ALGORITHMIC AUDITING AND COMPETITION UNDER THE CFAA: THE REVOCATION PARADIGM OF INTERPRETING ACCESS AND AUTHORIZATION

Annie Lee†

I. INTRODUCTION

Congress enacted the Computer Fraud and Abuse Act (CFAA) as an anti-hacking statute in 1984, seven years before the invention of the world-wide web.[1] Through a single statute, the CFAA today serves as the legal centerpiece for all computer-related offenses,[2] governing how we share and protect information on the Internet. For years, the scope of the CFAA has been hotly debated.[3] Congress has repeatedly broadened the statute to encompass wide ranges of computer behavior,[4] while commentators have consistently criticized the statute for being overly broad and vague.[5] Today, the CFAA is again at the forefront of legal discourse because it meets a wave of new technology: artificial intelligence and the rise of Internet platform power.

Consider the following scenario. Ellen and Michelle are new graduates looking for jobs on MBAHired, an online hiring website where MBA graduates can create personal profiles and search for job opportunities posted by

DOI: https://doi.org/10.15779/Z38SQ8QH9J

† J.D. Candidate, 2019, University of California, Berkeley, School of Law.

1. The worldwide web was invented by a Swiss computer programmer in 1991. *The Invention of the Internet*, HISTORY (July 30, 2010), https://www.history.com/topics/inventions/invention-of-the-internet [https://perma.cc/WS7J-TM5D].

2. *See* S. REP. NO. 104-357, at 5 (1996) (stating that the intent of the original Act was to address "in a single statute the problem of computer crime, rather than identifying and amending every potentially applicable statute affected by advances in computer technology").

3. *See, e.g.*, Kim Zetter, *The Most Controversial Hacking Cases of the Past Decade*, WIRED (Oct. 26, 2015), https://www.wired.com/2015/10/cfaa-computer-fraud-abuse-act-most-controversial-computer-hacking-cases/ [https://perma.cc/4YAM-PPWT].

4. *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1563–71 (2010) [hereinafter Kerr, *CFAA Vagueness*] (describing 6 amendments that broadened the "ever-expanding CFAA").

5. *See, e.g.*, Tim Wu, *Fixing the Worst Law in Technology*, NEW YORKER (Mar. 18, 2013), https://www.newyorker.com/news/news-desk/fixing-the-worst-law-in-technology [https://perma.cc/P7Z4-J543]; Grant Burningham, *The Most Hated Law on the Internet and Its Many Problems*, NEWSWEEK (Apr. 6, 2016), http://www.newsweek.com/most-hated-law-internet-and-its-many-problems-cfaa-448567 [https://perma.cc/2CB2-CHD8]. *See generally* Kerr, *CFAA Vagueness*, *supra* note 4, at 1571–87 (advocating for courts to limit the Act using the constitutional vagueness doctrine).

recruiters. Ellen performs a search and receives a list of opportunities ranked in order of "relevance." When Michelle performs the same search on the same website, she also receives a list of opportunities. But the two lists are not the same.

This scenario is not uncommon on the Internet today. Online giants such as Amazon, Google, and Facebook regularly use artificial intelligence algorithms to provide each user a customized experience with the most relevant information.[6] Thus, often for good reason, one user will have a different experience than another on the same website.[7] On a hiring website with millions of opportunities,[8] this ability to provide individual users with curated search results can be critical to helping candidates find the right jobs.

However, this powerful new tool can also be a dangerous channel for discrimination. Imagine that Ellen and Michelle have similar work experience, but Ellen has identified herself as white, and Michelle has identified herself as black. Artificial intelligence algorithms are often "trained" to make decisions that follow patterns found in historic data.[9] Thus, if data show that black candidates historically have had lower success rates applying for management positions, the website may omit those higher-paying positions from Michelle's search results purely because she has listed her race.[10]

Today the Internet is undergoing wildfire adoption of these types of algorithms.[11] Unfortunately, as demonstrated in Michelle's situation, the

6. *See* Erik Brynjolfsson & Andrew Mcafee, *The Business of Artificial Intelligence*, HARV. BUS. REV. (July 2017), https://hbr.org/cover-story/2017/07/the-business-of-artificial-intelligence [https://perma.cc/A5RY-G5RK].

7. The Facebook Newsfeed is perhaps one of the most illustrative examples of the customized user experience. *See How News Feed Works*, FACEBOOK, https://www.facebook.com/help/327131014036297/ [https://perma.cc/J99R-6ZES] (last visited Feb. 21, 2018) (explaining that the News Feed is meant "to keep you connected to the people, places, and things that you care about, starting with your friends and family").

8. At the time this Note was written, a quick search on Indeed.com for all available jobs in the United States returned 2,985,526 results.

9. *See* Lauren Kirchner, *When Discrimination Is Baked into Algorithms*, ATLANTIC (Sep. 6, 2015), https://www.theatlantic.com/business/archive/2015/09/discrimination-algorithms-disparate-impact/403969/ [https://perma.cc/4BCZ-N2LJ] (explaining how "[s]oftware making decisions based on data can reflect, or even amplify, the results of historical discrimination").

10. *See id.*

11. In a study run by Harvard professor Latanya Sweeney, Sweeney showed that across 2000 name searches on Google, those associated with black people were 25 percent more likely to generate an arrest-related ad. Latanya Sweeney, *Discrimination in Online Ad Delivery*, 56 COMMS. ACM 44, 44 (May 2013). In another incident, Google mistakenly tagged two black people as "gorillas." Maggie Zhang, *Google Photos Tags Two African-Americans As Gorillas Through Facial Recognition Software*, FORBES (July 1, 2015), https://www.forbes.com/sites/mzhang/

tremendous ability of these algorithms to make our online marketplaces more efficient also creates incredible potential for troubling business practices to lurk in the shadows.[12]

External pressures from third parties are necessary because businesses are failing to self-regulate.[13] This Note identifies two groups of third parties that have emerged to promote online integrity in response to the rise of artificial intelligence: algorithmic auditors and online competitors. Algorithmic auditors largely consist of academics,[14] computer scientists from nonprofits,[15] and journalists[16] who scrutinize online websites powered by algorithms for bias and

2015/07/01/google-photos-tags-two-african-americans-as-gorillas-through-facial-recognition-software/#50867719713d [https://perma.cc/E5MN-YQUJ]. *See* Gillian B. White, *When Algorithms Don't Account for Civil Rights*, ATLANTIC (Mar. 7, 2017), https://www.theatlantic.com/business/archive/2017/03/facebook-ad-discrimination/518718/ [https://perma.cc/YS75-CUCX] (describing how Facebook's advertising platform gives advertisers the option to target users based on their assigned "ethnic affinity"); Julia Angwin et al., *Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [https://perma.cc/RHR2-CBZA].

12. *See* Ray Fisman & Michael Luca, *Fixing Discrimination in Online Marketplaces*, 94 HARV. BUS. REV. 88, 88 (Dec. 2016) (discussing the emergence of "digital discrimination"); *see also* Michael Todisco, *Share and Share Alike? Considering Racial Discrimination in the Nascent Room-Sharing Economy*, 67 STAN. L. REV. ONLINE 121, 121 (Mar. 14, 2015) ("Airbnb and other housing-focused companies of the new 'sharing economy' facilitate virtually unregulated discrimination—both implicit and intentional—in housing and accommodations.").

13. Instead, under Section 230 of the Communications Decency Act, Internet businesses have often asserted immunity to avoid liability for discrimination on their platforms by characterizing themselves as mere "passive conduits" through which users engage with one another. *See* Karen Levy & Solon Barocas, *Designing Against Discrimination in Online Markets*, 32 BERKELEY TECH. L.J. 1183 (2017).

14. The MBAHired hypothetical was inspired by a study being conducted by Associate Professor Alan Mislove and Assistant Professor Christopher Wilson at Northeastern University. Their study tests whether the ranking algorithms on major online hiring websites produce discriminatory outputs by systematically ranking specific classes of people below others. Complaint for Declaratory and Injunctive Relief at 6, Sandvig et al. v. Sessions, No. 1:16-cv-01368 (D.D.C. June 29, 2016) [hereinafter Complaint for Declaratory and Injunctive Relief]. For more on this case, see discussion, *infra* Part III.C.2.

15. *See, e.g.*, Michael Tschantz, *Accountable Information Use: Privacy and Fairness in Decision-Making Systems*, INT'L COMPUT. SCI. INST. (2017), https://www.icsi.berkeley.edu/icsi/projects/networking/accountable-information-use [https://perma.cc/48PU-3GJV] (navigate to "Projects" tab). The International Computer Science Institute (ICSI) is a nonprofit center for research in computer science affiliated with, but independent of the University of California, Berkeley. Many of ICSI's scientists hold faculty appointments at the university. *See id.* (navigate to "About" tab).

