Computer Criminal Intent

By MICHAEL S. DORSI* *and* KEENAN W. NG**

Introduction

IN THE CRIMINAL JUSTICE SYSTEM, computer-based offenses are governed by vague and ambiguous laws.[1] But despite the broad range of conduct potentially covered by these *computer crime* laws, these laws require proof of intentionally unauthorized conduct. Extensive commentary concerning computer crime law discusses culpable conduct, but little discusses culpable intent.

This Article contributes to the literature in two ways: First, this Article directly addresses the intent requirements, arguing for a greater showing of culpable intent. This Article documents that the Ninth Circuit's *en banc* decision in *United States v. Nosal* weakened the required showing of intent under the Computer Fraud and Abuse Act ("CFAA"), that the relevant language is not mere dicta, but was briefed, argued, and decided, reaching a result that we contend is in error. Second, this Article addresses the often-discussed subject of culpable conduct, criticizing the popular (at least among academics) *technical access barrier* rule. This rule, as articulated in *Facebook v. Power Ventures*, would require that the plaintiff or prosecutor prove that a defendant circumvented some technical or code-based barrier; and if such proof is not made, the defendant should prevail. We review the

* Ad Astra Law Group, LLP, San Francisco, California; J.D. Harvard Law School, 2011; B.A. University of California, Berkeley, 2006.

** Labor and Employee Relations, University of California, San Francisco; J.D. University of San Francisco, 2009; B.A. University of California, Los Angeles, 2004. All views are solely the Authors' own and do not reflect the positions of Ad Astra Law Group, LLP, its clients, or the University of California.

Mr. Dorsi and Mr. Ng were counsel for plaintiffs in *NovelPoster v. Javitch Canfield Group, et al.*, U.S. District Court for the Northern District of California case no. 3:13-cv-05186, and *Reyes & Barsoum LLP v. Knox Ricksen LLP et al.*, Los Angeles County Superior Court case no. BC572975. The authors wish to thank Katy Young and Ad Astra Law Group, LLP for the work on the litigation that relates to this Article.

1. *Apologies to Law and Order* (Wolf Films/NBC Universal, Sept. 13, 1990–May 24, 2010) for this phrase, and to *Law and Order: Criminal Intent* (Wolf Films/NBC Universal, Sept. 30, 2001–June 26, 2011) for the title.

results from a series of district court cases that offer compelling evidence that the *technical access barrier* rule, a rule designed to protect defendants by limiting culpable conduct, does not improve outcomes for defendants. We argue that such a rule is not compatible with statutory text. And we contend that a technical barrier rule would be undesirable on policy grounds.

Computer crime law is serious business. The federal government and every state have enacted computer crime statutes. These statutes protect important privacy interests, but have received meritorious criticism for imposing excessive liability on innocuous behavior. The CFAA is the principal tool for federal prosecutors to address computer hacking, a crime that was arguably beyond the scope of older criminal trespass laws. Originally designed to protect confidential information, financial records, and government computers, several amendments have transformed the statute into an all-purpose computer misuse statute. The CFAA has attracted substantial media attention.[2] Notable cases include the prosecutions of Aaron Swartz concerning access to JSTOR[3] via MIT's systems,[4] Andrew Auernheimer's involvement with the disclosure of AT&T security flaws,[5] and Lori Drew for the creation and use of a fabricated MySpace profile.[6]

In its broadest provision, the CFAA makes it a crime to access information without authorization or in excess of authorized access.[7] One federal appeals court even held that it was a felony to use a company's information for non-company purposes because the agency relationship terminates upon breach of the duty of loyalty.[8] Another federal appeals court recognized how this might extend criminal liability to ordinary behavior, providing this among several colorful examples:

2. *See, e.g.*, Tim Wu, *Fixing the Worst Law in Technology*, THE NEW YORKER (Mar. 18, 2013), http://www.newyorker.com/news/news-desk/fixing-the-worst-law-in-technology [https://perma.cc/D2J3-KXZS]; *see also* The Documentary Network, *The Internet's Own Boy: The Story of Aaron Swartz*, YOUTUBE (Mar. 19, 2017), https://www.youtube.com/watch?v=vxr-2hwTk58.

3. JSTOR is a digital library of academic journals, books, and primary sources. JSTOR, https://www.jstor.org/ (last visited Jan. 23, 2016).

4. United States v. Swartz, 945 F. Supp. 2d 216, 217 (D. Mass. 2013) (order on confidentiality of materials disclosed).

5. United States v. Auernheimer, 748 F.3d 525, 530 (3d Cir. 2014).

6. United States v. Drew, 259 F.R.D. 449, 451 (C.D.Cal. 2009).

7. 18 U.S.C. § 1030(a)(2)(C) (2006).

8. Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006) (Posner, J., writing for a unanimous panel).

"[C]onsider the numerous dating websites whose terms of use prohibit inaccurate or misleading information. *See, e.g.*, eHarmony Terms of Service § 2(I), http://www.eharmony.com/about/terms ("You will not provide inaccurate, misleading or false information to eHarmony or to any other user.") (last visited Mar. 4, 2012). . . . Under the government's proposed interpretation of the CFAA, posting for sale an item prohibited by Craigslist's policy, or describing yourself as 'tall, dark and handsome,' when you're actually short and homely, will earn you a handsome orange jumpsuit."[9]

Because of the potentially broad and excessively punitive interpretations, several courts have attempted to cabin the CFAA and its state law counterparts. Perhaps the most popular suggestion in academic and advocacy literature is a *technical access barrier* rule. Under such a rule, a defendant would not be held to have acted without authorization unless the defendant circumvented a technical or code-based barrier to access—regardless of any proof of intent offered by the prosecutor or plaintiff.[10] No appellate court has adopted this restriction.[11] Nonetheless, many of the federal district judges in the Northern District of California began applying this rule to California's state-law analog, the Comprehensive Computer Data Access and Fraud Act ("CDAFA") when raised in federal court on supplemental jurisdiction.[12] By a quirk of procedure, the order establishing CDAFA's *technical barrier rule* did not also apply to the CFAA. For the most part, other judges accepted that distinction.[13] As a result, the two similar statutes were interpreted differently, allowing for a side-by-side

9. United States v. Nosal, 676 F.3d 854, 862 (9th Cir. 2012) (*Nosal I*) (en banc) (Kozinski, J., writing for the majority).

10. *See, e.g.*, Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1650–51 (2003) (hereinafter *Kerr 2003*); *Statutory Interpretation—Computer Fraud and Abuse Act—Ninth Circuit Holds that Employees' Unauthorized Use of Accessible Information Did Not Violate the CFAA*—United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (en banc), 126 Harv. L. Rev. 1414, 1454–1456 (2013); Brief for Electronic Frontier Foundation as Amici Curiae Supporting Defendant-Appellant, United States v. Nosal, 676 F.3d 854, 862 (9th Cir. 2012) (No. 13-10037), *available at* https://www.eff.org/document/eff-amicus-brief-2014.

11. A Ninth Circuit panel indicated that such a rule does not apply under the federal CFAA, but has not extended the application of this decision to California's state-law counterpart. *See* United States v. Nosal, 828 F.3d 865, 878 (9th Cir. 2016) (*Nosal II*).

12. *See, e.g.*, Top Agent Network, Inc. v. Zillow, Inc., No. 14-cv-04769, 2015 WL 7709655, at 11 (N.D. Cal. Apr. 13, 2015). As discussed in *infra* Part III, although Professor Kerr initially advocated a *technical access barrier* rule, his most recent article, *Norms of Computer Trespass*, argues that authentication gates (usernames and passwords) are the most important barriers, and other barriers may be insufficient. Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143 (2016) (hereinafter *Kerr 2016*).

13. *See infra* Part II.B.

analysis of how the law applies to numerous cases. Results of this experiment are underwhelming for advocates of a *technical barrier rule*. Cases where the technical barrier rule is invoked tend to see the federal CFAA claims dismissed on other grounds.[14] And when conduct seems sufficiently egregious, courts find a way around the rule and preserve CDAFA claims.[15]

Despite judicial scrutiny, media attention, and academic literature, few articles and even fewer judicial opinions address the criminal intent requirements—known as *mens rea*. The CFAA requires that a person "intentionally accesses a computer without authorization or exceeds authorized access."[16] Courts have split on the meaning of this statute, sometimes suggesting that a person need only intend to access, but may not even have to know that the access is without authorization.[17] Other courts have held that the defendant must intend that their access be without authorization or in excess of authorized access.[18]

This Article addresses the question of *mens rea* directly, arguing that the CFAA and similarly phrased state statutes require not only that access be intentional, but that lack of authorization be intentional. This awkward phrasing, unavoidable given the statute, means the defendant must know the facts relevant to unauthorized access and intentionally act contrary to the lack of authorization.[19] This is a proper reading of text and purpose, and affords substantial protection to defendants. The Article acknowledges that the Ninth Circuit ruled contrary to this interpretation, and argues that such an interpretation is in error.

This Article addresses the importance of *mens rea* in light of the proposed *technical access barrier rule*. We conclude that imposing a technical access barrier rule is inconsistent with the text, purpose, and precedent under the CFAA and its California state-law counterpart. While circumvention of technical barriers may be good evidence of criminal intent, it should not be required. The inherent ambiguity in what qualifies as a technical barrier also has the potential to render the rule

14. *See id.* (discussing catalog of cases).

15. *See, e.g.*, NovelPoster v. Javitch Canfield Grp., 140 F. Supp. 3d 954, 967 (N.D. Cal. 2014).

16. 18 U.S.C. § 1030(a)(2) (2006).

17. United States v. Nosal, 676 F.3d 854, 859 (9th Cir. 2012) (en banc) (*Nosal I*).

18. *See, e.g.*, Butera & Andrews v. IBM Corp., 456 F. Supp. 2d 104, 110 (D.D.C. 2006); United States v. Morris, 928 F.2d 504, 505 (2d Cir. 1991); United States v. Sablan, 92 F.3d 865, 868 (9th Cir. 1996); *see also* Kerr 2016, *supra* note 12.

19. *See* Kerr 2016, *supra* note 12, at 1180–81.

arbitrary. Given this potential, we engage in an empirical inquiry: Does a technical access barrier rule actually help defendants? The evidence indicates that it does not. Our review of district court cases applying a technical access barrier rule under the analogous California CDAFA, but not the federal CFAA, shows that the rule does not provide the sort of protection defendants seek. We analyze the role played by the *mens rea* requirement both in the presence and absence of a *technical access barrier rule*. We address textual analysis, which weighs against a technical access barrier rule. And we address policy. We argue that a technical access barrier rule presents two policy problems. First, such a rule would eliminate liability in cases of clear wrongdoing, such as schemes to lock owners out of their own computer systems. Second, we contend that rapidly changing technology standards ensures the law would struggle to define what constitutes a requisite barrier, making the understanding of "without authorization" a moving target based on the latest technological developments.

This Article also seeks to speak to attorneys who, sometimes by surprise, find their clients either needing to bring or defend computer misuse claims. This is not an uncommon occurrence, particularly given the use of the CFAA to bring state-law trade secrets cases in federal court.[20] For those attorneys, this Article seeks to provide a comprehensive look at the law and how to apply it in its current form, avoiding oversimplification but maintaining clarity and support.

We conclude, with a few notable but narrow exceptions, that the proper application of *mens rea* requirements to computer crime statutes provides protection for defendants and remedies for aggrieved victims. We concede one important exception: the misdemeanor provision—18 U.S.C. 1030(a)(2)(C)—may not be possible to save from constitutional scrutiny. This provision makes it a crime to "intentionally access[ ] a computer without authorization or exceed[ ] authorized access, and thereby obtain[ ] . . . information from any protected computer." Even the most stringent application of *mens rea* requirements may not resolve the problems with this provision. This Article suggests that subsection (a)(2)(C) may be unconstitutional, and that the current trend in appellate decisions may force courts to address this question soon.

20. This may change given the creation of a civil right of action under the Economic Espionage Act, 18 U.S.C. § 1831 (2013).

I. Development of Intent and Conduct Requirements Under the Computer Misuse Statutes

Today's CFAA is the result of the original statute and nine amendments, which cumulatively broadened the statute.[21] Originally focused on classified information, financial records, and government computers, the statute now extends to any computer in interstate commerce.[22] This history is well-documented in the literature.[23] For purposes of this Article, the background section will cover particular enactments and cases that bear on the intent requirements and definitions of culpable conduct.

Our review illustrates that the intent requirement should have been an easy matter of statutory interpretation, and for some time this appeared to be the course of the law. However, this trajectory broke down. In *United States v. Nosal*, a case focused primarily on culpable conduct, the Ninth Circuit eviscerated the intent requirement. Despite increased attention to culpable intent in recent high-profile cases, it has not addressed this error.

