commerce power.

122 *See id.* at 919–20.

123 *See id.* at 920.

124 *Id.* at 921 (alterations in original).

125 *Id.*

126 *See id.* The court quoted a decision from the Third Circuit, which posited that "the Internet is an instrumentality and channel of interstate commerce." *Id.* (quoting United States v. MacEwan, 445 F.3d 237, 245 (3d Cir. 2006)).

127 *See id.* (quoting *MacEwan*, 445 F.3d at 245).

128 *See id.* at 921–22.

III. APPLICATION OF THE CFAA TO VOTING MACHINES

Given Russia's interference with the 2016 U.S. election and the looming threat of continued Russian cyber interference,[129] the United States must ensure that its election systems are secure and that it can deter and punish any hackers. Because the CFAA has been the United States' principal tool in criminalizing cyberattacks,[130] it is critical to understand whether the hacking of electronic voting machines falls within the scope of the CFAA. Though the DOJ's Cyber-Digital Task Force asserted that such conduct would not be covered by the CFAA,[131] this Part reaches the opposite conclusion after carefully applying the hacking of voting machines to the key parts of the Act: § 1030(a), § 1030(e)(1), and § 1030(e)(2)(B). It seems that the crux of the Task Force's argument is that voting machines are not protected because they do not have internet and, as a result, do not meet the "affecting interstate or foreign commerce" requirement under § 1030(e)(2)(B). However, as discussed below, this argument should fail because most voting machines are still networked to a centralized election-management system, which is what makes them capable of being hacked and what causes them to affect interstate commerce.

A. Voting Machine Hacking Certainly Falls Within 18 U.S.C. § 1030(a)

Broadly speaking, the purpose of the CFAA is to prevent "fraud and related activity in connection with computers."[132] The intentional hacking of a voting machine to manipulate election results is obviously fraudulent. The first definition of "fraud" under Black's Law Dictionary is "[a] knowing misrepresentation or knowing concealment of a material fact made to induce another to act to his or her detriment."[133] Hacking a voting machine involves a knowing misrepresentation (the hacker knowingly manipulates votes) of a material fact (votes have a substantial effect on political outcomes) made to induce another to act to his or her detriment (the government would be induced to present incorrect election results, which destroys the integrity of the system).

Technically, Congress passed the roots of the CFAA in 1984 then passed the CFAA itself in 1986.[134] Perhaps unsurprisingly, around the time when Congress began to regulate computer fraud is when electronic voting machines first began coming into use. James Narey, with the help of William Saylor, patented the first model of the modern precinct-based optical scan

129 *See* Dan Coats Address, *supra* note 1.

130 *See* DOJ CYBER DIGITAL REPORT, *supra* note 10, at 62.

131 *See id.* at 121.

132 Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030 (2012).

133 *Fraud*, BLACK'S LAW DICTIONARY (10th ed. 2014). To further elaborate on the definition, the dictionary includes a quote from John Willard, in which he describes fraud as "any *kind of artifice by which another is deceived*." *Id.* (quoting JOHN WILLARD, A TREATISE ON EQUITY JURISPRUDENCE 147 (Platt Potter ed., New York, Banks & Bros. 1879)).

134 *See* Tuma, *supra* note 19.

systems in 1977.[135] This type of system uses an optical scanner to read marked paper ballots and tally the results; it is still used in elections today (and will be more closely examined as a "computer" in Section III.B). Nebraska was the first state to adopt an optical scan system as part of its elections, when several of its counties used the American Information Systems Central-Count Ballot Tabulator in 1982.[136] Five years later, in 1987, the R.F. Shoup Corporation and Robert Boram patented the Shouptronic ELECTronic voting machine, which was "one of the first [push-button] direct recording electronic voting machines to achieve significant commercial success."[137] Though the innovation of electronic voting machines overlapping with the time period in which Congress legislated the CFAA could be construed as irrelevant to the CFAA's legal application,[138] this bit of information might be used to rebut someone who argues that Congress could have never foreseen the introduction of these devices and therefore could have never intended the CFAA to apply to them.

As for the conduct of the hacking itself, it would be an insurmountable stretch to conceive of a situation where the hacking of a voting machine does not satisfy the "without authorization or exceeding authorized access" requirement, especially in the context of Russia hacking U.S. election devices. Though the courts have struggled to understand what it means to lack authorization, they certainly would have no trouble in deciding that the cyber hacking of U.S. elections constitutes unauthorized conduct. Although both the *Nosal* and *Citrin* cases arose in the employment context, their holdings still suggest this conclusion. After all, the holding in *Citrin* implies that an employee could be charged under the CFAA for violating an employer's computer-use policy—a laughable offense when compared to election hacking.[139] Relying on the rule of lenity, the Ninth Circuit held that the CFAA does not extend to violations of an employer's use policy.[140] However, the Ninth Circuit's concern about a broad interpretation of the CFAA leading to arbitrary and discriminatory prosecution has no bearing in this context;[141] unauthorized hacking of an electronic voting machine is the exact type of conduct that the CFAA was designed to prohibit.