16. *See, e.g.*, Cathy O'Neil, *The Ivory Tower Can't Keep Ignoring Tech*, N.Y. TIMES (Nov. 14, 2017) (calling for more social research on online discrimination).

discrimination.[17] Online competitors similarly promote fair online practices by providing users with a choice between competitive products: if Michelle suspects that MBAHired is not giving her the right opportunities, she should be able to switch to a different hiring platform.

Under the CFAA, however, both of these third parties face the threat of litigation and prosecution[18] because their need for information from online platforms clashes with the CFAA's prohibition on unauthorized access to a computer or website. An algorithmic auditor who needs information about a website's inner workings to determine whether the website's algorithms are providing discriminatory results may run afoul of the CFAA while obtaining such information. Similarly, a competitor who needs to understand an incumbent's online product in order to provide a comparable or complementary product is also at risk.

The CFAA can be especially troubling for these parties because courts have struggled to adopt a national standard for interpreting the meaning of "unauthorized access" on the Internet.[19] Instead, courts have adopted a patchwork of competing paradigms for interpretation, creating a legal minefield for algorithmic auditors and competitors who look to the law to inform their online behavior.[20] In *Facebook v. Power Ventures* and *United States v. Nosal* (*Nosal II*), the Ninth Circuit articulated yet another paradigm for interpretation: Once an online service provider revokes a user's access to their website, any subsequent attempt to access that website—regardless of the method employed—is considered unauthorized under the CFAA.[21]

By allowing courts to adopt a patchwork of paradigms for interpreting authorization on the Internet, Congress has enabled incumbent website owners to use the CFAA to exclude algorithmic auditors and competitors from accessing information they need to encourage online integrity. Indeed, the newest revocation paradigm provides some legal clarity; but in exchange, it grants a troubling amount of power to the online service provider, who

17. The first national Conference on Fairness, Accountability, and Transparency (FAT) was held in February 2018. *See Conference on Fairness, Accountability, and Transparency*, ACM FAT CONF. (Dec. 20, 2017), https://fatconference.org/index.html [https://perma.cc/WZ58-WRJ2]. The conference's steering committee included over 40 members consisting of academics and individuals from private companies such as Microsoft, Google, and Spotify. *See id.* (navigate to "Organization" tab).

18. The CFAA contains both a criminal cause of action and a civil cause of action for private parties. *See infra* note 23.

19. *See* discussion, *infra* Part III ("Existing Paradigms of Unauthorized Access").

20. *Id.*

21. *See* discussion, *infra* Part IIII ("Revocation as a New Paradigm"); Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058 (9th Cir. 2016), *cert. denied*, 138 S. Ct. 313 (2017); United States v. Nosal, 844 F.3d 1024 (9th Cir. 2016), *cert. denied*, 138 S. Ct. 314 (2017).

becomes the de facto enforcer of the CFAA's prohibition on unauthorized access.

Part II of this Note gives an overview of current paradigms for interpreting unauthorized third-party access under the CFAA and how each paradigm has discouraged algorithmic auditors from exposing questionable business practices and fostered a hostile market for new competitors. Part III proposes that two recent Ninth Circuit cases, *Facebook* and *Nosal II*, have created a new revocation paradigm for interpreting authorization that may create more clarity for courts. Part IV then identifies the dangers of the singling-out power created by the revocation paradigm and discusses the implications of this phenomenon for algorithmic auditors and competitors. Finally, Part V sets forth a normative legislative proposal to narrow the scope of the CFAA, encourage algorithmic accountability, and foster healthy competition.

II. EXISTING PARADIGMS OF UNAUTHORIZED ACCESS

The CFAA was originally a criminal statute that aimed to protect a narrow scope of computers owned by government and financial institutions from outside hackers.[22] Since its enactment, however, the CFAA has been amended several times to reach its modern-day form: the CFAA now regulates behavior on almost any device connected to the Internet and includes a private civil cause of action.[23]

22. The original Counterfeit Access Device and Computer Fraud and Abuse Act (CADCFAA) focused on three forms of improper access: government information for national defense, financial information from financial institutions, and information from government computers. Pub. L. 98-473, ch.21, sec. 2101, § 1030, 98 Stat. 2190, 2190–91 (1984). The legislative history shows that Congress was particularly concerned about "the advent of activities of so-called 'hackers' who have been able to access (trespass into) both private and public computer systems, sometimes with potentially serious results." H.R. REP. No. 98-894 (1984), as *reprinted in* 1984 U.S.C.C.A.N. 3689, 3695. The House report also referenced the cautionary tale of *WarGames*, a 1983 film in which a teenager unknowingly hacks into the government's nuclear arsenal while searching for an online video game. *Id.* at 3696; Scott Brown, Wargames: *A Look Back at the Film that Turned Geeks and Phreaks into Stars*, WIRED (July 21, 2008), https://www.wired.com/2008/07/ff-wargames/ [https://perma.cc/H99P-LJEM].

23. *See* Kerr, *CFAA Vagueness*, *supra* note 4, at 1563–71. Under section 1030(g), any person who "suffers damage or loss by reason of a violation of [the CFAA] may maintain a civil action against the violator." 18 U.S.C. § 1030(g) (2012). The scope of the civil provision is nearly as broad as the criminal statute itself. Of the six enumerated types of culpable conduct under the Act, there is only one where *only* a criminal case may be brought: where the plaintiff alleges "damage affecting 10 or more protected computers during any 1-year period." *See id.* (excluding section 1030(c)(4)(A)(i)(VI) in the civil provision).

The two broadest provisions of the CFAA, sections (a)(2)(C) and (a)(4), each create liability for anyone who "accesses a protected computer without authorization" or "exceeds authorized access."[24] Yet, since the inception of the Act, Congress has refrained from defining the meanings of "without authorization" and "exceeds authorized access" in terms of specific online behaviors.[25] In response, courts and commentators have taken it upon themselves to formulate their own standards of what types of online behavior constitute unauthorized access under the CFAA.

This Part surveys the three leading paradigms for interpreting unauthorized third-party access under the CFAA: agency theory,[26] the code-based approach,[27] and the text-based approach.[28] This Part describes how each of these paradigms attempts to distinguish between authorized and unauthorized access to a computer and how that distinction affects third-party algorithmic auditors and competitors.

A. AGENCY THEORY

1. Agency Theory and Its Critiques

Some courts use the commercial law theory of agency to set the boundary between authorized and unauthorized access.[29] These cases often involve a disloyal employee acting in conflict with his or her employer's interests.[30] In an

24. 18 U.S.C. §§ 1030(a)(2)(C), (a)(4).

25. The CFAA does not include a definition of "without authorization." 18 U.S.C. § 1030(e). It does define "exceeds authorized access" to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). However, there is a fundamental circuit split as to whether the definition prohibits only unauthorized *access* to information or also unauthorized *use* of information that a defendant was authorized to access only for specific purposes. *See* Memorandum Opinion at 24–25, Sandvig et al. v. Sessions, No. 1:16-cv-01368 (D.D.C. Mar. 30, 2018) (describing a split between the *access* interpretation adopted by the Second, Fourth, and Ninth Circuits, and the *use* interpretation adopted by First, Fifth, and Eleventh Circuits). Recently, the District Court of Columbia in *Sandvig* joined the latter circuits by adopting the narrower *access* interpretation, in part by applying the constitutional avoidance doctrine. *Id.* at 29–31.

26. *See* discussion, *infra* Part III.A.

27. *See* discussion, *infra* Part III.B.

28. *See* discussion, *infra* Part II.C.

29. *See, e.g.*, International Airport Centers, LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006); United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010); Amedisys Holding, LLC v. Interim Healthcare of Atlanta, Inc., 793 F. Supp. 2d 1302, 1315 (N.D. Ga. 2011); NCMIC Fin. Corp. v. Artino, 638 F. Supp. 2d 1042, 1061 (S.D. Iowa 2009); Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121 (W.D. Wash. 2000).