A. Origins of the Computer Fraud and Abuse Act and its Intent Requirements

Congress passed the CFAA after legislators watched the movie WarGames.[24] In WarGames, the hacker, David Lightman, played by Matthew Broderick, intentionally accesses computer systems that he is

21. Greg Pollaro, *Disloyal Computer Use and the Computer Fraud & Abuse Act: Narrowing the Scope*, 2010 DUKE L. & TECH. REV. 12, 7–8 (2010); *see also* Benjamin Glatstein, et. al, *Scraping Content: the CFAA, DMCA, and Terms of Use, Legal Frontiers in Digital Media*, MEDIA LAW RESOURCE CTR. (June 19, 2014), https://medialawmlrc.wordpress.com/2014/06/19/scraping-content-the-cfaa-dmca-and-terms-of-use/ [https://perma.cc/A4S6-GTSG].

22. 18 U.S.C.A. § 1030 (2008) (containing past versions of statute).

23. Pollaro, *supra* note 21, 7–10; *see, e.g.*, Kerr 2003, *supra* note 10.

24. H.R. Rep. No. 98-894, at 10 (1984), reprinted in 1984 U.S.C.C.A.N. 3689, 3695–96 ("[T]he motion picture WarGames showed a realistic representation of the automatic dialing and access capabilities of the personal computer."); *see also* Pollaro, *supra* note 21, ¶¶ 4–7. The concern with computer security inspired by WarGames extended to the White House, where President Reagan mentioned the movie to his advisors. Reagan reportedly asked whether something like the movie could actually happen, and after some investigation learned that government computer vulnerabilities were far more extensive than portrayed in the film. *See* Terry Gross, *From Reagan's Cyber Plan To Apple Vs. FBI: 'Everything Is Up For Grabs,'* FRESH AIR (NATIONAL PUBLIC RADIO), *available at* http://www.npr.org/sections/alltechconsidered/2016/03/22/471416946/from-reagans-cyber-plan-to-apple-vs-fbi-everything-is-up-for-grabs, [https://perma.cc/73YV-HSBQ] (discussing Fred Kaplan, DARK TERRITORY, ch. 1 (2016)).

not supposed to access, such as the gradebook at his school and the U.S nuclear arsenal.[25]

The first major prosecution would not be for breach of nuclear weapons computers, but for what by all accounts was intended to be an innocuous test of the early Internet. However, it turned out to overburden computers and cause many Internet-connected computers to stop functioning. The culprit was the *Morris Worm*, known today as the first widespread computer worm.[26]

The United States prosecuted Morris, charging him under the CFAA. At the time, the relevant provision criminalized:

> [I]ntentionally access[ing] a Federal interest computer without authorization, and by means of one or more instances of such conduct alters, damages, or destroys information in any such Federal interest computer, or prevent authorized use of any such computer or information, and thereby—(A) causes loss to one or more other of a value aggregating $1,000 or more during any one year period.[27]

The jury convicted Morris. Morris moved for acquittal, which the district court denied.[28] The trial court held that the statute was "clear and unambiguous" that the "intent requirement applied only to the accessing and not to the resulting damage."[29] Morris appealed, arguing that the statute required him not only to intend the wrongful act, but also to intend harm.[30] Morris was sentenced to serve three years' probation, 400 hours of community service, and was levied a $10,050 fine.[31] Morris appealed.

The Second Circuit Court of Appeals affirmed, concluding that the intent requirement applied only to unauthorized access, not intent to cause damage.[32] The court explained that "the wording, structure, and purpose of the subsection, examined in comparison with its

25. WarGames (Metro-Goldwyn-Mayer 1983); *see* WarGames, Wikipedia, https://en.wikipedia.org/wiki/WarGames (last visited Feb. 15, 2017) [https://perma.cc/A87G-STK3].

26. Jonathan Zittrain, The Future of the Internet — And How to Stop It, 37 (2008).

27. 18 U.S.C. § 1030(a)(5)(A) (1986), Pub. L. No. 99-474, 98 Stat. 2190.

28. United States v. Morris, 928 F.2d 504, 510 (2d Cir. 1991), *cert. denied*, 502 U.S. 817 (1991).

29. *Id.* at 506–507 (describing decision by Judge Munson of the Northern District of New York).

30. *Id.* at 508. Morris also argued that his conduct with the worm did not exceed his authorized access. The court rejected this as well. *Id.* at 510.

31. Zittrain, *supra* note 26, at 37–39.

32. *Morris*, 928 F.2d at 505. Judge Newman wrote the opinion of the court, and was joined by Judge Winter and Judge Daly of the U.S. District Court for the District of Connecticut, sitting by designation. *Id.*

departure from the format of its predecessor provision persuade us that the 'intentionally' standard applies only to the 'accesses' phrase of section 1030(a)(5)(A), and not to its 'damages' phrase."[33] While not the focus of the decision, the Court of Appeal emphasized that intent applied to lack of authorization. Judge Newman quoted the Senate Report, explaining that "Congress sought only to proscribe intentional acts of unauthorized access, not 'mistaken, inadvertent, or careless' acts of unauthorized access."[34] Morris petitioned for certiorari, which the Supreme Court denied.[35] The Second Circuit view of *mens rea* under the CFAA was adopted in other circuits,[36] and accepted by commentators[37] and research services.[38]

This ought to have been the end of the discussion of *mens rea* under the CFAA. However, in efforts to cabin *unauthorized access*, the Ninth Circuit revisited this subject. As discussed in Part I.D, *infra*, the Ninth Circuit appears to have created a circuit split by ruling that only intent to access is required, meaning that unauthorized access may be criminal even if the defendant does not know that access is unauthorized.

B. Introduction of CFAA Civil Suits and Broader Liability

In 1994, Congress passed one of several amendments to the CFAA, this time authorizing private suits.[39] To bring a civil suit, Congress established additional procedural hurdles that typically require civil litigants to prove damage or loss in excess of $5,000.

A civil action under the CFAA is limited to persons who have suffered "damage or loss."[40] Damage and loss are defined terms, and do not mean usual tort or contract damages. "[T]he term 'damage' means any impairment to the integrity or availability of data, a program, a system, or information."[41] "'[D]amage' means harm to com-

33. *Id.* at 509.

34. *Id.* at 507 (citing S.Rep. No. 99-432, 99th Cong., 2d Sess. 5 (1986), reprinted in 1986 U.S.Code Cong. Admin. News 2479, 2483).

35. United States v. Morris, 502 U.S. 817 (1991) (denial of certiorari).

36. *See, e.g.*, United States v. Sablan, 92 F.3d 865, 868 (9th Cir. 1996); Butera & Andrews v. IBM Corp., 456 F. Supp. 2d 104, 109–110 (D.D.C. 2006).

37. Kerr 2016, *supra* note 12, at 1180–82.

38. Charles Doyle, Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws, Cong. Research Serv., Br. No. 97-1025, at 3 (2014) (discussing House and Senate Reports).

39. *See* Pollaro, *supra* note 21 (citing H.R. REP. NO.103-711, 290001 (1994) (Conf. Rep.), as reprinted in 1994 U.S.C.C.A.N. (1839).

40. 18 U.S.C. § 1030(g) (2012).

41. 18 U.S.C. § 1030(e)(8) (2012).

puters or networks, not economic harm due to the commercial value of the data itself."[42]

"Loss" means "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."[43]

In addition, a civil action "may be brought only if the conduct involves [one] of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i)."[44] Subclauses II–V concern medical care, physical injury, public safety, and government activity in law enforcement and national security, respectively. They often do not apply. The remaining subclause, part I, requires $5,000 of damage or loss. Of course, few litigants sue in federal court over cases they believe to be worth less than $5,000. As a result, civil suits often drive the direction of the CFAA.[45]

The next set of amendments, passed as part of the Economic Espionage Act of 1996, expanded the scope of liability to include accessing a protected computer without authorization or in excess of authorized access.[46] This provision, now codified at 18 U.S.C. § 1030(a)(2)(C), remains the broadest provision in the statute.[47]

C. Litigating the Meaning of *Without Authorization* and *Exceeds Authorized Access*

Beginning in the 2000's, a split among the federal courts of appeal developed concerning the meaning of *without authorization* and *exceeds authorized access*. The Seventh Circuit weighed in first in the civil case of *International Airport Centers v. Citrin*.[48] Several affiliated companies, referred to as International Airport Centers or IAC in the opinion, alleged that former employee Jacob Citrin had misappropriated

42. NetApp, Inc. v. Nimble Storage, Inc., 41 F. Supp. 3d 816, 834 (N.D. Cal. 2014) (account of defendant's argument later adopted by court).

43. 18 U.S.C. § 1030(e)(11) (2012).

44. 18 U.S.C. § 1030(g) (2012).

45. *See, e.g.*, United States v. Drew, 259 F.R.D. 449, 456–57 (C.D. Cal. 2009) ("Because of the availability of civil remedies, much of the law as to the meaning and scope of the CFAA has been developed in the context of civil cases.").

46. *See* Patricia L. Bellia, *A Code-Based Approach to Unauthorized Access Under the Computer Fraud and Abuse Act*, 84 GEO. WASH. L. REV. 1442, 1462–63 (2016) (*citing* Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3492 (codified at 18 U.S.C. § 1030(a)(2)(C) (1996))).

47. United States v. Nosal, 676 F.3d 854, 859–860 (9th Cir. 2012) (en banc) (*Nosal I*).

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

information belonging to IAC and destroyed data on a company computer to cover his tracks.[49] Citrin moved to dismiss, claiming that his conduct did not violate the CFAA. Before trial, the court dismissed the CFAA allegations for failure to state a claim.[50] IAC appealed.

The Seventh Circuit reversed, concluding that when Citrin breached his duty of loyalty, this terminated his agency relationship—and from that moment on, he lacked authorization to access IAC's information.[51] Under the Seventh Circuit's interpretation in *Citrin*, nearly any employee who intentionally misappropriates company information—trade secret or otherwise—would have terminated his or her agency relationship. From that moment on, the employee would be acting without authorization and committing a federal crime. The Fifth and Eleventh Circuits adopted similar rulings criminalizing violations of use restrictions.[52] A leading California practice guide even recommended that plaintiffs who wanted to bring trade secrets actions in federal court could do so by alleging CFAA violations.[53]

The Ninth Circuit weighed in to the contrary in *LVRC Holdings v. Brekka* and twice in *United States v. Nosal*. In *Brekka*—a civil case—LVRC sued former employee Christopher Brekka and others for accessing proprietary information for personal gain while employed by LRVC as well as after the end of his employment.[54] Brekka won summary judgment at the trial court, which the Ninth Circuit affirmed. LRVC appealed, asserting that its case was analogous to *Citrin*.[55]

49. *Id.* at 419.

50. *Id.* at 418, 421. Judge Anderson of the Northern District of Illinois also closed the case because no supplemental claim conferred federal jurisdiction. *Id.*

51. *Id.* at 420 (Posner, J., writing for the majority, joined by Williams, J. and Sykes, J.). *Id.* at 418.

52. *See* United States v. John, 597 F.3d 263 (5th Cir. 2010); United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010).

53. Lowell Anderson et al., *Litigation Issues*, *in* TRADE SECRETS PRACTICE IN CALIFORNIA § 11.11 (2d ed. Supp. 2016) ("One strategy for plaintiffs that prefer having their trade secrets claims hears in federal court is to plead a cause of action for violation of the Computer Fraud and Abuse Act (CFAA) (18 USC § 1030).").

54. LVRC Holdings, LLC v. Brekka, 581 F.3d 1127, 1132 (9th Cir. 2009). While LVRC is the first name in the caption and therefore the ordinary short name, the case is typically referred to as *Brekka*.

55. *Id.* at 1130–1133 ("because Brekka accessed the company computer and obtained LVRC's confidential information to further his own personal interests, rather than the interests of LVRC, such access was 'without authorization' for purposes of" the CFAA). Judge Grace of the District of Nevada granted the motion for summary judgment. *Id.*

The Ninth Circuit explained that "'authorization' depends on actions taken by the employer."[56] The court concluded that where a person's job requires use of a computer, there cannot be an *access without authorization* violation.[57]

The Ninth Circuit, *en banc*, expanded on this view in *United States v. Nosal* ("*Nosal I*").[58] The United States had charged David Nosal with several violations of the CFAA and other federal criminal statutes for his alleged misappropriation from his former employer, the executive search firm Korn Ferry. On a pretrial motion, the court struck claims concerning Korn Ferry employees who, during their employment, obtained information for Nosal's work.[59] The United States appealed, and the Ninth Circuit entertained the appeal of the dismissed claims only.[60] The panel reversed, but the Ninth Circuit *en banc* granted review.