B. Voting Machines Fall Within 18 U.S.C. § 1030(e)(1)

Up until this point, this Note has referred to voting machines generally as if they were one uniform type of device. However, this is not the case, and

135 *Historical Timeline: Electronic Voting Machines and Related Voting Technology*, PROCON.ORG, https://votingmachines.procon.org/view.timeline.php?timelineID=000021 (last updated July 22, 2013).

136 *Id.*

137 *Id.*

138 A position both the Seventh and Eighth Circuits might take based on their respective decisions in *Mitra* and *Trotter*. *See supra* Section II.C.

139 *See* Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006).

140 *See* United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012) (en banc).

141 *See id.* at 862.

it is crucial to understand the full range of voting machine technology in order to define the machines as "computers" under the CFAA. That said, both *Mitra* and *Kramer* demonstrated that satisfying the definition of "computer" is a fairly simple step,[142] and as a precursor to the following discussion, it should be clear that all of the voting machine devices are "computers" under the CFAA. While this may be so, setting up what the "computers" are will be key in guiding the analysis as to whether they are "protected." There are three types of machines to be considered as "computers": (1) the optical-scan systems, (2) the direct recording electronic voting machines ("DREs"), and (3) the centralized election-management systems.

The optical-scan systems and DREs are used on-site at polling locations, and they are considered the two primary categories of voting machines.[143] More than 350,000 of these types of machines are used in the United States today.[144] As mentioned in Section III.A, James Narey patented the first optical-scan system in 1977, and these systems are used to streamline the process of scanning and tallying marked paper ballots.[145] The R.F. Shoup Corporation launched the first DRE in 1987.[146] This type of machine allows voters to touch a screen or button to place their vote, and both the ballots and votes are kept entirely digital.[147] Most crucially:

> With both kinds of voting systems, digital votes are stored on memory cards or flash drives that are collected from machines after an election and are supposed to be used for official results. But many machines also have embedded or externally connected modems to transmit unofficial results rapidly on election night.[148]

This means that both the optical-scan systems and the DREs are "data processing device[s] performing . . . storage functions," and the both "include[ ] . . . data storage facilit[ies]," all of which is language pulled directly from § 1030(e)(1).[149] The optical-scan system is of course an "optical" device, and the DRE is an "electronic" device. Therefore, both of these machines satisfy the definition of "computer" based on the objective text of the Act, which is what the Seventh Circuit said must be considered.[150] They

142 *See* United States v. Kramer, 631 F.3d 900 (8th Cir. 2011); United States v. Mitra, 405 F.3d 492 (7th Cir. 2005).

143 *See* Kim Zetter, *The Myth of the Hacker-Proof Voting Machine*, N.Y. TIMES MAG., (Feb. 21, 2018), https://www.nytimes.com/2018/02/21/magazine/the-myth-of-the-hacker-proof-voting-machine.html.

144 *Id.*

145 *Historical Timeline: Electronic Voting Machines and Related Voting Technology*, *supra* note 135.

146 *Id.*

147 Zetter, *supra* note 143. While the process is made entirely digital with DREs, "some DREs are outfitted with printers to produce a voter-verifiable paper trail." *Id.*

148 *Id.*

149 18 U.S.C. § 1030(e)(1) (2012) (emphasis added).

150 *See* United States v. Mitra, 405 F.3d 492, 495 (7th Cir. 2005).

both are devices that make use of an electronic data process, which for the Eighth Circuit concludes the analysis.[151]

The optical-scan systems and DREs usually transmit their unofficial results to the third type of machines: the centralized election-management systems. Often, the optical-scan systems and DREs are equipped with either analog or cellular modems that send the unofficial results to these central systems.[152] The centralized election-management systems are used to "receive results then check the signature to authenticate the data transmission."[153] The final votes are tallied by these systems. Because these systems make use of an electronic data process, and include both *data storage facilities* and *communications facilities*, they are also "computers" under the definition of the CFAA.