30. Professor Orin Kerr first discussed the agency paradigm as "employee misconduct cases." Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse*

agency relationship, the principal authorizes the agent to act on their behalf.[31] The agent in return owes a fiduciary duty of loyalty to advance the principal's interests over their own.[32] Applied to the CFAA in the employment context, the agency relationship terminates and an employee's access to an employer's computer becomes unauthorized if the employee "acquires adverse interests" or is in a "serious breach of loyalty" to the employer.[33]

For example, in *International Airport Centers, LLC v. Citrin*, the Seventh Circuit applied the agency theory to the CFAA where an employee installed a software program onto his employer's laptop to permanently delete company data before quitting and starting a competing business.[34] The court held that even though the defendant was still employed and had physical access to the computer at the time of deletion, he was nonetheless "without authorization" because his authority to access his employer's laptop terminated the moment he decided to quit and destroy files "in violation of the duty of loyalty."[35]

Aside from the Seventh Circuit, courts have largely rejected the agency theory.[36] Commentators have likewise criticized the agency theory as making the CFAA overly broad and susceptible to constitutional challenges under the void-for-vagueness doctrine.[37] Professor Orin Kerr argues that the agency theory provides insufficient notice to employees because it fails to outline specifically what types of behavior fall outside the duty of loyalty in the employment context: "Is mere waste of the employer's time enough?"[38]

Statutes, 78 N.Y.U. L. Rev. 1596, 1632–37 (Nov. 2003) [hereinafter Kerr, *Cybercrime's Scope*]; *see also* Petition for Writ of Certiorari, Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058 (No. 16-01105), *denied* at 24 ("[M]ost CFAA cases arise in the context of an employee or ex-employee accessing an employer's computers or database.").

31. Restatement (Second) of Agency § 112 (1958).

32. *Id.*

33. *See id.*; Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1124–25 (W.D. Wash. 2000) (holding under principles of agency that employees lost access to the employer's computers when they allegedly became agents of a competitor to appropriate trade secrets).

34. *Citrin*, 440 F.3d 418.

35. *Id.* at 420.

36. *See, e.g.*, United States v. Nosal, 676 F.3d 854, 862 (9th Cir. 2012) (rejecting "decisions of . . . sister circuits that interpret the CFAA broadly to cover . . . violations of a duty of loyalty"); WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 206 (4th Cir. 2012) ("reject[ing] any interpretation that grounds CFAA liability on a cessation-of-agency theory").

37. *See* Kerr, *CFAA Vagueness*, *supra* note 4, at 1586.

38. *Id.* at 1586.

2. Agency Theory for Algorithmic Auditors and Competitors

Although the agency theory is typically reserved for employment cases where an employee uses a work computer against the employer's best interests, it is also pertinent to algorithmic auditors and competitors because algorithmic bias research and online competition can stem from the employment context.

In the research setting, employers can use the agency theory against internal employees whose work aims to encourage online integrity. For example, organizations often assign internal employees to sniff out potential discrimination in their proprietary algorithms. [39] If the employment relationship is terminated, however, the organization could use the agency theory to accuse the now-prior employee of engaging in unauthorized access during their employment—the legal hook being that the employee's method of conducting the research was not in the employer's best interests.

Such was the case of Scott Moulton. In *Moulton v. VC3*, a Georgia city police department hired Moulton, the network administrator for the county 911 center, under a service contract to set up a router and connect the city police department with the county 911 center.[40] Before connecting the two, Moulton became concerned for the security of the networks and performed a remote port scan [41] to assess the vulnerability of the police department's network. When the police department noticed the unusual network behavior, it immediately terminated its service contract with Moulton and contacted the Georgia Bureau of Investigation to arrest Moulton for criminal computing trespass.[42] Under the agency theory, if a jury found that Moulton's specific decision to perform the port scan was not in the best interests of the police department, he could be held liable under the CFAA.[43] Therefore, even though the police department hired Moulton to work on their network, a CFAA claim

39. *See, e.g.*, Jessi Hempel, *For Nextdoor, Eliminating Racism Is No Quick Fix*, WIRED (Feb. 16, 2017), https://backchannel.com/for-nextdoor-eliminating-racism-is-no-quick-fix-9305744f9c6 [https://perma.cc/5UDX-PBTU] (describing Nextdoor's consultations with racial justice groups and government officials in their efforts to mitigate user bias on the platform).

40. Moulton v. VC3, No. 1:00CV434-TWT, 2000 WL 33310901, at *1 (N.D. Ga. Nov. 7, 2000).

41. *Id.* at *2. A port scan is a "common network security test that sends a query to each open port on the target computer to see if that port is open and ready to receive incoming traffic." Kerr, *Cybercrime's Scope*, *supra* note 30, at 1626.

42. *Id.* at *2.

43. Moulton's case was dismissed because the damages did not meet the statutory $5000 requirement. *Id.* at *7.

could still be available for specific decisions Moulton made while performing assigned tasks.[44]

Although Moulton was a network security professional rather than an algorithmic auditor, his case closely resembles the auditing context and therefore raises similar concerns. Moulton's worry about the integrity of the network led him to independently decide to perform a remote port scan. This is analogous to the work of a software employee, who may worry about the integrity of a website's algorithm and similarly choose to address the issue in a manner that has not been explicitly approved by the employer.[45] If the employee is terminated, the employer—as in Moulton's case—could feasibly use the agency theory to bring a CFAA claim.

Similarly, the agency theory can provide the legal hook for businesses to sue their competitors. If an employee leaves to start a competing business, the employer can use the agency theory to attach CFAA liability to the now-prior employee's actions before they left the company. The case of *LVRC Holdings LLC v. Brekka* provides an illustrative example.[46] In *Brekka*, a business sued a former employee under the CFAA for emailing company documents to himself and his wife before departing and starting a competing business.[47] The business argued that the employee accessed the company's computers "without authorization" because he acted against the best interests of the business and breached the agency relationship.[48] Although the Court eventually rejected this argument,[49] the case illustrates how interpreting authorization under the agency paradigm can empower a business to sue a competing business by clawing back at the actions of prior employees.

---

44. Security analyst Stefan Puffer had a similar fate. Puffer worked for the Harris County technology department. In a "war driving" exercise, Puffer demonstrated to a county official and a newspaper reporter how easy it was to access the county's court system using only a laptop and a wireless LAN card. Puffer was indicted by a grand jury for violating the CFAA. He was acquitted by a jury in fifteen minutes. Matthew Bierlein, *Policing the Wireless World: Access Liability in the Open Wi-Fi Era*, 67 OHIO ST. L.J. 1123, 1159 n.187 (2006).

45. For example, to address racial profiling on their mobile application, Nextdoor assembled a small team consisting of a communications director, a product manager, a designer, a data scientist, and an engineer. *See* Hempel, *supra* note 39. Though they may not be aware, this team could be vulnerable to the CFAA under the Moulton rationale if they choose to make decisions not explicitly approved by upper management.

46. LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009).

47. *Id.* at 1129–30.

48. *Id.* at 1133–34.

49. The Court refused to apply the agency paradigm as articulated in the Seventh Circuit's *Citrin* opinion. Invoking the rule of lenity, the Court held that Brekka was not liable under the CFAA because he had permission to access the documents at the time he emailed them to himself and his wife. *See id.* at 1134.

As demonstrated by *Moulton* and *Brekka*, the agency theory of interpreting authorization generates significant legal uncertainty for algorithmic auditors and competitors whose work stems from a prior employment relationship. Because the exact scope of the agency relationship is undefined, when the agency relationship is used as a proxy for the outer boundaries of authorized computer behavior, employees cannot be certain that they will not inadvertently run afoul of the CFAA while performing their jobs. Thus, if employees are involved in investigating algorithmic bias or leave to join a competing business, the malleability of the agency relationship makes it particularly easy for employers to allege CFAA violations before their departure.

B. CODE-BASED APPROACH

1. The Code-Based Approach and Its Critiques

A number of leading scholars have advocated for courts to adopt a code-based approach, which attempts to define the boundary between authorized and unauthorized conduct by examining whether the defendant circumvented technological barriers.[50] This approach requires a fact-intensive examination into the specific technical manner by which the defendant obtained access. Past cases have turned on a range of technological tactics used by defendants, such as whether the defendant exploited vulnerabilities in a software program,[51] bypassed an Internet Protocol (IP) block by changing IP addresses

50. *See, e.g.*, Patricia L. Bellia, *A Code-Based Approach to Unauthorized Access Under the Computer Fraud and Abuse Act*, 84 Geo. Wash. L. Rev. 1442 (2016) (endorsing the code-based approach because a user will always encounter a code-based barrier which provides clear notice that the system owner did not consent); David J. Rosen, *Limiting Employee Liability Under the CFAA: A Code-based Approach to "Exceeds Authorized Access"*, 27 BERKELEY TECH. L.J. 737, 740 (2012) (explaining how the code-based approach is "consistent with the text and purpose of the CFAA"); Kerr, *Cybercrime's Scope*, *supra* note 30, at 1600 (proposing that courts adopt a code-based approach to draw "a workable line between privacy and openness"). *But see* Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143 (2016) (arguing that "trying to figure out when access circumvented a code-based restriction" is too difficult). Professor Kerr instead proposed that courts look to whether the defendant circumvented an authentication gate, such as a password terminal. *See id.*