The Ninth Circuit, *en banc*, reversed the panel and affirmed the District Court.[61] In a colorful opinion, Judge Kozinski curbed the extent of the CFAA, restricting it to wrongful access, not misuse of information.[62] As the court explained, "that the phrase 'exceeds authorized access' in the CFAA . . . is limited to violations of restrictions on access to information, and not restrictions on its use."[63] Put another way, the CFAA only criminalizes how you obtain information, not what you do with it once you have it. In a less colorful but more focused opinion, the Fourth Circuit adopted a similar rule.[64] The Sec-

56. *Id.* at 1135 (Ikuta, J. writing for the majority, and joined by McKeown, J., and Selna, J., United States District Judge for the Central District of California, sitting by designation). *Id.* at 1127.

57. *Id.* at 1133. The same is true for an *exceeds authorized access* violation — there can be no such thing when the person regularly accessed the files in question as part of his or her job. *Id.* at 1135 n. 7. Although the court also affirmed the dismissal of claims based on post-employment access, it did so on the basis that there was no evidence of such conduct. *See id.* at 1136–37 (granting summary judgment because there was no material dispute of fact concerning lack of post-termination access).

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

59. *Id.* at 856. The court denied Nosal's initial motion, but reconsidered after the Ninth Circuit published *Brekka*. Judge Patel of the Northern District of California then granted Nosal's motion in part. *Id.*

60. *Id.* (citing 18 U.S.C. § 3731, United States v. Russell, 804 F.2d 571, 573 (9th Cir.1986) (explaining jurisdiction for interlocutory review of dismissed claims)).

61. *Id.* at 864.

62. *Id.* at 855. Judge Kozinski, writing for the majority, was joined by Judges Pregerson, McKeown, Wardlaw, Gould, Paez, Clifton, Bybee, and Murgia. Judge Silverman dissented, joined by Judge Tallman. *Id.*

63. *Id.* at 863–64.

64. WEC Carolina Energy Solutions, LLC v. Miller, 687 F.3d 199, 204 (4th Cir. 2012).

ond Circuit recently adopted the same interpretation as the Ninth and Fourth circuits, albeit in addressing a different provision.[65]

A jury convicted Nosal on the remaining felony charges, namely that his co-conspirators used the working password of a current employee to access the system—with that employee's consent but without that employee carrying out the access.[66] Affirming the conviction and sentence, the Ninth Circuit clarified that the term "without authorization" is "an unambiguous, non-technical term that, given its plain and ordinary meaning, means accessing a protected computer without permission."[67] Relying on *Brekka*'s holding that when "a person uses a computer 'without authorization' under §§ 1030(a)(2) and (4). . . when the employer has rescinded permission to access the computer and the defendant uses the computer anyway," as well as a textual analysis of the word "authorization," the "*Nosal II*" court held that the term "without authorization" is given its "ordinary meaning"[68]: "an unambiguous, non-technical term that, given its plain and ordinary meaning, means accessing a protected computer without permission."[69]

D. The Ninth Circuit Stumbled into a Circuit Split on *Mens Rea*

While the Ninth Circuit was aware it was creating a circuit split on the extent of wrongful conduct, and discussed that split,[70] the Ninth

65. United States v. Valle, 807 F.3d 508, 527 (2d Cir. 2015). *Valle* concerned subsection (a)(2)(B), the provision concerning unauthorized access to "information from any department or agency of the United States." *Id. Valle* also attracted attention as the notorious "cannibal cop" case. *Id.* at 512.

66. *Id.* at 856. Judge Chen, having replaced Judge Patel due to her retirement, sentenced Nosal to a year and a day in prison.

67. United States v. Nosal, 828 F.3d 865, 868 (9th Cir. 2016) (*Nosal II*).

68. *Id.* at 875.

69. *Id.* at 868. Notably, Judge McKeown, who was part of the *Nosal I en banc* majority and wrote *Nosal II*, foreshadowed the *Nosal II* decision during the *en banc* oral argument. Ted Sampsell-Jones, representing Nosal, attempted to distinguish the charges on appeal in *Nosal II* from the charges on appeal in 2011:

> Mr. Sampsell-Jones: I don't think that's quite the same as picking a lock or stealing.
>
> Judge McKeown: Well the one who's left, has a key that he or she didn't, quote, turn in, so to speak.
>
> Mr. Sampsell-Jones: No the one who's left doesn't have a key anymore. The one who has left gets the key consensually from the one who is still there.
>
> Judge McKeown: That's called hacking.

Oral Argument, *Nosal I*, 676 F.3d 854, at 46:53–47:10, available at http://www.ca9.uscourts.gov/media/view_video.php?pk_vid=0000006176 [https://perma.cc/C65S-M7JX].

70. *Nosal I*, 676 F.3d 854, 863–64.

Circuit only briefly addressed the *mens rea* requirement. As part of its analysis, although the United States charged Nosal with violation of 18 U.S.C. §1030(a)(4)—an *intent to defraud* provision—the Ninth Circuit concluded that it must consider multiple provisions.[71] Because the same terms must have the same meaning throughout a statute,[72] the Ninth Circuit focused on the narrowest provision in the CFAA. That provision, 18 U.S.C. §1030(a)(2)(C), confers misdemeanor liability on any person who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer."

In *Nosal*, the Ninth Circuit, *en banc*, announced "the broadest provision is subsection 1030(a)(2)(C), which makes it a crime to exceed authorized access of a computer connected to the Internet without any culpable intent."[73] This statement is not mere dicta; the *Nosal* court adopted its narrow measure of what actions violate the CFAA because, in the court's estimation, the intent requirement did little to protect defendants.[74]

When CFAA defendants invoke *Nosal* to limit the scope of wrongful conduct—*which Defendants do*—they must accept the burden of the *Nosal* court's analysis concerning intent because those analyses are interdependent. And without this conclusion, the most colorful segment of Judge Kozinski's opinion would need to be qualified by a digression about *mens rea*. The comment that a dishonest user of eHarmony might end up in prison is not so compelling when followed by the caveat *if the defendant knew that he was not supposed to err in his flattering personal descriptions and did so anyway.*

71. *Id.* at 859.

72. *Id.* (citing Powerex Corp. v. Reliant Energy Servs., Inc., 551 U.S. 224, 232 (2007)).

73. *Id.*

74. *See id.* at 858–59. A recently published article by Department of Justice attorney William Hall suggests that the *parade of horribles* from *Nosal I* was inaccurate hyperbole because a prosecutor would have to prove that the defendant knew the actions were unauthorized. 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, 1531 (2016). The article characterizes the *Nosal I* decision as "leaving out the 'intent[ional]' requirement when discussing 18 U.S.C. § 1030(a)(2)(C)." *Id.* at 1531 n.48. Hall's position is consistent with official Department of Justice statements, but not with the *Nosal I* opinion. Hall fails to mention that Nosal asked the Ninth Circuit to reject the Department of Justice's preferred interpretation of the intent requirement, and the Ninth Circuit did just that. Hall's reference to the Ninth Circuit Model Jury Instructions is similarly unconvincing; the jury instructions simply parrot the statute. NINTH CIRCUIT COMM. ON MODEL CRIMINAL JURY INSTRUCTIONS, MANUAL OF MODEL CRIMINAL JURY INSTRUCTIONS FOR THE DISTRICT COURTS OF THE NINTH CIRCUIT, 8.97 Obtaining Information by Computer—"Protected" Computer (18 U.S.C. § 1030(a)(2)(A) and (B)) (2010) (updated 9/2016).

This, too, was not an invention by the court; it was briefed by Nosal, the United States, and the Electronic Frontier Foundation ("EFF") in their papers supporting and opposing *en banc* review.[75] But it was Nosal, not the Justice Department, who asked for the narrow reading of the *mens rea* requirement. This is no error; the United States Department of Justice argued for intent applying to lack of authorization,[76] and the attorney for David Nosal, a criminal defendant facing jail time,[77] and arguably amicus EFF,[78] argued that there is, in effect, no *mens rea* requirement. Go figure.

75. *See infra* notes 76–78.

76. *See* Opposition to Petition for Rehearing En Banc, United States v. Nosal, 9th Cir. Case No. 10-10038, Dkt. No. 44, at 15 (July 20, 2011) ("In the alternative, Nosal argues that en banc review is necessary to clarify the panel's statement that an employee must know about the employer's limitations on authorization in order to be liable for 'exceeding authorized access' . . . . In any event, there is nothing novel about the panel's recognition that the CFAA imposes liability only on employees who knowingly or?intentionally exceed authorized access, notwithstanding Nosal's claim that the panel's statement about knowledge 'created a new mens rea element.'").?This position is consistent with the Justice Department's manual (Scott Eltringham, ed., Executive Office for U.S. Attorneys (EOUSA): Computer Crime and Intellectual Property Section Criminal Division, *Prosecuting Computer Crimes*, EOUSA (2d ed. 2010), (Jan. 14, 2015), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf [https://perma.cc/X22S-7A84]. The manual explains that "[i]n 1986, Congress changed the intent standard in this section from 'knowingly' to 'intentionally' in order to emphasize that 'intentional acts of unauthorized access—rather than mistaken, inadvertent, or careless ones— are precisely what the Committee intends to proscribe.'" *Id.* at 17 (citing S. Rep. No. 432, 99th Cong., 2d Sess., reprinted in 1986 U.S.C.C.A.N. 2479, 2483.).

77. *See* Petition for Rehearing En Banc, United States v. Nosal, 9th Cir. Case No. 10-10038, Dkt. No. 37, at 15 (June 13, 2011) ("The majority thus apparently held that a defendant's knowledge of an employer's limitations is essential—that knowledge is an essential element of the offense. The majority, in other words, created a new mens rea element. That holding is problematical . . ."). Nosal's position makes sense as a single criminal defendant. Nosal is charged under a different provision that requires fraudulent intent, this discussion is, for him, academic. So far, it's unusual, but it makes sense. For both Nosal and the United States, the briefs track with the oral argument. *See Recording for case United States v. Nosal*, U.S. COURTS FOR THE NINTH CIRCUIT (Dec. 15, 2011), http://www.ca9.uscourts.gov/media/view_video.php?pk_vid=0000006176. EFF was not afforded time at argument.

78. EFF appears to take for granted that the interpretation sought by Nosal is correct. *See* Brief of Amicus Curiae Electronic Frontier Foundation in Support of Defendant-Appellant's Petition for Rehearing En Banc, United States v. Nosal, 9th Cir. Case No. 10-10038, Dkt. No. 43, at 5 (June 23, 2011) ("Section 1030(a)(2)(C) has no intent requirement aside from 'intentionally accessing a computer without authorization or exceed[ing] authorized access[.]' Thus, the majority [made] a criminal out of any employee who might use her work computer for personal use in violation of her employer's computer policy." (citations omitted)). Unlike Nosal, EFF indicates that it believes this interpretation—one that EFF finds undesirable for policy reasons— is consistent with the panel opinion. *Id.* at 17 ("If the panel's opinion becomes the law of this circuit, then CFAA liability under § 1030(a)(2)(C) may extend . . . to the scores of individuals who never read a website's terms of service and *unknowingly* have become federal criminals." (emphasis added)).

The narrow reading of the CFAA *mens rea* requirement in *Nosal*, if taken at face value, is a poor interpretation that contradicts earlier Ninth Circuit precedent. In *United States v. Sablan*,[79] the Ninth Circuit adopted the Second Circuit's ruling on *mens rea* from *Morris*.[80] *Sablan* has been followed by district courts in the Ninth Circuit before the *Nosal* decision.[81]

E. Recent Cases Have Not Shed Light on *Mens Rea*

The Ninth Circuit has recently issued decisions on two CFAA cases: *Facebook v. Vachani*[82] and *Nosal II*.[83] Neither case has resulted in insightful development of the *mens rea* requirement under the broadest provision: subsection (a)(2)(C). *Vachani* held that a defendant who, with the permission of Facebook users, but without the permission of Facebook, continued to access Facebook user accounts and computers "without authorization."[84] While the Ninth Circuit commented on Vachani and Power's knowledge and intent, the court did not explain how to interpret the intent requirement. *Nosal II*, explained in greater detail above, held that a person, who does not have authorization to access a computer, but nevertheless utilizes the password belonging to a person who is authorized to access a computer, accesses the computer "without authorization."[85] In tandem with its denial of *en banc* review, the Ninth Circuit issued a revised opinion emphasizing that, under subsection (a)(4), the *mens rea* requirement of "intent to defraud" language coupled together with an unequivocal revocation of access prevents the "parade of hypotheticals by Nosal and amici."[86] Unlike in *Nosal I*, the court in *Nosal II* declined to explain how its interpretation would apply in cases brought under subsection (a)(2)(C).

79. United States v. Sablan, 92 F.3d 865, 868 (9th Cir. 1996).

80. United States v. Morris, 928 F.2d 504 (2d Cir. 1991).

81. *See, e.g.*, United States v. Drew, 259 F.R.D. 449, 467 (C.D. Cal. 2009).