The above descriptions contain a handful of qualifiers such as "many," "usually," and "most." This is because there is a general method that most states follow in collecting and counting their votes, but specific device models and tallying procedures vary across states, and even across counties within a given state.[154] For example, one of the more popular voting machine devices is the DS200, an optical-scan system that is used in thirty-one states and the District of Columbia.[155] Even still, that means nineteen states do not use the DS200, and of the states that use it, only Maryland, Maine, Rhode Island, and the District of Columbia use exclusively DS200 machines statewide.[156] All of this to say that if a hacking were to occur, it would be important to first identify the exact type of systems that were hacked because there is a range of possibilities.

C. Voting Machines Probably Fall Within 18 U.S.C. § 1030(e)(2)(B)

Though not every polling place uses the voting machines' modems to transmit results, most do, and it is the devices that transmit results by modem that pose the greatest opportunity for infiltration by cyberhackers.[157] Therefore, at this point in the analysis, it should be assumed that the optical-scan systems, DREs, and centralized election-management systems at issue are ones that use embedded or externally connected modems. It should also be assumed, as the Cyber-Digital Task Force put forward in their report, that

151 *See* United States v. Kramer, 631 F.3d 900, 902 (8th Cir. 2011).

152 Zetter, *supra* note 143.

153 *Id.*

154 *See id.*

155 *Id.* The DS200 is produced by Election Systems & Software, "[t]he top voting machine maker in the country." *Id.*

156 *Id.* Those using the DS200 statewide also have two other systems available for disabled voters and absentee ballots. *Id.*

157 *Id.* For example, "Richard Rydecki, Wisconsin's state elections supervisor, says counties in his state decide individually whether to transmit election results. Fred Woodhams, spokesman from the Michigan Department of State, said the same is true in his state." *Id.*

these machines are not connected to the internet.[158] To be sure, this Note concedes that the transmission of results via analog or cellular modem is distinguishable from transmissions sent over the internet. However, because the voting machines are still networked (be it in a more secure environment), they should be considered to affect interstate commerce, thus meeting the jurisdictional requirement laid out in § 1030(e)(2)(B).

Since the voting machines are not connected to the internet, they cannot be said to definitively affect interstate commerce like the Salvation Army computer network system in *Trotter*.[159] The court in *Trotter* treated the internet as both an "instrumentality and channel of interstate commerce," which makes computers connected to the internet fall squarely within Congress's regulatory power under the Commerce Clause.[160] Conversely, the highly secured modem transmissions made by voting machines are not "inexorably intertwined with interstate commerce" like the internet.[161] Thus, the *Trotter* decision leaves open the question of whether more securely hardened network systems—like voting machines—also affect interstate commerce. However, what is evident after *Trotter* is that, in conducting the interstate commerce analysis, it should not matter that voting machines are operated by local governmental officials.[162] Though the localness of voting machine operations could seem to remove the voting machines from interstate commerce, the Eighth Circuit made clear that "it is the characteristics of the computer or computer network, not the entity using the network, that is the focus of the statute."[163]

The holding in *Mitra* proved that it is unnecessary for a "computer" to be connected to the internet in order for it to affect interstate commerce.[164] This case is very relevant given the Task Force's assertion that voting machines are not covered under the CFAA because they are not connected to the internet.[165] In *Mitra*, the Seventh Circuit found that a radio communication system affected interstate commerce because the system operated on a spectrum licensed by the FCC and affected interstate "communication."[166] Furthermore, it was irrelevant that Mitra had only used the radio system in one state because the system itself affected interstate commerce and therefore could be regulated locally.[167] The largest contrast between voting

158 DOJ CYBER DIGITAL REPORT, *supra* note 10, at 121.

159 *See* United States v. Trotter, 478 F.3d 918 (8th Cir. 2007) (per curiam).

160 *Id.* at 921 (quoting United States v. MacEwan, 445 F.3d 237, 245 (3rd Cir. 2006)); *see also* United States v. Lopez, 514 U.S. 549, 558–59 (1995) (breaking down Congress's power to regulate interstate commerce into its ability to regulate channels of interstate commerce, instrumentalities of interstate commerce, and activities that substantially affect interstate commerce).

161 *See Trotter*, 478 F.3d at 921 (quoting *MacEwan*, 445 F.3d at 245).

162 *See id.*

163 *Id.*

164 *See* United States v. Mitra, 405 F.3d 492, 493 (7th Cir. 2005).

165 DOJ CYBER DIGITAL REPORT, *supra* note 10, at 121.

166 *See Mitra*, 405 F.3d at 496.

167 *Id.*

machines and the facts of *Mitra* is that the communication between voting machine devices across modem lines is not regulated by a federal agency. Rather, local government officials regulate this type of communication.[168] While this discrepancy is unfavorable to the case for voting machines being covered under the CFAA, it perhaps only means that the communication between voting machines cannot be considered a channel or instrumentality of interstate commerce.