51. In the first ever conviction under the CFAA, the Second Circuit in *United States v. Morris* convicted graduate student Robert Tappan Morris at Cornell for exploiting security vulnerabilities in a computer at the Massachusetts Institute of Technology (MIT) to spread a computer "worm," causing many university machines around the country to become "catatonic." 928 F.2d 504 (2d Cir. 1991). The Court held that Morris had acted "without authorization" because he used the university system's features "not in any way related to their intended function." *Id.* at 510. Morris would later return to graduate school to earn a doctorate from Harvard, join the faculty of MIT as a tenured engineering professor researching

or using a server proxy,[52] or sent repeated public queries ("GET requests") to retrieve user information from a company's database.[53]

The code-based approach bears close resemblance to the language of the anti-circumvention provision in the Digital Millennium Copyright Act (DMCA),[54] so the legal community's reactions and concerns in the copyright context are relevant to the code-based paradigm here. Section 1201(a)(1)(A) of the DMCA prohibits circumventing "a technological measure that effectively controls access" to a copyrighted work.[55] In response, an array of technological protection measures (TPMs) have emerged, including password protection, dongles, encryption, and watermarking, to name a few.[56] Courts have adopted several competing legal standards to assess the legal efficacy of these TPMs and to determine what constitutes circumvention of these TPMs in the copyright infringement context.[57] Nevertheless, because many of the legal standards are in disagreement with each other, it can be difficult for a copyright

computer networks, and co-found the renowned startup-funding firm Y Combinator. *See* Timothy B. Lee, *How a Grad Student Trying to Build the First Botnet Brought the Internet to Its Knees*, WASH. POST (Nov. 1, 2013), https://www.washingtonpost.com/news/the-switch/wp/2013/11/01/how-a-grad-student-trying-to-build-the-first-botnet-brought-the-internet-to-its-knees/?utm_term=.26e48191fbf8 [https://perma.cc/T2WB-D846].

52. In *Craigslist Inc. v. 3Taps Inc.*, Craigslist alleged that 3Taps had "scraped," or copied, all content posted on Craigslist to provide a "Craigslist API" for third parties and to operate websitecraiggers.com, a website which "essentially replicated the entire craigslist website" including all of the scraped content. 964 F. Supp. 2d 1178, 1180 (N.D. Cal. 2013). To stop 3Taps' actions, Craigslist configured the website to block access from IP addresses associated with 3Taps and sent 3Taps a cease and desist letter prohibiting 3Taps' access to the website. *Id.* at 1181. The Northern District of California denied 3Taps' motion to dismiss, holding that 3Taps was without authorization in part because the average person would not use anonymous proxies to bypass an IP block. *Id.* at 1184.

53. In *United States v. Auernheimer,* security researcher Andrew "Weev" Auernheimer was sentenced to 41 months of prison for exposing a technical hole in AT&T's iPads. 748 F.3d 525 (3d Cir. 2014). Auernheimer wrote a program to repeatedly access AT&T's website in a "brute force" attack and ultimately collected 114,000 customer email addresses. *Id.* at 531. When he publicized his exploits to media members, they notified AT&T, who immediately fixed the breach. *Id.* at 531.

54. Digital Millennium Copyright Act of 1998, S. 2037, 105th Cong. § 1 (1998) (stating that the purpose of the DMCA was to "brin[g] U.S. copyright law squarely into the digital age").

55. 17 U.S.C. § 1201(a)(1)(A) (2012).

56. *See* Ryan Iwahashi, *How to Circumvent Technological Protection Measures Without Violating the DMCA: An Examination of Technological Protection Measures Under Current Legal Standards*, 26 BERKELEY TECH. L.J. 491, 500–10 (2011) (explaining seven common TPMs).

57. *Id.* at 494–500 (explaining four different tests adopted by courts to interpret technical circumvention under the DMCA).

owner to know whether their TPM "effectively control[s] access" within the meaning of section 1201.[58]

The code-based paradigm of interpreting the CFAA suffers from even more lack of clarity than the DMCA. While courts have already developed some legal standards to assess circumvention of a TPM within the meaning of section 1201 of the DMCA, courts have yet to develop *any* legal standards that define what kinds of conduct amount to "technological circumvention" under the CFAA. Critics of the code-based approach such as the Electronic Frontier Foundation (EFF) argue that the paradigm is impossible for courts to administer in a consistent manner.[59] Without statutory guidance, courts will be forced to make the oft-difficult determination of whether certain technological maneuvers, such as IP address changes, are done with or without authorization within the meaning of the statute—leaving users with little guidance as to what types of computer behavior fall safely outside the reaches of the CFAA.[60] As one example, the EFF points out that a user changes IP addresses every time he or she changes devices, logs into an online account from a new location, or uses a Virtual Private Network (VPN).[61] Under the code-based paradigm, such commonly benign and standard practices could expose the regular Internet user to CFAA liability.[62]

The tragic case of Aaron Swartz demonstrates the issues of notice and the difficulties of consistent administration under the code-based paradigm. In 2011, Internet activist Aaron Swartz was indicted after allegedly downloading 2.7 million academic papers that were freely available to any campus visitor through the JSTOR service.[63] To obtain the papers, Swartz dodged several defensive tactics employed by the school. He changed his IP address multiple times, changed his MAC address, and finally accessed the school's wiring and

58. *Id.* at 491–92.

59. *See* Brief for Electronic Frontier Foundation as Amici Curiae Supporting Defendants-Appellants at 4–9, Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058 (2016) (No. 01-17154).

60. *Id.* at 16 ("A user often has no way of knowing why a block is in place, or whether that block is aimed at them specifically."). *But see* Bellia, *supra* note 50, at 1474 (arguing that code-based barriers provide "better notice of the system owner's consent" than text-based restrictions because the user "must confront and overcome a code-based limitation in order to use the system, but he or she will not always encounter [text-based] limitations when using the system").

61. *Id.* at 13.

62. *Id.* at 14–16 ("[T]here is nothing inherently improper or unlawful about switching IP addresses to avoid an IP block").

63. Indictment, United States v. Swartz, No. 1:11-cr-10260-NMG (D. Mass. July 14, 2011).

telephony closet to "hard-wire" his laptop directly to the network for uninterrupted downloads.[64] Under the code-based paradigm, the question becomes, at what point in dodging the school's technological defenses did Swartz cross the line of authorization? And how would a user know when they have crossed the line?[65]

2. The Code-Based Approach for Algorithmic Auditors and Competitors

The code-based approach has been problematic for algorithmic auditors and competitors because it exposes them to the threat of CFAA liability for engaging in technological measures necessary for their work. For example, one technique used in both contexts is commonly referred to as "data scraping," where a user "scrapes" information from a website in bulk by sending repeated queries to the website's server.[66] In such instances, an online platform—especially a dominant one that controls the majority of data in a certain field—can effectively thwart third parties from gathering data from their website by asserting a violation of the CFAA under the code-based approach.

In *hiQ Labs v. LinkedIn*, LinkedIn did just that: It relied on the code-based approach to sue a competitor for scraping information from LinkedIn's public user profiles.[67] Data analytics company hiQ had used bots[68] to automatically scrape information from public LinkedIn profiles, including any changes made by users.[69] It then analyzed that information for its Keeper product, which told employers which of their employees were at the greatest risk of being recruited away.[70] In an attempt to stop hiQ's actions, LinkedIn alleged that hiQ had violated the CFAA under the code-based paradigm by circumventing IP address blocks, scraping data from their website using high frequency queries, and avoiding measures LinkedIn had adopted to prevent the use of automated

64. *Id.*

65. Three months before Aaron Swartz was set to go to trial, in which he faced up to thirty-five years in prison, Swartz committed suicide. In the weeks after his death, Congress members introduced "Aaron's Law," a bill inspired by Aaron's life's work in online activism. David Amsden, *The Brilliant Life and Tragic Death of Aaron Swartz*, ROLLING STONE (Feb. 15, 2013), https://www.rollingstone.com/culture/news/the-brilliant-life-and-tragic-death-of-aaron-swartz-20130215 [https://perma.cc/U8EJ-9N2T].

66. Christian Sandvig et al., Auditing Algorithms: Research Methods for Detecting Discrimination on Internet Platforms 12–13 (May 22, 2014) (unpublished manuscript).

67. 273 F. Supp. 3d 1099 (N.D. Cal. 2017).