82. Facebook v. Vachani, 828 F.3d 1068 (9th Cir. 2016). This case was captioned *Facebook v. Power Ventures* at the trial level (Mr. Vachani and his company Power Ventures are co-defendants). This Article adopts that naming convention to clearly distinguish between the trial and appellate rulings, and refers to the trial court decisions in sequence by roman numerals.

83. *Nosal II*, 828 F.3d 865 (9th Cir. 2016).

84. *Vachani*, 828 F.3d at 1078.

85. *Nosal II*, 828 F.3d at 875.

86. *Id.* at 877.

The Supreme Court has yet to grant certiorari in any case concerning the interpretation of the CFAA.[87] The only CFAA case to reach the Court, *Musacchio v. United States*,[88] arises from a CFAA prosecution. However, the only questions before the Court were: (1) whether sufficiency of evidence is measured against an erroneous jury instruction, and (2) whether the statute of limitations may be raised on appeal.[89] These issues did not interpret the substance of the CFAA. While the justices made interesting comments concerning culpable conduct—notably Justice Alito suggested that the terms *without authorization* and *exceeds authorized access* may be intentionally redundant—the oral argument did not address the intent requirements.[90]

II. Laboratories of Democracy: State Experimentation in Computer Crime Law Treatment at the State Level

While federal courts receive most of the attention surrounding computer fraud laws, it is often overlooked that most states also have computer fraud laws. This section will first briefly summarize which states have a private right of action for violation of its computer fraud laws—a necessity for practitioners in private practice.

We then explore how state law claims, raised on supplemental jurisdiction in civil cases alongside federal question CFAA claims, provide a valuable natural experiment concerning the technical access barrier rule. This rule requires that a prosecutor or plaintiff prove lack of authorization by showing that a defendant has circumvented a

87. The Supreme Court will review two petitions for certiorari in 2017. Defendants Power and Vachani jointly petitioned for certiorari on a CFAA question. Petition for Writ of Certiorari at i, Power Ventures et al. v. Facebook (No. 16-1105) (Mar. 9, 2017). Nosal applied for and obtained an extension of time seeking certiorari. Docket, Nosal v. United States, No. 16A840, *available at* https://www.supremecourt.gov/search.aspx?filename=/docketfiles/16a840.htm [https://perma.cc/9JCV-68GW]. The docket also indicates that Nosal retained former solicitor general, Neal Katyal, as counsel. *Id.*

88. Musacchio v. United States, 136 S. Ct. 709, 714, 717 (2016).

89. Three other cases include references to the CFAA: Nijhawan v. Holder, 557 U.S. 29, 39 (2009), refers to the CFAA in a list of federal fraud statutes to assist in interpreting the term "aggravated felony" within the meaning of federal immigration law; Jones v. Bock, 549 U.S. 199, 220 (2007), considered the CFAA when interpreting statute of limitations rules for prisoner litigation; and in TRW Inc. v. Andrews, 534 U.S. 19, 38 (2001), Justice Scalia's concurring opinion referred to the CFAA when analyzing the statute of limitations in the Fair Credit Reporting Act.

90. Oral Argument, Musacchio v. United States, 136 S. Ct. 709 ___(2016) (No. 14-1095), https://www.oyez.org/cases/2015/14-1095 [https://perma.cc/6PBB-89UB]; *see also* WEC Carolina Energy Solutions, LLC v. Miller, 687 F.3d 199, 204 (4th Cir. 2012) (citing Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 419 (7th Cir. 2006)) ("Recognizing that the distinction between these terms is arguably minute.").

technical barrier—such as a password—set up to prevent unauthorized entrance. We argue that such a requirement is inconsistent with the law. We agree with proponents that if a defendant was determined enough to circumvent technical barriers, that may provide good evidence that the defendant had requisite knowledge that they did not have permission to access the information in the first place.[91] However, we contend that such circumvention, while perhaps sufficient to prove intent, is not necessary to prove lack of authorization.

We focus on California because of the unique natural experiment that occurred. We survey outcomes of civil suits with plaintiffs asserting claims under both the CFAA, which does not require proof of circumventing a technical barrier, and California's CDAFA, which does. Finally, we discuss the seminal California state court case of *People v. Childs*, showing that the natural experiment resulted from a misinterpretation of state law, and then look at similar cases in other jurisdictions.

A. States Consistently Enact Computer Hacking Laws, but Do Not Uniformly Enact Private Rights of Action

While federal courts addressed the CFAA, state legislatures did not sit on the sidelines of the computer fraud debate. All fifty states enacted some form of a computer crime law that roughly emulates the CFAA.[92] Interestingly, only nineteen states provide a civil right of ac-

91. Facebook, Inc. v. Power Ventures, Inc., No. 08-5780, 2010 WL 3291750, at *11 (N.D. Cal. July 20, 2010) (*Power Ventures I*).

92. *See* ALA. CODE §§ 13A-8-112, 13A-8-113 (2012) (Alabama); ALASKA STAT. § 11.46.740 (1984) (Alaska); ARIZ. REV. STAT. ANN. §§ 13-2316 (1978), 13-2316.01 (2000), 13-2316.02 (2000) (Arizona); ARK. CODE ANN. §§ 5-41-101 (1987), 5-41-206 (2001) (Arkansas); CAL. PENAL CODE § 502 (West 1987) (California); COLO. REV. STAT. ANN. §§ 18-5.5-101, 18-5.5-102 (West 1979) (Colorado); CONN. GEN. STAT. ANN. §§ 53a-250–261 (West 1984) (Connecticut); DEL. CODE ANN. TIT. 11, §§ 931–941 (West 1984) (Delaware); FLA. STAT. §§ 815.01–815.07 (1978), 668.801–668.805 (2015) (Florida); GA. CODE ANN. §§ 16-9-90–16-9-94 (West 1991), 16-9-150–16-9-157 (West 2005) (Georgia); HAWAII REV. STAT. §§ 708-890– 708-895.7 (1992) (Hawaii); IDAHO CODE ANN. §§18-2201, 18-2202 (1984) (Idaho); 720 ILL. COMP. STAT. ANN. §§ 5/17-50 to -55 (1987) (Illinois); IND. CODE §§ 35-43-1-4 (1986), 35-43-2-3 (1986) (Indiana); IOWA CODE § 716.6B (2000) (Iowa); KAN. STAT. ANN. § 21-5839 (2010) (Kansas); KY. REV. STAT. ANN. §§ 434.840 (1984), 434.845 (1984), 434.850 (1984), 434.851 (2002), 434.853 (2002), 434.855 (2002), 434.860 (2002) (Kentucky); LA. REV. STAT. ANN. §§ 14:73.1–14:73.8 (1984) (Louisiana); ME. REV. STAT. ANN. tit. 17-A, §§ 431–437 (1989) (Maine); MD. CODE ANN., CRIM. LAW § 7-302 (2002) (Maryland); MASS. GEN. LAWS ANN. ch. 266, § 33A (West 1994) (Massachusetts); MICH. COMP. LAWS §§ 752.791, 752.792, 752.793, 752.794, 752.795, 752.796, 752.797 (1996) (Michigan); MINN. STAT. §§ 609.87–609.893 (1982) (Minnesota); MISS. CODE ANN. §§ 97-45-1–97-45-33 (West 1985) (Mississippi); MO. REV. STAT. §§ 537.525 (1987), 569.095 (1982), 569.097 (1982), 569.099 (1982) (Missouri); MONT. CODE ANN. §§ 45-2-101 (1973), 45-6-310 (1981),

tion: Arkansas,[93] California,[94] Delaware,[95] Florida,[96] Georgia,[97] Illinois,[98] Iowa,[99] Missouri,[100] Nevada,[101] North Dakota,[102] Pennsylvania,[103] Rhode Island,[104] South Carolina,[105] Tennessee,[106] Vermont,[107] Virginia,[108] West Virginia,[109] Wisconsin,[110] and Wyoming.[111]

California, home to the Silicon Valley companies involved in frequent CFAA litigation, did not enable civil actions until 2000—and only then passed an amendment sponsored by eBay.[112] But once enacted, California provided additional benefits for plaintiffs, most nota-

45-6-311 (1981) (Montana); NEB. REV. STAT. §§ 28-1341–28-1348 (1985) (Nebraska); NEV. REV. STAT. §§ 205.473 to 205.513 (1983) (Nevada); N.H. REV. STAT. ANN. §§ 638:16, 638:17, 638:18, 638:19 (1985) (New Hampshire); N.J. REV. STAT. §§ 2C:20-2 (1978), 2C:20-23–34 (1984) (New Jersey); N.M. STAT. ANN. §§ 30-45-1 to 30-45-7 (1989) (New Mexico); N.Y. PENAL LAW §§ 156.00–156.50 (McKinney 1986) (New York); N.C. GEN. STAT. §§ 14-453–14-458 (1979) (North Carolina); N.D. CENT. CODE § 12.1-06.1-08 (1983) (North Dakota); OHIO REV. CODE ANN. §§ 2909.01, 2909.04, 2909.07(A)(6), 2913.01–2913.04 (1972) (Ohio); OKLA. STAT. tit. 21, §§ 1951–1959 (1984) (Oklahoma); OR. REV. STAT. § 164.377 (1985) (Oregon); 18 PA. CONS. STAT. §§ 5741–5749 (1988) (Pennsylvania); R.I. GEN. LAWS §§ 11-52-1–11-52-8 (1979) (Rhode Island); S.C. CODE ANN. §§ 16-16-1–16-16-40 (1984) (South Carolina); S.D. CODIFIED LAWS §§ 43-43B-1–43-43B-8 (1982) (South Dakota); TENN. CODE ANN. §§ 39-14-601–39-14-605 (1989) (Tennessee); TEX. PENAL CODE ANN. § 33.02 (1985) (Texas); UTAH CODE ANN. §§ 76-6-702–76-6-705 (West 1986) (Utah); VT. STAT. ANN. tit. 13, §§ 4101–4107 (1999) (Vermont); VA. CODE ANN. §§ 18.2-152.1–18.2-152.15 (1984), 19.2-249.2 (2005) (Virginia); WASH. REV. CODE §§ 9A.52.110, 9A.52.120, 9A.52.130 (1984) (Washington); W. VA. CODE §§ 61-3C-3–61-3C-21 (1989) (West Virginia); WIS. STAT. § 943.70 (1981) (Wisconsin); and WYO. STAT. ANN. §§ 6-3-501–6-3-506 (1982), 40-25-101 (2014) (Wyoming) (All dates indicate the year of original enactment; statutes may have been subsequently altered or repealed.).

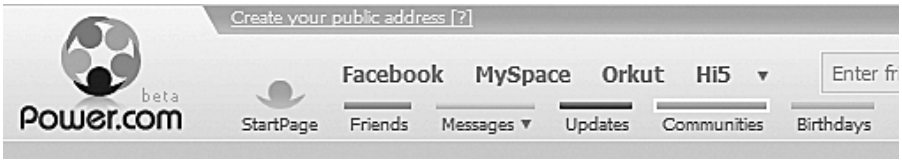
93. ARK. CODE § 5-41-106(a)(1) (1987).
94. CAL. PENAL CODE § 502(e)(1) (1987).
95. DEL. CODE TIT. 11, § 941(a) (1984).
96. FLA. STAT. § 668.803 (2015).
97. GA. CODE § 16-9-93(g) (1991).
98. ILL. COMP. STAT. § 5/17-50(c) (1987).
99. IOWA CODE § 716.6B(2) (2000).
100. MO. REV. STAT. § 537.525(1) (1987).
101. NEV. REV. STAT. § 205.511 (1999).
102. N.D. CENT. CODE § 12.1-06.1-08(3) (1983).
103. 18 PA. STAT. § 5747 (1988).
104. R.I. GEN. LAWS § 11-52-6 (1989).
105. S.C. CODE § 16-16-25 (2002).
106. TENN. CODE § 39-14-604 (2003).
107. VT. STAT. ANN. TIT. 13, § 4106 (1999).
108. VA. CODE § 18.2-152.12 (1984).
109. W. VA. CODE § 61-3C-16 (1989).
110. WIS. STAT. § 943.70(5) (1981).
111. WYO. STAT. § 40-25-101 (2014).
112. Civil Liability and Punitive Damages for Disruption of Computer Systems, AB 2727, Reg. Sess. (Cal. 2000), ftp://leginfo.public.ca.gov/pub/99-00/bill/asm/ab_2701-2750/ab_2727_cfa_20000809_103544_sen_comm.html [https://perma.cc/GRY6-N4N7].

bly punitive damages and attorneys' fees.[113] Presumably because of these remedies, CDAFA claims often accompany civil CFAA claims in federal court.