This still leaves room for the communication between voting machines to be an activity that "substantially affects interstate commerce."[169] Voting machines, as the sum of component parts and technological development, are a bit more complex than the simple commodity goods of wheat and marijuana, which were respectively scrutinized before the Supreme Court in the Commerce Clause cases of *Wickard* and *Gonzales*. Despite the factual difference, those cases stand for a relevant proposition: an activity that only places indirect effects on interstate commerce can still be regulated by Congress under the commerce power.[170] Applying that test here, while borrowing some of the language from *Gonzales*, the hacking of a local county's election would tend to frustrate the federal interest in eliminating election fraud in the interstate market in its entirety.[171] As to the "interstate market in its entirety" in this context, the voting machine industry is currently dominated by three privately held companies: Dominion Voting Systems Corporation, Election Systems & Software, and Hart InterCivic.[172] If a hacker were to infiltrate a local election in a county using Dominion's products, that could have grave effects on Dominion's overall business and thus affect the entire interstate market for voting machines because other local counties (across state lines) using Dominion products would probably lose trust in Dominion's system and switch vendors. On top of that, Dominion's suppliers would stand to lose a customer account.

Overall, because the voting machines are networked via modem lines, they have the potential to be hacked, and even a purely local hacking could substantially affect the interstate market. This satisfies the interstate commerce requirement, as laid out in 18 U.S.C. § 1030(e)(2)(B).

168 *See* Zetter, *supra* note 143. Also, note how this is different than the reasoning from *Trotter*. It has no bearing on the analysis that local government officials are the ones using the network, but it might matter that they are the ones regulating it.

169 *See* United States v. Lopez, 514 U.S. 549, 559 (1995).

170 *See* Gonzales v. Raich, 545 U.S. 1 (2005); Wickard v. Filburn, 317 U.S. 111 (1942).

171 *Gonzales*, 545 U.S. at 19. *Gonzales* held that "the diversion of homegrown marijuana tends to frustrate the federal interest in eliminating commercial transactions in the interstate market in their entirety." *Id.*

172 Anders Melin & Reade Pickert, *Private Equity Controls the Gatekeepers of American Democracy*, BLOOMBERG (Nov. 3, 2018), https://www.bloomberg.com/news/articles/2018-11-03/private-equity-controls-the-gatekeepers-of-american-democracy.

CONCLUSION

On the whole, there is a strong case for voting machines (at least those networked in some way, which are most of them) to be covered under the CFAA. Although it might seem safer to expressly add voting machines to the scope of the CFAA through another amendment, this solution is not a workable one. The hacking of a voting machine clearly satisfies § 1030(a) and § 1030(e)(1). The heart of the issue is whether this conduct satisfies § 1030(e)(2)(B). Right now, § 1030(e)(2)(B) invokes the full breadth of Congress's commerce power. That said, even if "protected computers" were to expressly include voting machines, a defendant could still argue that this amendment should be void for being outside the scope of the commerce power. A better fallback option would be for state and local governments to create laws within the scope of their police power to protect elections from fraud. But hypothetically, if Russia were to hack California's voting machines in the next presidential election (and successfully change the national result), the burden, it seems, should fall on the federal system to prosecute the hackers, rather than on California's state system alone.

Obviously, the conclusion that voting machines are covered under the CFAA is only doing more to expand the CFAA's scope. From one angle, this is positive because there is a need for cybercrime laws to be flexible given how rapidly technology continues to change. Particularly here, the nation has a compelling interest in having the CFAA at its disposal in combating election fraud, given the CFAA's role as the "principal tool for prosecuting computer crimes."[173] But looked at in another way, the CFAA is perhaps becoming too broad for its own good. Along with more breadth comes more discretion given to to judges and juries, which tends to lead to arbitrary and discriminatory prosecutions.

The good news is that the voting machine devices have yet to be directly hacked by Russia. Although Russia may only continue to interfere with elections in other ways (like their dissemination of fake ad campaigns on social media), it is impossible to know exactly what they are capable of doing. As Dan Coats said, "the warning lights are blinking red again."[174] Given the dangerous level of threat, an attack on U.S. voting machines might be one of Russia's next moves in its ongoing cyber warfare. In the aftermath, the DOJ should have the CFAA at its disposal to restore justice.

If that time does come, consider this Note a ballot cast: voting machines are "protected computers."

173 DOJ CYBER DIGITAL REPORT, *supra* note 10, at 62.

174 Dan Coats Address, *supra* note 1.