68. A "bot" refers to a computer which automatically follows instructions in a script written by a person. For example, thousands of "bots" can be generated and instructed to visit websites and click links automatically to gather information about how the website works. *See* Complaint for Declaratory and Injunctive Relief, *supra* note 14, at 27.

69. *hiQ Labs*, 273 F. Supp. 3d at 1104.

70. *Id.*

bots.[71] The court ultimately rejected LinkedIn's reliance on the code-based approach by distinguishing between public and private data, holding that hiQ had not been "without authorization" when it accessed and scraped information from LinkedIn's *public* user profiles.[72] The court expressed concern that because hiQ was "wholly dependent" on data available only on LinkedIn's website, LinkedIn was "unfairly leveraging its power in the professional networking market for an anticompetitive purpose."[73]

Analogous situations arise in the algorithmic auditing context, where dominant online platforms can use the code-based approach to thwart auditors from scrutinizing their websites. In fact, in response to this concern, the American Civil Liberties Union (ACLU) recently filed a lawsuit, *Sandvig v. Sessions*, on behalf of several professors and a media organization challenging the constitutionality of the CFAA.[74] Two of the plaintiffs, professors Christian Sandvig and Kyratso Karahlios, planned to run a "sock puppet" study in which they would generate automated bots to simulate users of different races and scrape data from residential real estate websites to examine the websites' algorithms for racial discrimination.[75] The plaintiffs alleged that the CFAA chilled their ability to uncover and report on harmful discriminatory practices because they were "placed in reasonable fear of being prosecuted" for engaging in their work.[76]

Similar to the *LinkedIn* court, the District Court for the District of Columbia at the motion-to-dismiss stage adopted a narrow version of the code-based approach based on a distinction between public and private data. It dismissed the government's motion as applied to the plaintiffs' study, holding that scraping is "merely a technological advance that makes information collection easier;"[77] therefore scraping "from a site that is

71. *Id.*

72. *Id.* at 1108.

73. *Id.* at 1103, 1117.

74. *See* Complaint for Declaratory and Injunctive Relief, *supra* note 14. At the time of this writing, the court had recently released its opinion at the motion-to-dismiss stage. Subsequent developments in the case are therefore not incorporated in this Note.

75. *Id.* at 22–25. These "sock puppet" studies mimic the paired-testing methodology employed by the U.S. Department of Housing and Urban Development (HUD) to enforce the Fair Housing Act (FHA), which prohibits discrimination in the housing market. In those studies, HUD sent white and black "testers" to pose as equally qualified homeseekers to determine whether ethnic homeseekers were shown fewer homes than white homeseekers. *Id.* at 9–11.

76. *Id.* at 33.

77. Memorandum Opinion at 15, Sandvig et al. v. Sessions (D.D.C. Mar. 30, 2018) (No. 1:16-cv-01368).

accessible to the public is merely a particular use of information that plaintiffs are entitled to see."[78]

At the same time, the Court's holding also reaffirmed that there are certain circumstances where the code-based approach is enforceable. It reasoned that "code-based restrictions which 'carve[] out a virtual private space . . . that require[] proper authentication to gain access,' remove those protected portions of a site from the public forum," and therefore enjoy stronger CFAA enforceability.[79]

The court's decision in *Sandvig v. Sessions* will likely be perceived as a victory for the ACLU and algorithmic auditors generally because it adopted a narrow interpretation of the CFAA under the code-based approach.[80] But it is important to recognize that it also maintains significant ambiguity in the interpretation of authorization on the Internet. The Court seems to suggest that certain forms of technological savvy are permitted by law while others are prohibited with the force of the CFAA: It permits scraping and similar techniques of automatically gathering information in public forums but prohibits trespassing into virtual private spaces carved out of the public forum by "code-based restrictions." Yet it does not provide specific guidance as to how parties should navigate the difficult question of what online information is technically "in the public forum" and consequently freely accessible. For instance, is the meta-deta of a publicly available website "in the public forum"? Thus, even after the *Sandvig* court's opinion, the concerns of notice and consistent administration under the code-based approach will continue to persist for algorithmic auditors. It is also still yet to be seen how other jurisdictions will react to the *Sandvig* decision and subsequently interpret the law.

Finally, as algorithmic auditors and competing online businesses develop new computational techniques, the question of what specific types of computer behavior constitute "technological circumvention" will continue to be a moving target. Without more guidance from the courts, third parties will continue to lack certainty in determining whether they have crossed the line

78. *Id.* at 32.

79. *Id.* at 11 (quoting Kerr, *Norms of Computer Trespass*, *supra* note 50, at 1171).

80. As a logical prior to holding that the CFAA does not reach scraping or other means of automated data collection in an online public forum, the Court adopted the narrower "access" interpretation of the circuit split discussed *supra* note 25. *Id.* at 26. ("The Court finds the narrow interpretation adopted by the Second, Fourth, and Ninth Circuits—and by numerous other district judges in this Circuit—to be the best reading of the statute.").

from authorized to unauthorized behavior, and therefore may refrain from even embarking on projects in the first place.

C. TEXT-BASED APPROACH

1. The Text-Based Approach and Its Critiques

Under the text-based approach, the distinction between authorized and unauthorized access turns on whether a user has violated a written policy, such as a website terms of use (TOU) that attempts to limit the boundaries of permitted computer behavior.[81] In *United States v. Drew*, the government invoked the text-based approach in bringing a CFAA claim against Lori Drew.[82] The government contended that Drew, a mother who had created a false Myspace account to harass her 13-year-old neighbor, had violated the site's TOU and therefore had violated the CFAA.[83]

Courts and commentators have largely rejected this approach, focusing on the outsized authority the paradigm places on website TOUs. Indeed in *Drew*, though the jury found Drew guilty of a misdemeanor violation of the CFAA for violating Myspace's TOU, the Court eventually vacated the jury's conviction.[84] In *United States v. Nosal* (*Nosal I*), the Ninth Circuit also rejected the texted-based approach because "most people are only dimly aware of and virtually no one reads or understands [TOUs]."[85] The Court pointed out that because "website owners retain the right to change the terms at any time and without notice . . . behavior that wasn't criminal yesterday can become criminal today without an act of Congress, and without any notice whatsoever."[86]

---

81. Other commentators have described similar judicial approaches as paradigms based in "contract" or "policy." *See, e.g.*, Bellia, *supra* note 50, at 1451–57 (dividing the text-based approach into the "contract paradigm" and the "policy paradigm"); Rosen, *supra* note 50, 752–56 ("employer-policy approach"); Katherine M. Field, *Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 MICH. L. REV. 819, 827–29 (2009) ("contract-based interpretation").

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

83. *Id.* at 452. Unfortunately, before trial, the young girl committed suicide, which the prosecution alleged was directly caused by Drew's harassment through the false Myspace account. *Id. See also* U.S. v. Lowson, No. CRIM. 10-114 KSH, 2010 WL 9552416, at *7–8 (D.N.J. Oct. 12, 2010) (finding liability under the CFAA for defendants who had purchased more than one million event tickets for subsequent resale because they had violated website TOUs *and* code-based restrictions).

84. Drew, 259 F.R.D. 449.

85. United States v. Nosal, 676 F.3d 854, 861 (9th Cir. 2012).

86. *Id.* at 862. In *United States v. Drew*, Judge Wu explained in dicta that when applied to TOUs, the CFAA is vulnerable to the void-for-vagueness doctrine due to "actual notice deficiencies" because website owners can "unilaterally amend . . . the terms with minimal notice to users." *Drew*, 259 F.R.D. at 463–65; *see also* Bellia, *supra* note 50, at 1472–73 (criticizing

Professor Orin Kerr similarly critiqued the use of a website TOU as a proxy for the bounds of authorization under the CFAA. In his seminal article *Norms of Computer Trespass*, Kerr argued that a website TOU should not control your access to online information.[87] Kerr reasoned that a TOU should be given similar legal authority as the standard waiver of rights on the back of a baseball game ticket, which may determine your legal rights to sue, but does not control your rights to enter the ballpark.[88]

Though the Department of Justice has publicly stated to Congress that it has no intention of prosecuting harmless terms of service violations that are not in furtherance of other criminal activity,[89] commentators have argued that this type of prosecutorial discretion cannot be trusted.[90]

2. The Text-Based Approach for Algorithmic Auditors and Competitors

Of the three paradigms, the text-based approach gives the computer owner the most power to control third-party interactions and ward off algorithmic auditors and competitors. Terms are unilaterally drafted without negotiation and do not require extensive technological savvy beyond changing the language of the terms, so they can go well beyond the bounds of agency relationships or code-based restrictions with fairly minimal efforts.[91] TOUs can—and often do—explicitly prohibit conduct commonly used by algorithmic auditors and competitors, even if the conduct would not violate the CFAA under the agency or code-based paradigms of interpretation.[92] As a

---

the text-based approach because "[w]hen a court treats a policy or a contract as the basis for liability under the CFAA, it permits private parties to dictate the contours of the state" and raises constitutional concerns about whether defendants are given "fair notice of the basis for criminal sanctions").