B. The California Federal Courts' Experiment with a *Technical Access Barrier* Rule

1. Origin of the Rule: *Facebook v. Power Ventures*

In late 2008, a website called Power.com offered to aggregate multiple social media websites into one platform.[114] Power users entered their username and password for other sites, and Power accessed those sites and displayed the content in a single interface, as shown here:



Facebook, which had recently overtaken MySpace to become the largest social networking site, demanded that Power cease accessing Facebook.[115] At around the same time, Power sent out a launch promotion that purportedly caused a large volume of email to be sent from @facebookmail.com email addresses.[116] Facebook sued under the CFAA, CDAFA, and CAN-SPAM Act.[117] On an early motion, the court explained that to prove a CDAFA violation, the plaintiff would have to prove that a defendant circumvented a technical or code-based barrier.[118] Because the motion concerned only the CDAFA claims,[119] the court never considered whether the technical barrier requirement would also apply to the federal CFAA.

113. CAL. PENAL CODE § 502(e)(2), (e)(4) (2016) (subsections that provide attorney's fees and punitive damages).

114. Facebook, Inc. v. Power Ventures, Inc., 844 F. Supp. 2d 1025, 1027–1028 (N.D. Cal. 2012) (*Power Ventures II*).

115. *Id.* at 1028.

116. *Id.*

117. *Power Ventures I,* No. 08-5780, 2010 WL 3291750, at *1 (N.D. Cal. July 20, 2010).

118. *Id.* at *11.

119. *Id.* Facebook, as plaintiff, moved for judgment on the pleadings. *Id.* at *11 (quoting allegations from Complaint admitted in Answer). Although Facebook pled jurisdiction based on federal question for its CFAA claim, Facebook's motion for judgment on the pleadings concerned only the CDAFA. *Id.* at *1.

The court explained that "interpreting the statutory phrase 'without permission' (the state-law analog to 'without authorization') in a manner that imposes liability for a violation of a term of use or receipt of a cease and desist letter would create a constitutionally untenable situation."[120] The court explained its rule as follows:

> [A] distinction can be made between access that violates a term of use and access that circumvents technical or code-based barriers. . . . Limiting criminal liability to circumstances in which a user gains access to a computer, computer network, or website to which access was restricted through technological means eliminates any constitutional notice concerns, since a person applying the technical skill necessary to overcome such a barrier will almost always understand that any access gained through such action is unauthorized. Thus, the Court finds that accessing or using a computer, computer network, or website in a manner that overcomes technical or code-based barriers is "without permission," and may subject a user to liability under Section 502.[121]

Although district court rulings are not binding, they are readily available, and the requirement that CDAFA claims allege and prove circumvention of a technical or code-based access barrier became the majority rule in the Northern District of California.[122]

In a pattern the authors found across numerous cases,[123] the imposition of a *technical access barrier* rule did not change the outcome of the case. Facebook eventually prevailed on summary judgment, proving that defendants admittedly "implemented a system that would be immune to such technical barriers."[124] The Ninth Circuit affirmed

120. *Id.* at *11.

121. *Id.* Judge Ware further explained that the admission concerning technical barriers was insufficient to find liability and denied the motion. *Id.* Professor Kerr, who had suggested a technical barrier rule in his 2003 article commented favorably on this ruling. *See* Orin Kerr, *District Court Adopts "Technical Barriers" Approach to California Computer Crime Law*, THE VOLOKH CONSPIRACY (Aug. 25, 2010), http://volokh.com/2010/08/25/district-court-adopts-technical-barriers-approach-to-california-computer-crime-law/, [https://perma.cc/DTB6-XFPW].

122. *See, e.g.*, Top Agent Network, Inc. v. Zillow, Inc., No. 14-cv-04769-RS, 2015 U.S. Dist. LEXIS 161556, at *19 (N.D. Cal. Apr. 13, 2015); Enki Corp. v. Freedman, No. 5:13-cv-02201-PSG, 2014 U.S. Dist. LEXIS 9169, at *10 (N.D. Cal. Jan. 23, 2014); In re Google Android Consumer Privacy Litig., No. 11-MD-02264 JSW, 2013 U.S. Dist. LEXIS 42724, at *37 (N.D. Cal. Mar. 26, 2013); Hernandez v. Path, Inc., No. 12-CV-01515 YGR, 2012 U.S. Dist. LEXIS 151035, at *14 (N.D. Cal. Oct. 17, 2012); In re iPhone Application Litig., No. 11-MD-02250-LHK, 2011 U.S. Dist. LEXIS 106865, at *40 (N.D. Cal. Sept. 20, 2011). Because the Northern District of California includes the headquarters of Google, Apple, Facebook, Yahoo, HP, Intel, Cisco, Oracle, and numerous other companies, it is no surprise that a large share of CFAA and CDAFA cases are filed within the District.

123. *See* Part II.B.2, *infra*.

124. *Power Ventures II*, 844 F. Supp. 2d 1025, 1038 (N.D. Cal. 2012) (citing Vachani's deposition testimony). The court concluded that Facebook's IP-blocking and Power's use

Facebook's CFAA claim, explaining that "after receiving the cease and desist letter from Facebook, Power intentionally accessed Facebook's computers knowing that it was not authorized to do so, making Power liable under the CFAA."[125] Because Facebook proved circumvention of a technical access barrier, the Ninth Circuit did not address whether such proof was necessary.[126] As a result, the *Power Ventures* order imposing a technical access barrier for CDAFA claims has not been considered by a federal appellate court.[127]

Briefing by *amicus curiae* Electronic Frontier Foundation illustrated the present confusion concerning the *mens rea* requirement in the Ninth Circuit. EFF emphasized the concern that users often find technology confusing and complicating, and may inadvertently circumvent IP-blocking technologies.[128] In EFF's own words, a user may have "no way of knowing why he is being denied access, or whether that denial was due to a technical problem or an intentional block."[129] This Article does not contend that EFF is incorrect about the technology. But, regarding EFF's hypothetical user who did not know why he or she was blocked, that user would not have culpable intent—at least under the *Morris* rule.[130]

---

of different IP addresses qualified as circumvention of a technical or code-based barrier, noting that the statute did not require Power to take additional steps because its initial software was designed to circumvent technical barriers. *Id.* While not the subject of this Article, Facebook's CAN-SPAM Act claim was the source of most of its purported damages. Facebook, Inc. v. Power Ventures, Inc., Case No.: 08-CV-5780-LHK, at *33 (N.D. Cal. Sept. 25, 2013) (*Power Ventures III*) (Facebook "will be awarded $3,031,350 ($50 for each of the estimated 60,627 spam messages sent) in CAN-SPAM damages."). This award, affirmed by Judge Koh after reassignment, was reversed on appeal. Facebook v.Vachani, 828 F.3d 1068, 1072, 1075 (9th Cir. 2016) (Graber, J.). Judge Graber was joined by Judges Wardlaw and Murgia.

125. *Vachani*, 828 F.3d 1079. The opinion does not neatly distinguish the intent requirement from the lack of authorization—a point noted by Vachani seeking *en banc* review. *See* Petition for Panel Rehearing and Rehearing En Banc at 7–8, Facebook, Inc. v. Vachani. 9th Cir. Case No. 13-17102, Dkt. No. 85 (9th Cir. Filed Aug. 9, 2016).

126. *Vachani*, 828 F.3d 1068

127. While not addressing *Power Ventures*, the Ninth Circuit's decision in *United States v. Christensen* rejected a defendant's contention that the CDAFA "defines 'access' in terms redolent of hacking . . . ." 801 F.3d 971, 994 (9th Cir. 2015). In support, the Ninth Circuit identified examples of CDAFA violations that did not require circumvention of a technological access barrier. *Id.* (discussing Gilbert v. City of Sunnyvale, 130 Cal.App.4th 1264, 1281 (2005) (police officer "accessed a police database") and People v. Hawkins, 98 Cal.App.4th 1428, 1437 (2002) ("copy of his employer's proprietary source code")).

128. Brief of Amicus Curiae Electronic Frontier Foundation in Support of Defendant-Appellants, Facebook, Inc. v. Vachani, 9th Cir. Case No. 13-17154, Dkt. No. 22, p. 9. (Mar. 10, 2014).

129. *Id.*

130. A review of state court decisions reveals that the CDAFA's intent requirement that a defendant act knowingly applies to lack of permission—comparable to the *Morris* intent

2. Analysis of the Full Set of Court Decisions Applying the Technical Barrier Rule

After the Northern District of California announced the *technical access barrier* rule in *Power Ventures*, other judges in the district began applying the rule. For CDAFA cases, the technical or code-based barrier requirement became the majority rule in the Northern District and has been adopted in other districts as well. However, because of a procedural quirk, *Power Ventures* did not apply the same rule to the federal CFAA, and to date no court has done so.

Based on the authors' research performed in 2016, twenty-two cases have discussed a technical or code-based barrier rule in relation to the CDAFA.[131] Of those cases, four rejected a technical barrier rule at least for one or more offenses under the CDAFA,[132] two declined to

rule, not the *Nosal* intent rule. People v. Hawkins, 98 Cal.App.4th 1428, 1439 (6th Dist. 2002). Under the California Penal Code, "[t]he word 'knowingly' imports only a knowledge that the facts exist which bring the act or omission within the provisions of this code. It does not require any knowledge of the unlawfulness of such act or omission." CAL. PENAL CODE §7, subd. (5) (Section 7 is the dictionary for the Penal Code); *see also* People v. Burns, 75 Cal. 627, 630-631 (1888).

131. The authors reviewed all cases appearing in searches for key terms on LexisNexis. Our search method first identified cases citing to California Penal Code section 502, then searched for terms including *technical and barrier, code and barrier*. The authors also looked at cases citing cases found in the initial searches. In the results, the authors excluded four cases as false positives. Three, Welenco, Inc. v. Corbell, 126 F. Supp. 3d 1154 (E.D. Cal. 2015), Capitol Audio Access, Inc. v. Umemoto, 980 F. Supp. 2d 1154, 1159 (E.D. Cal. 2013), and Mintz v. Bartelstein, 906 F. Supp. 2d 1017, 1031 (C.D. Cal. 2012), appeared in the search despite their failure to discuss or apply a technical barrier rule because they contained similar language (although *Welenco* and *Mintz* contain analysis similar to the analysis in NovelPoster v. Javitch Canfield Grp., 140 F. Supp. 3d 954, 955 (2014), rejecting a technical barrier rule). The fourth, NetApp, Inc. v. Nimble Storage, 41 F. Supp. 3d 816, 823–833 (N.D. Cal. 2014), concerned only CFAA claims, and compared the lack of a technical barrier rule under the CFAA with the *Power Ventures* rule under the CDAFA. The authors also identified three cases with two orders in the search results—for each of these cases the authors identified the principal decision on point, and excluded the following other orders from the analysis: Perkins v. LinkedIn Corp., 53 F. Supp. 3d 1222, 1238 (N.D. Cal. 2014) (order on later motion), Craigslist Inc. v. 3taps Inc., 964 F. Supp. 2d 1178 (N.D. Cal. 2013) (subsequent order on court-ordered briefing), NovelPoster v. Javitch Canfield Grp., 140 F. Supp. 3d 938, 943–51 (N.D. Cal. 2014) (prior order dismissing claim with leave to amend on other grounds). The remaining twenty-four orders are identified in the following paragraphs and footnotes.

132. *See* NovelPoster v. Javitch Canfield Grp., 140 F. Supp. 3d 954, 955, 967 (N.D. Cal. 2014); Weingand v. Harland Fin. Solutions, Inc., No. C-11-3109 EMC, 2012 U.S. Dist. LEXIS 84844, at *16 (N.D. Cal. June 19, 2012), Synopsys, Inc. v. Atoptech, Inc., No. C 13-2965 SC, 2013 U.S. Dist. LEXIS 153089, at *37–39 (N.D. Cal. Oct. 24, 2013); In re Carrier IQ, Inc., Consumer Privacy Litig., No. C-12-md-2330 EMC, 2015 U.S. Dist. LEXIS 7123, at *1101 (N.D. Cal. Jan. 21, 2015); Welenco, Inc. v. Corbell, 126 F. Supp. 3d 1154, 1170 (E.D. Cal. 2015).

decide the issue,[133] and sixteen said there was such a rule. But a closer analysis shows the rule to be less valuable for defendants than it may appear. In at least twelve of the cases, the result would likely have been the same even if there were no technical barrier rule but, instead, an access versus use distinction as applied in *Nosal*.[134] Among these cases, *Top Agent Network v. Zillow* and *Enki Corp v. Freedman* are instructive. In both cases, the courts concluded that the lack of unauthorized *access* was sufficient to dismiss the CFAA allegations under *Brekka* and *Nosal*, and then applied the different *technical barrier* rule from *Power Ventures* to dismiss the CDAFA claim.[135] Not a single case sustained allegations under the CFAA but dismissed the state-law CDAFA claim under the *technical access barrier* rule.[136]

Three of the remaining four cases are part of the *surreptitious software* cases, which concerned privacy on devices and services provided by Google, Apple, and Facebook.[137] These cases may well have

133. Craigslist Inc. v. 3Taps Inc., 942 F. Supp. 2d 962, 969–970 (N.D. Cal. 2013) (citing both *Power Ventures I & II* and *Weingand* with approval); Hernandez v. Path, Inc., 2012 U.S. Dist. LEXIS 151035, *14 (N.D. Cal. Oct. 17, 2012) (discussing *Weingand*). The court in *Hernandez* declined to discuss the issue in depth because pleadings would be insufficient given the nature of the case. In *Craigslist*, on the other hand, the court faced the issue of whether an IP block is a sufficient barrier (as it was in *Power Ventures I & II*) and whether the public nature of Craigslist made a difference (the court concluded it did not). Craigslist Inc. v. 3taps Inc., 964 F. Supp. 2d 1178, 1183–1184 (N.D. Cal. 2013).