87. Kerr, *Norms of Computer Trespass*, *supra* note 50, at 1165–67.

88. *Id.*

89. Government's Brief in Support of Defendant's Motion to Dismiss at 21, Sandvig et al. v. Sessions (D.D.C. Jun. 29, 2016) (No. 1:16-cv-01368).

90. *See* Complaint for Declaratory and Injunctive Relief, *supra* note 14, at 4; *see also* Jamie Williams, *New Federal Guidelines for Computer Crime Law Do Nothing to Reign in Prosecutorial Overreach Under Notoriously Vague Statute*, ELECTRONIC FRONTIER FOUND. (Oct. 31, 2016), https://www.eff.org/deeplinks/2016/10/what-were-scared-about-halloween-prosecutorial-discretion-under-notoriously-vague [https://perma.cc/A7L9-V5BJ]; United States v. Valle, 807 F.3d 508, 528 (2d Cir. 2015) ("While the Government might promise that it would not prosecute an individual for checking Facebook at work, we are not at liberty to take prosecutors at their word in such matters.").

91. *See, e.g.*, Snap Inc. Terms of Service, https://www.snap.com/en-US/terms/ [https://perma.cc/62JU-P3BX] (last modified Feb. 18, 2019) ("You will not solicit login credentials from another user.").

92. *See, e.g.*, Complaint for Declaratory and Injunctive Relief, *supra* note 14, at 37 ("The online research that Plaintiffs wish to conduct includes accessing websites using artificial tester

result, even though courts, commentators, and the DOJ have all publicly rejected a purely text-based approach, the uncertainty surrounding the enforceability of TOUs still serves as a deterrent for investigative work and free competition on the Internet.

In *Sandvig v. Sessions*,[93] the plaintiffs alleged that standard TOUs often prohibit the use of "the very research tools and methods that are necessary to determine whether discrimination is taking place."[94] While the complaint did not state specific TOU provisions from the targeted real estate websites in the professors' study, it did state that scraping is prohibited by TOUs of "virtually all real estate websites," and that the plaintiffs "are aware that [their] experimental design will violate websites' [TOUs]."[95] The plaintiffs alleged that without court relief, they "must refrain from conducting research or testing" that violates website TOUs to "avoid the risk of prosecution."[96]

Researcher and computer scientist Michael Tschantz ran into a similar problem when designing experiments to study Google ads and LinkedIn algorithms.[97] Tschantz and other researchers planned to run studies similar to those alleged in *Sandvig v. Sessions*, one of which would have involved placing purchased ads on Google, the other of which would have involved collecting ads shown to actual users on LinkedIn.[98] But after reading through the websites' TOUs and an article about the expansive scope of the CFAA, Tschantz put both projects on pause.[99]

Online competitors face similar legal uncertainty under the text-based approach because they commonly engage in the same technological techniques. Instead of harvesting data for investigative purposes, competitors may use scraping techniques to learn about an incumbent online service

profiles, in violation of terms of service that prohibit providing false information."); *see also Terms of Service*, FACEBOOK, https://www.facebook.com/terms.php [https://perma.cc/Y3R2-9MG8] (last modified Apr. 19, 2018) [hereinafter *Facebook Terms of Service*] ("You will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission. . . . You will not create more than one personal account.").

93. For a refresher on the background of the case, *see* discussion, *supra* Part III.B.2.

94. Complaint for Declaratory and Injunctive Relief, *supra* note 14, at 18.

95. *Id.* at 24.

96. *Id.* at 33.

97. Interview with Michael Tschantz, Principal Investigator, International Computer Science Institute, in Berkeley, Cal. (Dec. 4, 2017).

98. *Id.*

99. *Id.*; *see also* Quinn Norton, *We Should All Step Back from Security Journalism – I'll Go First*, MESSAGE (Jan. 23, 2015), https://medium.com/message/we-should-all-step-back-from-security-journalism-e474cd67e2fa [https://perma.cc/8X7J-K33U].

provider's offerings[100] or to create add-on products.[101] These behaviors lead competitors to run into common TOU terms that categorically prohibit data scraping and use of website information for third-party products.[102] Because of the inevitable clash between incumbent businesses and their incoming competitors, ambiguity surrounding the enforceability TOUs can give the incumbent a significant legal advantage and even thwart competitors from entering the market in the first place.[103]

III. REVOCATION AS A NEW PARADIGM

The agency theory, the code-based approach, and the text-based approach create a patchwork of legal standards for interpreting unauthorized access under the CFAA. In two recent cases, *Nosal II* and *Facebook*, the Ninth Circuit established yet another paradigm of interpretation: revocation.[104] Under the revocation paradigm, a user runs afoul of the CFAA if he or she continues to obtain access to a computer after his or her authorization has been explicitly revoked.

This new standard does provide some clarity for determining when a user loses the authorization because it rests on a simple concept that is easy to apply.[105] That is, to determine whether a user has accessed a computer

100. *See, e.g.*, Aaron Gordon, *How Southwest Airlines Kills Startups that Monitor Its Prices*, OUTLINE (Dec. 1, 2017), https://theoutline.com/post/2554/swmonkey-southwest-airlines-kills-startups [https://perma.cc/ZK8S-QHZG] (describing how Southwest used cease and desist letters and CFAA allegations to shut down multiple software start-ups that scraped Southwest fares to alert customers of price drops).

101. *See, e.g.*, discussion of *hiQ v. LinkedIn*, *supra* Part III.B.2.

102. *See, e.g.*, *Statement of Rights and Responsibilities*, FACEBOOK, https://www.facebook.com/terms.php [https://perma.cc/3N5L-ZC44] (last updated Apr. 19, 2018) (prohibiting data scraping); Gordon, *supra* note 100 (describing Southwest's policy, which forbids use of information on its website "for or in connection with offering any third-party product or service not authorized or approved by Southwest"); Complaint at 6, Craigslist v. 3Taps Inc., 964 F. Supp. 2d 1178 (N.D. Cal. 2013) (prohibiting "any program, application or service that enables or provides access to, use of, operation of or interoperation with craigslist is prohibited").

103. A common concern in mergers and acquisitions and venture capital funding deals is whether the company is likely to be engaged in future litigation. Even if a competitor is not deterred from pursuing a product by a TOU under the text-based approach, investment and acquisition may still depend on potential exposure to CFAA allegations. *See* Jeffrey Estes et al., *Venture Capital Investment in the United States: Market and Regulatory Overview*, Westlaw Practical Law Country Q&A 7-501-0057 (database last updated Mar. 1, 2015) (listing "disputes and potential litigation" as one area VC funds review in legal due diligence after a term sheet has been signed).

104. *See* discussion, *infra* Part IIII.A ("Revocation in *Nosal II* and *Facebook*").

105. *See* discussion, *infra* Part IIII.B ("Clarity and Notice Under a New Paradigm").

"without authorization," a court need only look into two inquiries: (1) whether the computer owner revoked authorization; and (2) whether the user continued to obtain access knowing their authorization had been revoked. Thus, in cases where the computer owner has clearly taken action to revoke a user's access, these bright-line rules do away with the hard questions that arise under the agency theory, the code-based approach, and the text-based approach.[106]

The losing parties in both *Nosal II* and *Facebook* petitioned for writ of certiorari to the Supreme Court.[107] Both petitions were denied, meaning that authorization under the CFAA will remain a national debate. Even though the Ninth Circuit in *Facebook* and *Nosal II* explicitly rejected the text-based approach[108] and some aspects of the code-based approach,[109] the existing paradigms will continue to play a role in interpreting authorization in other jurisdictions.[110]

A. REVOCATION IN *NOSAL II* AND *FACEBOOK*

In an amended opinion in *United States v. Nosal* (*Nosal II*), the Ninth Circuit articulated the revocation paradigm in a classic employer-employee case.[111] David Nosal was a senior executive who resigned from his position with executive search firm Korn/Ferry International (K/F).[112] Upon Nosal's resignation, K/F revoked Nosal's employee credentials and negotiated a one-year non-compete agreement in exchange for one million dollars.[113] During that year under contract, however, Nosal started a competing business with

106. *See* discussion, *supra* Part III.