134. *See* Sunbelt Rentals, Inc. v. Victor, 43 F. Supp. 3d 1026, 1033 (N.D. Cal. 2014) (independent grounds under *Twombly*); New Show Studios LLC v. Needle, No. 2:14-cv-01250-CAS(MRWx), 2014 U.S. Dist. LEXIS 90656, at *1 (C.D. Cal. June 30, 2014) (no allegation of access); Perkins v. LinkedIn Corp., 53 F. Supp. 3d 1190, 1219 (N.D. Cal. 2014) (no loss to plaintiff); Facebook, Inc. v. Grunin, 77 F. Supp. 3d 965, 973 (N.D. Cal. 2015) (court treats circumvention as sufficient but not necessary); Siebert v. Gene Sec. Network, No. 11-cv-01987-JST, 2013 U.S. Dist. LEXIS 149145, at *37 (N.D. Cal. Oct. 16, 2013) (no allegation that defendant lacked authorization); In re Google Inc. Cookie Placement Consumer Privacy Litig., 988 F. Supp. 2d 434, 449 (D. Del. 2013) (insufficient pleadings); Custom Packaging Supply, Inc. v. Phillips, No. 2:15-CV-04584-ODW-AGR, 2015 U.S. Dist. LEXIS 164523, at *9 (C.D. Cal. Dec 07, 2015) (no description of damage); Opperman v. Path, Inc., 87 F. Supp. 3d 1018, 1054 (N.D. Cal. 2014) (appeared there was no restriction); Integral Dev. Corp. v. Tolat, No. C 12-06575 JSW, 2013 U.S. Dist. LEXIS 153705, at *11–12 (N.D. Cal. Oct 25, 2013) (misappropriation not access case); Top Agent Network, Inc. v. Zillow, Inc., No. 3:14-cv-04769, 2015 U.S. Dist. LEXIS 161556, at *19 (N.D. Cal. Apr. 13, 2015) (same); Enki Corp. v. Freedman, No. 5:13-cv-02201-PSG, 2014 U.S. Dist. LEXIS 9169, at *10 (N.D. Cal. Jan. 23, 2014) (same).

135. *Top Agent.*, Case No. 3:14-cv-04769, at *10–11, *Enki*, 2014 U.S. Dist. LEXIS 9169, at *10.

136. In fact, the only case to suggest that such an incongruous result may be correct was NetApp, Inc. v. Nimble Storage, 41 F. Supp. 3d 816, 832–834 (N.D. Cal. 2014), a case in which the plaintiff did not bring CDAFA claims.

137. *See* In re Google Android Consumer Privacy Litig., No. 11-MD-02264 JSW, 2013 U.S. Dist. LEXIS 42724, at *37 (N.D. Cal. Mar. 26, 2013); In re iPhone Application Litig.,

had the same result, albeit through more complex analysis, because of the consent afforded by using a service or application.

The fourth case, *Flextronics v. Parametric*, concerned a computer contaminant. There, the court concluded that while some allegations did not satisfy the *technical barrier rule*, that rule operated differently with regard to subsection (c)(8) of the CDAFA.[138] The court then reasoned that while the computer contaminant must overcome a technical or code-based barrier, the introduction of the contaminant need not satisfy the same standard. Accordingly, the claim could proceed past the pleading stage.

One case that the authors coded as rejecting a technical barrier rule, *NovelPoster v. Javitch Canfield Group*, is instructive. In *NovelPoster*, the court granted a motion to dismiss with leave to amend because the plaintiff had not sufficiently alleged damage and loss.[139] In that order, the court noted that the CDAFA claim would also require circumvention of a technical barrier.[140] This presented a problem for NovelPoster because it alleged that it gave defendants administrator passwords as part of a business deal, and then defendants misused those passwords to change other passwords, locking NovelPoster's owners out of their own system and permitting defendants to snoop through NovelPoster's files. After NovelPoster amended and defendants moved to dismiss again, the court declined to enforce a technical access barrier.[141] Although the California Court of Appeal decision in *People v. Childs* compelled the court to not impose a technical barrier rule on the lockout allegation,[142] the court also sustained NovelPoster's claims under other sections of the CDAFA. Questioning the application of *Power* Ventures, Judge Orrick stated:

> NovelPoster's allegations that defendants without authorization changed the passwords to NovelPoster's online accounts, thereby preventing NovelPoster from accessing those accounts and eliminating the very technical access barriers that NovelPoster had set

No. 11-MD-02250-LHK, 2011 U.S. Dist. LEXIS 106865, at *40 (N.D. Cal. Sept. 20, 2011); In re Facebook Privacy Litig., 791 F. Supp. 2d 705, 708, 716 (N.D. Cal. 2011).

138. Flextronics Int'l, Ltd. v. Parametric Tech. Corp., No. 5:13-cv-00034-PSG, 2014 U.S. Dist. LEXIS 73354, at *14 (N.D. Cal. May 28, 2014).

139. NovelPoster v. Javitch Canfield Grp., 140 F. Supp. 3d 938, 943–51 (N.D. Cal. 2014). The authors were counsel for NovelPoster.

140. *Id.* at 950 n.8 (citing Enki Corp. v. Freedman, No. 13–cv–2201–PSG, 2014 U.S. Dist. LEXIS 9169, at *10 (N.D. Cal. Jan. 23, 2014)).

141. NovelPoster v. Javitch Canfield Grp., 140 F. Supp. 3d 954, 967 (N.D. Cal. 2014). Dorsi argued at this motion at the hearing.

142. *See infra* Part II.C. It appears that *NovelPoster* was the first federal court case where a party briefed *Childs* to a federal court.

> up to protect them, are sufficient at the pleading phase to show that defendants overcame a technical access barrier.[143]

While in theory a *technical access barrier* rule may seem like a great tool for defendants, in practice it has not worked that way. Most cases ended with the same results they would have had with an access versus use distinction, and in hard cases with compelling facts, courts found ways to allow claims to go forward.

We recognize what may be the principal criticism of our argument: if the technical barrier rule has no impact on outcomes over a reasonable sample size of cases, we should have nothing to worry about when courts adopt it. There are two principal problems with this criticism:

First, there is an unfortunately common fact pattern where a defendant excludes the victim from accessing a system—a situation we discuss further in Part II.D, *infra*. In these cases, the defendant may not have circumvented a technical or code-based barrier, but has arguably imposed or relied on one to commit the underlying offense. That courts seem to find a way around this—or consider this to be an opportune time to question technical barrier rules—provides insufficient comfort to victims. Sometimes judges might not find such a way out. Many disputes are resolved not by final judgments but by settlement. The uncertainty that a plaintiff or prosecutor might fail for lack of circumventing a technical barrier lowers their expected outcome and creates an incentive to settle for far less than justice.

Second, we ask the critic to turn the tables. What justifies this departure from the interpretation most grounded in statutory text? If courts that apply a technical barrier rule are not producing greater protection for defendants, what is the purpose of the rule? Why is their parade of hypotheticals, which have not been brought in either the civil or criminal context, a more serious concern than the lockout cases documented in this Article? We see no good answer.

C. The State Courts Fight Back: *People v. Childs*

In 2007, the City and County of San Francisco lost control of its FiberWan Network—not to an overseas hacker, but to its network administrator Terry Childs. Childs, who had done much of the development of the network, locked the city out of its own system.[144] The San Francisco District Attorney's Office prosecuted Childs for violation of

143. *NovelPoster*, 140 F. Supp. 3d 954, 967.

144. People v. Childs, 220 Cal.App.4th 1079, 1093 (1st Dist. 2013) ("During the period from July 9 through July 21, DTIS was effectively locked out of the FiberWAN network.

California Penal Code section 502(c)(5), part of the CDAFA.[145] Subsection (c)(5) makes it a crime when a person "[k]nowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network."[146] Except as otherwise stated, in the entire California Penal Code "[t]he word 'knowingly' imports only a knowledge that the facts exist which bring the act or omission within the provisions of this code. It does not require any knowledge of the unlawfulness of such act or omission."[147] The jury returned a guilty verdict, and the court denied motions to arrest judgment and for new trial.[148] Childs appealed, contending *inter alia* that he had not hacked into the system, and therefore was not liable under the CDAFA.

The California Court of Appeal affirmed the verdict.[149] Writing for a unanimous panel,[150] Justice Reardon announced "that the [California] Legislature intended for some parts of section 502, subdivision (c) to apply only to external hackers and for some parts—including subdivision (c)(5)—to apply to users who were given lawful access to the computers."[151] The California Court of Appeal rejected Childs's arguments, finding that the state made an adequate showing that Childs did not have permission to lock city government out of its own systems. The California Supreme Court denied review, and as of this writing, the CDAFA has not been interpreted by the California Supreme Court.[152]

Neither DTIS employees nor other computer experts were able to obtain administrative access to the network until Childs revealed the access codes.").

145. *Id.*

146. CAL. PENAL CODE § 502(c)(5) (2016).

147. CAL. PENAL CODE § 7(5) (2016).

148. *Childs,* 220 Cal.App.4th at1093.

149. *Id.* at 1082.

150. Justice Reardon was joined by Justices Ruvolo and Rivera. *Id.* at 1108. In California state courts, appellate judges are referred to as justices.

151. *Id.* at 1107.

152. While never interpreted, the CDAFA is mentioned in three California Supreme Court cases: In Sierra Club v. Superior Court, 57 Cal. 4th 157, 170 (2013), the California Supreme Court considered definitions in Section 502 when evaluating the definition of computer mapping software under part of California's Government Code; in People v. Davis, 18 Cal. 4th 712, 723 (1998), the Court noted that a defendant's wrongful act might have been a violation of Section 502, though he was not charged with such a violation; and in People v. Eubanks, 14 Cal. 4th 580, 584 (1996), the Court addressed a question of prosecutor's conflicts of interests, noting that the underlying charges included Section 502 but not addressing the statute because it was not at issue on appeal.

The decision in *Childs* appears to conflict with—or at least limit—the *technical access barrier* rule announced in *Power Ventures.*[153] And because *Childs* is a state court decision interpreting state law, when in conflict, *Childs* trumps *Power Ventures.*[154] While it is unclear if *Childs* marks the beginning of a trend or simply the correct reading of a subpart of a statute, it does illustrate the *lockout* scenario—an unpleasant situation for the party locked out—that has repeatedly appeared in cases arising under state computer crime statutes.

D. Lockout Cases Under State Law

The Georgia Court of Appeals encountered a similar situation and reached the same result as *Childs* in *Fugarino v. State.*[155] Fugarino was a computer programmer for a private company. After some workplace disputes, Fugarino deleted company files on the company computer, imposed password restrictions over other files and refused to share the passwords. A jury convicted Fugarino for computer trespass, O.C.G.A. § 16-9-93(b). Fugarino appealed, contesting that the state could not prove beyond a reasonable doubt that he knowingly acted "without authority."[156] Fugarino, like Childs, was an insider and did not need to circumvent any technical access barriers in order to inflict damage.

The Georgia Court of Appeals affirmed the verdict and did not impose a technical access barrier requirement. Rather, the court held that authority ran from the permissions granted by the owner of the computer network and affirmed Fugarino's conviction.[157]

This resembles the aforementioned case of *NovelPoster v. Javitch Canfield Group*, where the plaintiff hired defendants to manage online

153. NovelPoster v. Javitch Canfield Grp., 140 F. Supp. 3d 954, 966 (N.D. Cal. 2014); *but see* Welenco, Inc. v. Corbell, 126 F. Supp. 3d 1154, 1169–1170 (E.D. Cal. 2015) (recognizing *Childs* as binding and citing *NovelPoster* for the application of *Childs* to the civil context, but concluding that denial of access for only two hours was not cognizable under the CDAFA).