107. Petition for Writ of Certiorari, Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058 (9th Cir. 2016) (No. 16-01344), *denied* [hereinafter Facebook Writ Petition]; Petition for Writ of Certiorari, United States v. Nosal, 844 F.3d 1024 (9th Cir. 2016) (No. 16-01105), *denied* [hereinafter Nosal Writ Petition].

108. *See Facebook*, 844 F.3d at 1067 ("[A] violation of the terms of use of a website—without more—cannot establish liability under the CFAA."); *Nosal*, 844 F.3d at 1028 ("[W]e have held that authorization is not pegged to website terms and conditions . . . .").

109. *See Facebook*, 844 F.3d at 1068 n.5 ("Simply bypassing an IP address [block], without more, would not constitute unauthorized use.").

110. However, largely due to its proximity to the Silicon Valley, the Ninth Circuit has traditionally exercised disproportionate influence in issues of technology law. Facebook Writ Petition, *supra* note 107 at 11. ("Ninth Circuit precedents are often *de facto* the law of the land on cutting-edge social media issues owing to the circuit's hegemony over Silicon Valley.").

111. *Nosal*, 844 F.3d 1024 (amended opinion). The original *Nosal II* opinion was reported on July 5, 2016. *See* United States v. Nosal, 828 F.3d 865 (9th Cir. 2016).

112. *Nosal*, 844 F.3d at 1030–31.

113. *Id.*

two prior K/F employees.[114] The team enlisted another K/F employee who stayed on with the firm and used her credentials to continue to access the firm's database.[115] When K/F caught wind of Nosal's conduct, it notified him by email, launched a private investigation, and contacted government authorities.[116]

The government sued Nosal in a criminal case, claiming that Nosal had violated the CFAA by accessing K/F's internal system "without authorization."[117] Nosal argued that he had neither circumvented any technological barriers under the code-based approach nor was he otherwise "without authorization" because he had borrowed an employee's valid credentials with her full consent.[118] The Court was unpersuaded by Nosal's technical interpretations of authorization.[119] Instead, it relied on an "unambiguous, non-technical" interpretation to hold that Nosal had acted "without authorization" because he had obtained access without "permission."[120] His credentials had been revoked when he resigned from his job and signed the non-compete agreement.[121] Thus, he no longer had permission to access the firm's database, even if he had done so with the help of an employee with valid credentials.[122] In the Ninth Circuit's words, "[u]nequivocal revocation of computer access closes both the front door and the back door."[123]

One day after the Ninth Circuit released its amended opinion in *Nosal II*, it released its amended opinion in *Facebook v. Power Ventures*.[124] In *Facebook*,

114. *Id.*
115. *Id.*
116. *Id.*
117. *Nosal*, 844 F.3d at 1031–32.
118. *Id.* at 1038–39.
119. *Id.* The Court rejected Nosal's code-based interpretation of authorization, reasoning that the statute made no mention of technological circumvention and that even if it did, "a password requirement is designed to be a technological access barrier." *Id.*
120. *Id.* at 1035–36. The Court held that Nosal needed permission from both the employee and K/F to use the employee's credentials to access the database. *Id.*; *see also* United States v. Valle, 807 F.3d 508, 524 (2d Cir. 2015) (interpreting "without authorization" as "without permission"); WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 204 (4th Cir. 2012) (interpreting authorized access as when an employer "approves or sanctions" the access).
121. *Nosal*, 844 F.3d at 1035–36.
122. *Id.*
123. *Nosal*, 844 F.3d at 1028.
124. Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058 (9th Cir. 2016) (amended opinion). The original *Facebook* opinion was reported on July 12, 2016. *See* Facebook, Inc. v. Power Ventures, Inc., 828 F.3d 1068.

Power Ventures ("Power") operated a social networking website that enabled individuals to aggregate social media from multiple accounts—for example a Facebook, a Twitter, and a LinkedIn—and view all of their information from a single Power account.[125] In December 2008, Power began a promotional campaign to attract new users to join. It placed new buttons on the website, allowing Power users with Facebook accounts to "Share with friends" by selecting from a list of connected friends and clicking, "Yes, I do!" When the button was clicked, Facebook's website automatically generated an internal message inviting the selected recipients to create Power accounts.[126]

Facebook became aware of the campaign and responded with a cease and desist letter. The letter demanded that Power terminate the campaign and enroll in Facebook's Connect program for developers, where it would be required to assent to Facebook's Developer Terms of Use. Power ignored Facebook's demands. Facebook then instituted an Internet Protocol (IP) block to prevent Power from accessing the Facebook website. Power sidestepped the block by changing its code to routinely monitor whether its IP addresses had been blocked and using proxy servers to change those IP addresses in the event of a block.[127]

Within weeks, Facebook filed a civil suit against Power and its CEO Steve Vachani under the CFAA for accessing its website "without authorization." The Northern District Court of California granted summary judgment in Facebook's favor.[128] Invoking the code-based approach, the district court held that Power had accessed Facebook's website "without authorization" because it had specifically designed its code to be immune to IP blocks by third-party servers.[129] By routinely monitoring whether its IP addresses had been blocked and using proxy servers to change the IP address in the event of a block, Power had "circumvented technical barriers" and acted "without authorization" within the meaning of the CFAA.[130]

Power appealed in the Ninth Circuit, arguing that changing an IP address should not lead to liability under the CFAA.[131] The Court was persuaded and distilled two "general rules" for interpreting authorization. First, once a defendant's permission to access a computer has been "revoked explicitly,"

125. *Facebook*, 844 F.3d at 1062–64.
126. *Id.*
127. *Id.*
128. Facebook, Inc. v. Power Ventures, Inc., 844 F. Supp. 2d 1025, 1038–39 (N.D. Cal. 2012).
129. *Id.*
130. *Id.*
131. *Facebook*, 844 F.3d 1058 (9th Cir. 2016).

"technological gamesmanship or the enlisting of a third party to aid in access" will not excuse liability.[132] Second, "a violation of the terms of use of a website—without more—cannot establish liability."[133]

Judge Graber, writing for the Court, also rejected the district court's reliance on the code-based approach, holding that "[s]imply bypassing an IP address, without more, would not constitute unauthorized use."[134] Instead, the Court held under the new revocation paradigm that Power had run afoul of the CFAA earlier in the dispute: the moment it continued its promotional campaign after receiving the cease and desist letter.[135] Once it received Facebook's cease and desist letter, Power could not continue accessing Facebook's website through "technological gamesmanship" or the "enlisting of" Facebook's users' consent.[136]

Just as Nosal argued that he had accessed K/F's computers with authority by borrowing an employee's legitimate access credentials with her consent,[137] Power also argued that it was shielded from liability because it had obtained its users' explicit consent to send messages through their Facebook accounts.[138] But again, the Court was unpersuaded by the narrow interpretation of unauthorized access.[139] The Court held that Facebook had in fact acted "without authorization" and that consent from Facebook users to send automated messages through their accounts was insufficient.[140]

B. CLARITY AND NOTICE UNDER A NEW PARADIGM

The Ninth Circuit's two closely successive opinions seem to be a deliberate attempt to articulate the revocation paradigm as a new standard, distinct from the existing paradigms. Even though the facts in *Nosal II* and *Facebook* resemble past cases—making them ripe to invoke existing notions of authorization—

132. *Id.*

133. *Id.*

134. *Id.* at 1068 n.5.

135. *Id.* at 1068. The Court went on to explain that Power's circumvention of IP barriers merely "further demonstrated that Facebook had rescinded permission." *Id.*

136. *See id.* at 1067.

137. United States v. Nosal, 844 F.3d 1024, 1038–39 (9th Cir. 2016) (arguing that Nosal had not circumvented any technical barriers because he had borrowed an employee's credentials with her consent).

138. *Facebook*, 844 F.3d at 1068.

139. *Id.*

140. *Id.* ("The consent that Power had received from Facebook users was not sufficient to grant continuing authorization to access Facebook's computers after Facebook's express revocation of permission.").

the Court refused to rely on the agency theory, the text-based approach, or the code-based approach.

For example, the Court could have found that the employee who lent her credentials to Nosal violated her duty of loyalty to the firm under the agency theory by using her authority to aid a competing business.[141] Alternatively, the Court could have held that Power acted "without authorization" by using proxy servers to sidestep an IP block, a tactic previously held to violate the CFAA under the code-based approach.[142] Or under the text-based approach, the Court could have found that Nosal and his compatriots were "without authorization" when they downloaded confidential information in violation of the firm's computer use policy.[143]

As a distinct standard of its own, the revocation paradigm does provide some clarity under the CFAA. It draws a hard line in the sand based on a rather simple concept—if I explicitly tell you to stop accessing my website, you can no longer access my website. Thus, in cases where a computer owner has taken action to revoke authorization by sending something as simple as a cease and desist letter, the revocation paradigm provides a two-step framework for courts to apply: (1) whether the computer owner revoked authorization;[144] and (2) whether the user continued to obtain access knowing the authorization had been revoked.[145] This bright-line framework provides clarity for the courts by removing the need to delve into the ill-defined scope of an agency relationship, the technical mechanics of IP blocks and data scraping, or the tough question of when TOUs should be enforceable under the CFAA.