154. "[T]he duty of the federal court is to ascertain and apply the existing California law." Klingebiel v. Lockheed Aircraft Corp., 494 F.2d 345, 346 (9th Cir. 1974). "Decisions of the California Courts of Appeal are to be followed by a federal court where the Supreme Court of California has not spoken on the question." *Id.* When a new state court case changes or clarifies state law, federal courts are obligated to follow the new state case, even if it conflicts with prior state and federal precedent. *See, e.g.*, Quinionez v. United States, 526 F.2d 799, 799–800 (9th Cir. 1975) (applying new California contributory negligence rule from *Li v. Yellow Cab*); Haragan v. Union Oil Co., 312 F. Supp. 1392, 1396 (D. Alaska 1970) (applying strict product liability rule after adopted by Alaska Supreme Court).

155. Fugarino v. State, 531 S.E.2d 187 (Ga. Ct. App. 2000).

156. *Id.* at 270.

157. *Id.* at 189.

operations, and defendants changed passwords.[158] Although brought in federal court, substantial argument in *NovelPoster* concerned the CDAFA, which the court considered under supplemental jurisdiction. Denying a motion to dismiss by defendants Javitch and Canfield,[159] the court concluded that *Childs* contradicted, or at least limited, *Power Ventures* in the lockout context.[160]

The experiences in *Childs*, *Fugarino*, and *NovelPoster* illustrate that lockout situations are serious and computer crime statutes can be effective ways to address the lockout. While a strict *technical access barrier* rule might prevent the use of computer crime statutes in lockout situations, courts seem inclined not to apply such a strict rule.

III. Technical Access Barrier Rules Are Wishful Thinking; the Best way to Protect Defendants Is a Proper *Mens Rea* Rule

The useful lens for circumvention of technical barriers is intent, not culpable conduct. Showing circumvention of a technical barrier could be a very powerful way to illustrate culpable intent. But requiring a showing of circumvention to prove culpable conduct is inconsistent with the language as well as the purpose of the CFAA. We recognize the potential for the CFAA to be applied to an unreasonably broad set of conduct if there is not a limiting principle. In this section, we argue that the *mens rea* requirement under the CFAA should require intentional unauthorized actions, meaning that the defendant must know the facts making the act unauthorized and intentionally act anyway. Nonetheless, we acknowledge that one offense under the CFAA, subsection (a)(2)(C), may be constitutionally infirm even under our proposed intent requirement. We explain how the courts are moving in a direction where they may be forced to address the constitutionality of subsection (a)(2)(C) and offer a suggestion for how Congress could eliminate this dilemma.

A. A Technical Access Barrier Rule Would Contradict the Text and Purpose of the CFAA

Defendants seeking a *technical barrier rule* have, and will, continue to face an uphill battle. The CFAA imposes liability for actions taken without authorization. The statute does not state that it is limited to

158. *NovelPoster*, 140 F. Supp. 3d at 956.
159. Nominal defendant Javitch Canfield Group defaulted, but individuals defended.
160. *NovelPoster*, 140 F. Supp. 3d at 966.

actions that circumvent technological or code-based barriers to access. If Congress had intended to require such circumvention, it could have said so, as it has done in other statutes.[161]

A rule requiring circumvention of a technical access barrier is also incompatible with several provisions of the CFAA that criminalize activities that do not require accessing a computer. Subsection (a)(5)(A) makes it a crime to "knowingly cause[ ] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause[ ] damage without authorization, to a protected computer."[162] The absence of an access requirement is incompatible with a requirement that a defendant circumvent a technical access barrier.

Here, the same logic that constrained the CFAA in *Nosal* works to prevent further constraint by requiring circumvention of technical barriers. Once a court defines a term for the purpose of one subsection, "that definition must apply equally to the rest of the statute pursuant to the 'standard principle of statutory construction . . . that identical words and phrases within the same statute should normally be given the same meaning.'"[163] Because this Court's interpretation of "without authorization" for purposes of subsection (a)(4) would apply not only to subsection (a)(2)(C), but also to subsection (a)(5)(A), this constraint creates a tension that is potentially fatal to proposed technical barrier rules. The Ninth Circuit adopted this reasoning in *Nosal II*,[164] which is presently subject to an extension for filing a petition for a *writ of certiorari*.[165] Despite this, we expect the *technical access*

161. *See, e.g.*, 17 U.S.C. § 1201 (making it a crime to "circumvent a technological measure that effectively controls access to a work protected under" copyright law).

162. 18 U.S.C. § 1030(a)(5)(A) (2012) (emphasis added); *see also* 18 U.S.C. 1030(a)(6) & (7) (2012). Subsection (a)(5)(A) protects the important rights of computer users from interference, whether the interference comes from persons who circumvent technical access barriers, or persons who do not need to. Even prominent advocates have applauded statutes, including subsection (a)(5)(A), for offering protection to persons with legitimate rights to access computers and data. *See, e.g.*, Kerr 2003, *supra* note 10, at 1660–61.

163. United States v. Nosal, 676 F.3d 854, 859 (9th Cir. 2012) (*Nosal I*) (quoting Powerex Corp. v. Reliant Energy Servs., Inc., 551 U.S. 224, 232 (2007)).

164. United States v. Nosal, 828 F.3d 865, 878 (9th Cir. 2016) (*Nosal II*) ("Nosal challenges the instruction on the basis that the CFAA only criminalizes access where the party circumvents a technological access barrier. Not only is such a requirement missing from the statutory language, but it would make little sense because some § 1030 offenses do not require access to a computer at all. For example, § (a)(6) imposes penalties for trafficking in passwords 'through which a computer can be accessed without authorization . . . .'").

165. Docket, Nosal v. United States, No. 16A840, *available at* https://www.supremecourt.gov/search.aspx?filename=/docketfiles/16a840.htm [https://perma.cc/9JCV-68GW].

barrier rule to remain a popular argument for CFAA defendants in other circuits, under state law,[166] and eventually at the Supreme Court.

Furthermore, a *technical access barrier* rule might also render Denial of Service ("DoS") attacks—perhaps one of the most easily identifiable computer crimes—outside the scope of the CFAA. "A DoS attack occurs when the attacker floods the target website with e-mails and/or information requests, so that the website cannot respond to normal, legitimate user traffic. Legitimate users therefore experience a 'denial of service' because they cannot access the target website."[167] DoS attacks in 2016 temporarily disabled notable websites including Twitter, Spotify, and Reddit.[168] Under the plain meaning of the statute, a DoS attack would be a violation of subsection (a)(5)(A), causing damage by impairing the "availability of data, a program, a system, or information."[169] However, such an attack need not circumvent any technical or code-based barrier. Congress clearly did not intend for DoS attacks to be excluded by an unstated rule.

Given rapidly changing technology standards, requiring a technological access barrier ensures the law will always struggle to define it and could require a complex understanding of technology to determine if the mechanism was a requisite barrier. This could make the understanding of "without authorization" a moving target based on the latest technological developments. Understandings will be slowed further by the time it takes for courts to react. *Nosal* provides a useful example. Still on appeal, *Nosal* concerns conduct that took place in October 2005. At that time, the iPhone was still under development, and smartphones, as we think of them today, were "unheard of . . . [but] a significant majority of American adults now own such phones."[170] In 2005, companies—including victim Korn Ferry—

166. This is particularly true under California law. Despite frequent attempts by litigants to treat the CFAA and CDAFA as analogous, the Ninth Circuit has rejected this analogy. United States v. Christensen, 801 F.3d 971, 994 (9th Cir. 2015) (concluding that "[t]he statutes are different" and that difference in interpretation results from different statutory text).

167. Massre v. Bibiyan, No. 12 Civ. 6615(KPF), 2014 U.S. Dist. LEXIS 82444, at *2–3 n.2 (S.D.N.Y. June 16, 2014) (quoting Complaint); *see also* eBay Inc. v. Digital Point Solutions, Inc., 608 F. Supp. 2d 1156, 1164 (N.D. Cal. 2009) (considering DoS attack as potentially analogous to cookie stuffing).

168. Brian Krebs, *DDoS on Dyn Impacts Twitter, Spotify, Reddit*, KREBS ON SECURITY, krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/ [https://perma.cc/B6DH-RSGG].

169. 18 U.S.C. § 1030(e)(8) (2012) (definition of damage).

170. Riley v. California, 134 S. Ct. 2473, 2484 (2014).

tended to need centralized private servers for their data, while today companies rely extensively on cloud computing. What might have been seen as a technical access barrier in 2005 may scarcely be recognized today. And even those functions that were understood when today's cases originated, such as IP blocking, raise difficult questions about whether they are in fact technical barriers.[171]

If the text and purpose are not enough to warn defendants not to rely on technical barriers, experience should be. Even when interpreting the CDAFA, the review of cases in this Article shows that even when a technical barrier rule allegedly applies, very few cases turn on that fact.[172]

B. Alternative Limitations Concerning Wrongful Conduct are Undesirable

In his most recent article, Professor Kerr argues that the open architecture of the Internet makes it analogous to the public square.[173] He explains:

> The protocols of the web make websites akin to a public forum. To draw an analogy, websites are the cyber-equivalent of an open public square in the physical world. A person who connects a webserver to the Internet agrees to let all access the computer much like one who sells his wares at a public fair agrees to let everyone see what is for sale. If you want to keep people out, backed by the authority of criminal trespass law, you don't set up shop at a public fair.[174]

But this misses an important piece of Internet architecture: the server. When a user accesses a website, the user sends a signal that reaches a private server owned, or more often leased, and usually kept on private property under very high physical security. The investment in building this backbone is less like a public square and more like a public house (which most Americans know as a pub).[175]

171. Craigslist Inc. v. 3Taps Inc., 942 F. Supp. 2d 962, 970 (N.D. Cal. 2013).

172. *See supra* Part II.B.

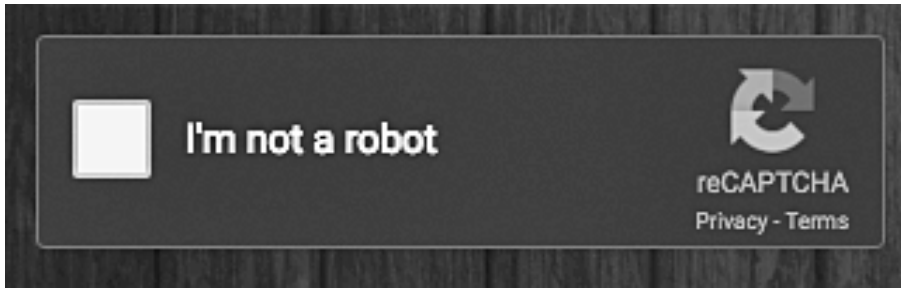
173. Kerr 2016, *supra* note 12, at 1163.

174. *Id.*

175. The origin of the term pub is useful. It comes from the distinction between a public house, which served alcohol to any guest, and a private club, which admits only members. Notable for lawyers, public houses evolved as part of inns, which were legally treated as places of public accommodation—not public squares or commons. The analogy to the internet works quite well. A website which requires authentication operates like a private club: members say the secret password and then may go inside. Alternatively, a pub lets anyone enter. Of course, a pub may establish certain rules for people who wish to enter (no shirt, no shoes, no service) or ban particularly rowdy patrons from returning. These

Like the proprietors of pubs, a principal concern of website operators is the nature of the users. Since users can surf the web from the privacy of their own homes, the old rule of no shirt, no shoes, no service does not apply. But website operators do care about the nature of the visitor. Specifically, they often care about the person versus bot distinction. A bot is a computer program often used to perform highly repetitive operations, such as trawling websites to collect email addresses.[176] Website owners may not want bots because bots are able to take content which required substantial investment to develop and reproduce it on other platforms.

Using authentication—as suggested by Professor Kerr—does not solve this problem. A bot can create an email or other account. Past efforts to eliminate bots used CAPTCHAs designed to stop bots. New systems are leaning toward requiring the user to check a box next to a message indicating that the user is not a bot, as shown here:



This is actually a security feature—the nature of cursor movement and click by humans differs from bots—but it does double as a legal notice.[177] Inevitably some bots will breach security and create accounts, and the law should not bury its head in the sand pretending this problem will never arise.

There are two principal ways the law could address this. The simpler way is to adopt a broader view of authorization—akin to a public house rather than a public square—and allow the owners to exclude certain patrons by reasonable notice. Terms and conditions will often

rules are, of course, imperfect. The bouncer at the door may not recognize someone who is banned, or may be looking the other way when the shirtless shoeless patron enters.

176. Shoggoth, *Top Definition—Bot (2)*, URBAN DICTIONARY (Aug. 11, 2003), http://www.urbandictionary.com/define.php?term=bot&defid=210890[https://perma.cc/47MG-57B3]; *see also* QVC, Inc. v. Resultly, LLC, 159 F. Supp. 3d 576, 600 n.3 (E.D. Pa. 2016) (describing use of robots.txt).

177. *See, e.g.*, *reCAPTCHA: Tough on Bots Easy on Humans*, GOOGLE, https://www.google.com/recaptcha/intro/index.html, [https://perma.cc/R7XB-H5ZR].

fail because nobody reads them, but active and clearly received notice will be more effective. As discussed below, this can be bolstered by proper understanding of *mens rea*.

Alternatively, we could adopt Kerr's proposal, with caveats. First, any circumvention of authentication would be without authorization. Second, the law would need to enforce rules placed on authentication, such as the requirement that accounts are maintained by a human user. Otherwise the problems are circumvented by making a false account. Third, separate law would be needed to address the lockout problem, where rightful ownership has been divorced from the credentials. And fourth, the law will need to address the software that tags along with authorized users. That's quite a mess.

C. Proper Textual Analysis of the *Mens Rea* Requirement Under the CFAA Compels Requiring Knowing and Intentional Unauthorized Acts

Subsection (a)(2)(C)—the broadest provision of the CFAA—criminalizes "intentionally access[ing] a computer without authorization or exceeds authorized access, and thereby obtain[ing] . . . information from any protected computer."[178] As discussed earlier, there are two interpretations applied in federal courts, one adopted in *Morris* and one adopted in *Nosal*.[179]

First, the term *intentionally* must modify the full phrase *accessing without authorization or exceeds authorized access*, not just the first half of the phrase. If the word *intentionally* only modified the term *access*, then the *mens rea* requirement is nearly abolished. Any person who clicks a mouse to open a file has intentionally accessed that file. This is the interpretation sought and, albeit vaguely, adopted in *Nosal I*. This reading of the intent requirement would protect only inadvertent access, such as a person who opens the wrong file or clicks the wrong link. In all of the research for this paper and as counsel on multiple computer misuse cases, the authors have never found a case where the defendant claimed that access itself was unintentional.

The alternative interpretation, that *intentional* modifies *without authorization* and also *exceeds authorized access*, provides far greater protection to defendants. If the defendant must intend to act without authorization, then the defendant must know, or should have reason to know, that she or he is not authorized.

178. 18 U.S.C. § 1030(a)(2)(C) (2012) (ellipsis to remove alternative violations).
179. *See supra* Part I.

While courts appear divided on this question, few have engaged in any serious analysis of the issue. On other questions of interpretation, courts have applied well-established principles of statutory interpretation to the CFAA. Principally, words in a statute are assumed to have the same meaning in different places. This means that the term *without authorization* cannot require circumvention of a technical access barrier in one part of the statute but not in another. Omitting alternative language, subsection (a)(2)(C) makes it a crime to "intentionally access a computer without authorization or exceeds authorized access, and thereby obtain . . . information from any protected computer."[180]

This *mens rea* requirement is *intent*, but the structure of the sentence alone does not answer what must be intentional. The sentence can be grammatically correct if the term *intentional* modifies only *access*, modifies *accesses a computer without authorization*, or modifies *access a computer without authorization or exceeds authorized access*.

The disjunctive nature of the phrase is useful. The term *exceeds authorized access* exists in the alternative to something. That something necessarily includes all words including and after *access*, but it is unclear if it applies to *intent*. If intent does not apply to *exceeds authorized access*, then a person who accidentally exceeds authorized access commits a crime. That's quite harsh—it's a strict liability. Alternatively, if *intentionally* does modify *exceeds authorized access*, then the person who accidentally exceeds authorized access is not a criminal. While pure grammar does not tell us the answer, the absence of an answer based on grammar does. Where two interpretations are plausible, the rule of lenity will cause the less harsh interpretation to be correct.[181] This is particularly the case with the potential for strict liability crimes.[182]

At this point in the analysis, it is clear that the word *intentionally* modifies two disjunctive phrases. The latter of those phrases criminalizes intentional exceeding of authorized access. The former phrase criminalizes intentional access without authorization. Again we have a problem: Does the word *intentionally* only modify *access* or does it also modify *without authorization*? Again, the rule of lenity can be useful. Any person who clicks on a file has intentionally accessed, so the inadvertent wrongdoing is again at risk of criminalization. This argues strongly for understanding the word *intentionally* to apply not only to *access* but also to *without authorization*. The argument here is not quite

180. 18 U.S.C. § 1030(a)(2)(C) (2012).
181. *See, e.g.*, United States v. Wiltberger, 18 U.S. (5 Wheat.) 76, 95 (1820).
182. *See, e.g.*, United States v. U.S. Gypsum Co., 438 U.S. 422, 437 (1978).

as strong as with *exceeds authorized access*; it is not a strict liability because access must be intended. But it is quite harsh. That alone is probably enough to push for the narrower interpretation. But the final useful analysis is a comparison of the disjunctive parts. If *exceeds authorized access* requires intent to perform an unauthorized act, then *accesses without authorization* should be understood the same way. An alternative reading would make those who access from outside face disproportionate lack of intent requirement compared with defendants who exceed authorized access. This is particularly true because the two types of violations may be overlapping categories.[183] Seeking to find congruence between the terms should seal the deal: the defendant must intend that the access be without authorization.

This correct reading of the *mens rea* requirement solves most of the problems addressed in this Article. The *mens rea* requirement prioritizes the privacy interest that the CFAA was designed to protect. Persons who intentionally invade that privacy, regardless of the level of security circumvented, would be liable. The lockout cases would clearly be covered, except perhaps in cases of good faith misunderstandings. And terms of service violations would generally be excluded since as a matter of practice few people read the terms of service.

D. The Problem of Subsection (a)(2)(C)

The Ninth Circuit issued a revised opinion in tandem with denial of *en banc* review, emphasizing that the *mens rea* requirement of "intent to defraud" under subsection (a)(4) prevents the "parade of hypotheticals by Nosal and amici."[184] The court declined to apply its analysis to subsection (a)(2)(C), which does not contain the same "intent to defraud" *mens rea* requirement.[185]

By declining to apply the *transitive property of statutory interpretation*, the Ninth Circuit may have backed itself into a corner where it will have to address whether subsection (a)(2)(C), under a broad interpretation, is unconstitutional. The Supreme Court has made clear that terms in a statute must be interpreted consistently.[186] The Ninth

183. *See* Oral Argument, Musacchio v. United States, 136 S. Ct. 709 ___(2016) (No. 14-1095), https://www.oyez.org/cases/2015/14-1095 (last visited Apr. 17, 2016) (statement of Justice Alito) [https://perma.cc/C6RR-RT8M]; *see also* WEC Carolina Energy Solutions, LLC v. Miller, 687 F.3d 199, 204 (4th Cir. 2012) (citing Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 419 (7th Cir. 2006) ("Recognizing that the distinction between these terms is arguably minute")).

184. United States v. Nosal, 828 F.3d 865, 869 (9th Cir. 2016) (*Nosal II*).

185. *Id.* at 869.

186. Powerex Corp. v. Reliant Energy Servs., Inc., 551 U.S. 224, 232 (2007).

Circuit has now rejected a narrow interpretation of *without authorization*. The Ninth Circuit could turn back on its interpretation of the *mens rea* requirement for subsection (a)(2)(C) explained in *Nosal I*. Although this interpretation resulted from positions that were briefed, argued, and decided, the *Nosal I* decision contains such sufficiently vague language that the court could explain that it did not mean quite what it said. This Article contends that such a move would align the Ninth Circuit with the correct understanding of the *mens rea* requirement, but even that move may be insufficient to save subsection (a)(2)(C) from constitutional concerns.

The problem is that many people are aware of restrictions and violate them regularly. Couples share passwords for email and social media knowing that the host companies prohibit this behavior. People lie about their physical attributes on dating sites despite knowing that such lies are not allowed. None of these are wonderful things, but none of these should send a person to jail, even for less than a year.[187]

A statute that criminalizes such a broad category of ordinary behavior and makes everyone a potential criminal under *the law that sticks*.[188] The problem with the CFAA, and subsection (a)(2)(C) specifically, is not that it renders some random or obscure form of conduct criminal. The problem is that it renders as criminally liable conduct that almost everyone commits, at least for those unlucky enough to know about relevant terms and conditions.

Even with a strong intent rule, the CFAA imposes overbroad liability on a subject where there is no societal consensus about authorized behavior. Recent empirical research suggests that many Americans—potential jurors—have mixed views of the meaning of authorized access and the seriousness of unauthorized access. Matthew Kugler published the results of a survey of 593 United States citizens, asking questions concerning the authorization, blameworthiness, and appropriate punishment for potential CFAA violations.[189] The survey questions concerned misuse of an employer's computer, use of a neighbor's WiFi network, and unauthorized access to a business website. Kugler's survey results indicated that Americans have inconsistent

187. Violation of subsection (a)(2)(C) is a misdemeanor, punishable by less than a year in prison. 18 U.S.C. § 1030(c)(2)(A) (2012).

188. Reply All, *The Law That Sticks*, GIMLET MEDIA (Oct. 28, 2015), https://gimletmedia.com/episode/43-the-law-that-sticks/ [https://perma.cc/6WLA-EQWV].

189. Matthew B. Kugler, *Measuring Computer Use Norms*, 84 GEO. WASH. L. REV. 1568 (2016).

views on authorization, and those views do not correspond with blameworthiness and punishments.[190]

Given the potential overbreadth and the low chance of any court reaching a good solution, it is far from clear that subsection (a)(2)(C) would survive a challenge on the basis that it is void for vagueness.[191] That courts have so ruled otherwise, and the resulting basis in *stare decisis* for affirming the CFAA as a whole, is insufficient. "Unlike other judicial mistakes that need correction, the error of having rejected a vagueness challenge manifests itself precisely in subsequent judicial decisions: the inability of later opinions to impart the predictability that the earlier opinion forecast."[192]

Prior decisions, such as *Nosal* and *Power Ventures* devoted substantial effort to avoiding constitutional frailty. They did not succeed. Technical barrier-based approaches are incompatible with a fair reading of the text, and will fail as technology evolves. Duty of loyalty approaches are even more vague. And even accepting the access versus use distinction in *Nosal*, there are still potential problematic cases. That the Justice Department may avoid problematic cases is no answer. Courts "cannot construe a criminal statute on the assumption that the Government will use it responsibly."[193]

Alternatively, Congress could amend the law and avoid the risk of losing in court. A return to first principles illustrates an option. Three foundational goals of computer security are protecting the confidentiality, integrity, and availability of data.[194] Impairment of integrity and availability of data is criminalized under subsection (a)(5) of the CFAA. Threatening to impair confidentiality is explicitly addressed under subsection (a)(7)(B), but actually impairing confidentiality would be covered only by subsection (a)(2)(C).

This language offers an opportunity for legislatures, though probably not for courts. Courts would be hard-pressed to read a confidentiality requirement into subsection (a)(2)(C) when language

190. *Id.* at p. 1590.

191. Subsection (a)(2)(C) is probably severable from other offenses. It was enacted in an amendment in 1996, after several other offenses existed. Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3492 (codified at 18 U.S.C. § 1030(a)(2)(C) (2012)).

192. Johnson v. United States, 135 S. Ct. 2551, 2562 (2015).

193. United States v. Nosal, 828 F.3d 865, 896 (9th Cir. 2016) (*Nosal II*) (Reinhardt, J., dissenting) (quoting McDonnell v. United States, 579 U.S. ———, 136 S. Ct. 2355 (2016) (citation omitted)).

194. Orin S. Kerr, *Trespass, Not Fraud: The Need for New Sentencing Guidelines in CFAA Cases*, 84 GEO. WASH. L. REV. 1544, 1554 n.65 (2016) (citing MATT BISHOP, INTRODUCTION TO COMPUTER SECURITY 1 (2005)).

concerning confidentiality appears elsewhere in the statute but not in that subsection. Congress, on the other hand, could borrow the confidentiality language from subsection (a)(7)(B) to amend subsection (a)(2)(C), adding an element that confidentiality be impaired. Such an amendment would narrow the scope of subsection (a)(2)(C) to the sort of privacy invasions that may not be prohibited elsewhere in the statute.

Conclusion

The CFAA and its state law counterparts are trouble. They address a hard-to-manage area of law, and often depend on undefined terms. But these laws are also important. They are extremely valuable tools that protect important interests, including privacy and the ability to control one's own digital spaces. The proposed requirement that a defendant circumvent a technical access barrier was tested in cases under California's CDAFA. The results of our survey of cases show little benefit for any defendant and serious detriments for victims. We conclude that there is no easy solution to the ambiguities of the CFAA and its state law counterparts. In the interim, the best way to sort the good cases from the bad is to focus on intent. Actions by defendants circumventing those barriers can form strong evidence of criminal intent. So can other conduct. As long as courts apply the correct intent requirement—requiring that the defendant know the action is unauthorized—most of the *parade of horribles* cannot be prosecuted. Proper reading of the intent requirement may or may not save the CFAA from all constitutional challenges, but it will help draw the line between wrongful and innocuous conduct.