Aside from providing a bright-line framework for courts, the revocation paradigm also provides clarity for the user. The second inquiry of the revocation paradigm introduces a notice requirement: whether the defendant accessed the computer system *knowing* that their authorization had been revoked. In *Nosal II* and *Facebook*, the Court answered yes. Power had acted

141. *Cf.* International Airport Centers, LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006) (holding that an employee had acted "without authorization" under the CFAA when he permanently deleted leaving to start a competing business).

142. *Cf.* Craigslist Inc. v. 3Taps Inc., 964 F. Supp. 2d 1178, 1180 (N.D. Cal. 2013) (holding that a competitor had scraped the Craigslist website "without authorization" in part because it used anonymous proxies to bypass an IP block).

143. *Cf.* United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009) (holding that a mother who created a false Myspace account to harass her neighbor had accessed the site "without authorization" because the site's TOU prohibited the creation of false accounts).

144. *See Facebook*, 844 F.3d at 1067 ("Facebook expressly rescinded that permission when Facebook issued its written cease and desist letter to Power . . . .").

145. *See id.* ("The record shows unequivocally that Power knew that it no longer had authorization to access Facebook's computers, but continued to do so anyway.").

"without authorization" when it "deliberately disregarded" the cease and desist letter and continued to run its promotional campaign through Facebook's website, "knowing that it was not authorized to do so."[146] Similarly in *Nosal II*, K/F had revoked Nosal's login credentials, "unequivocally convey[ing] to Nosal that he was an 'outsider' " by giving him "particularized notice of his revoked access."[147]

This focus on notice is unseen in the existing paradigms of interpretation. Under the agency theory in *Citrin*, the Court's analysis turned on whether the defendant's decision to permanently delete company data was in the best interests of the company, regardless of whether the defendant knew he had exceeded the bounds of his employment relationship.[148] The code-based approach similarly revolves around the technicalities of when unusual computer behavior amounts to "technological circumvention" without inquiring into a user's knowledge of when they have crossed the line of authorization.[149] Finally, the text-based approach provides perhaps the least amount of attention to notice by giving legal force to TOUs and other text-based documents, which are seldom read by the computer user.[150]

Thus, the revocation paradigm adds some clarity to the authorization debate. It provides a framework that is easy for courts to apply and requires that users are given some explicit notice that their permission has been revoked, both of which are entirely lacking in the existing assemblage of paradigms for interpreting authorization.

Despite this promise of clarity for the courts and for users, the revocation paradigm does not provide clarification on when or how authorization is established in the first place. In *Facebook*, the Court stated, "we need not decide whether websites such as Facebook are presumptively open to all comers, unless and until permission is revoked expressly."[151] The Court lightly suggested that initial authorization rests in part on the defendant's intent rather than any technical standard by stating that Power was not initially "without authorization" under the CFAA because it had "at least arguable permission" from the Facebook users; that is, Power "reasonably could have thought" that consent from the users alone was sufficient to run its campaign.[152] By speaking

146. *Id.* at 1068–69.
147. United States v. Nosal, 844 F.3d 1024, 1036 (9th Cir. 2016)
148. *See* discussion, *supra* Part III.A.
149. *See* discussion, *supra* Part III.B.
150. *See* discussion, *supra* Part III.C.
151. *Facebook*, 844 F.3d at 1067 n.2.
152. *Id.* at 1067.

only in terms of "arguable permission," the Court left the question open of when authorization is established in the first place.

IV. IMPLICATIONS OF THE REVOCATION PARADIGM

This Note's analysis of the revocation paradigm thus far has been positive rather than normative, focusing on what the revocation paradigm is and how it is applied in courts. But in addition to adding judicial clarity to the CFAA, the revocation paradigm also dramatically alters the landscape of the Internet by giving computer owners the power to single out any user for revocation. More specifically, a computer owner can revoke any individual's access at a moment's notice, without rhyme or reason. This singling-out power is unlike any of the existing paradigms. Employer-employee agency relationships are typically governed by boilerplate language in policies that apply to *all* employees of a company.[153] Technological barriers such as password gates or firewalls are generally erected to stop the masses from accessing a specific part of a website.[154] And TOUs are addressed to the general public.[155] Therefore, the revocation paradigm is the first of its kind to create a new powerful ability to single out an individual and revoke their access with the force of the CFAA.

This Part is dedicated to exploring the implications of this dramatic shift in power for algorithmic auditors and online competitors. As this Note will explain, algorithmic auditors and competitors are in a uniquely vulnerable position under the revocation paradigm because they both have inherently adversarial relationships with incumbent website owners. Website owners will naturally guard their data from third parties who seek to scrutinize their websites or create competing products that may draw away users. The revocation paradigm simply provides the website owner with the scalpel to single out an unwanted third party with the force of law.

153. For example, the employer in *Nosal I* had a singular computer use policy that granted "certain rights" regarding computer use to all their employees. United States v. Nosal, 676 F.3d 854, 857 (9th Cir. 2012)

154. IP blocks are perhaps the technological defense closest to providing a computer owner the ability to single out an individual. But unlike revocation by a cease-and-desist letter which is addressed to an individual, IP blocks are targeted at an IP address, which are not tied to an individual's identity. Additionally, IP blocks can be easily side-stepped intentionally or unintentionally.

155. *See, e.g.*, *Facebook Terms of Service*, *supra* note 92 (setting forth the rights and responsibilities that govern Facebook's relationship with "[all] users and others who interact with Facebook, as well as Facebook brands, products and services").

A. DANGERS OF THE SINGLING-OUT POWER

Under the revocation paradigm, the computer owner has extraordinary power to single out a user and revoke their access. This singling-out power is uniquely troubling for Internet users because of the convergence of three factors: the computer owner may single out anyone; revoke their access for any reason; and do so with minimal effort.

First, the computer owner may revoke any individual or entity's access. They may revoke access to multiple parties or just one—in one fell swoop or in succession.[156] Most importantly, they may revoke access to *any* person, regardless of the underlying reason.[157] On one hand, this makes sense. Much like a store is able to reserve the right to refuse service to a customer,[158] a computer owner should be able to control who accesses their website. On the other hand, however, when a store owner begins rejecting patrons who behave very similarly to other patrons, we begin to be concerned about underlying discrimination or unfairness.[159] In the context of the CFAA, the ability to choose any individual for revocation gives incumbent online service providers extraordinary power over the distribution of information. For instance, in *Facebook*, Facebook could have chosen to revoke Power's access, but maintain access for another social media aggregator. In the research context, a website like Google could choose to revoke access from an auditor looking at algorithmic bias against black users but maintain access for an auditor looking at discrimination against white users. Judge Chen put his finger on the issue in *hiQ v. LinkedIn*, where he found the potential arbitrariness of singling out

156. An example of this is Oracle's effort to sue third-party support suppliers. In the third-party support industry, which consists of at least eight main players, Oracle has chosen to sue only three (including Rimini). *See Secondary Software Market Providers*, CLEARLICENSING.ORG, http://www.clearlicensing.org/secondary-market/ [https://perma.cc/M9QJ-Y9B9] (listing eight Third Party Support Specialist companies); *see also* Oracle America, Inc. v. Terix Computer Company, Inc., et al., 2015 WL 1886968 (N.D. Cal. 2015) (suing two other third-party support suppliers, Terix and Maintech).

157. An example of this is the case of *Rimini Street v. Oracle*, in which Oracle sent Rimini a cease and desist letter with allegations of CFAA violations for accessing Oracle's support websites to provide third-party support to Oracle's software customers, even after Rimini had changed its manner of access to comply with prior court summary judgment orders. Rimini Street, Inc. v. Oracle Intl. Corp., 2017 WL 5158758, at *2–4 (D. Nev. 2017).

158. *See, e.g.*, *Dress Code*, NEWPORT BEACH COUNTRY CLUB (2017), http://www.newportbeachcc.com/dress-code [https://perma.cc/F3J5-NEEP] (stating that "[m]anagement reserves the right to refuse privileges to anyone found in violation of the dress code. Management in its sole discretion will determine attire in good taste").

159. The main limitation on the right to refuse service is Title II of the Civil Rights Act of 1964, which prohibits a "place of public accommodation" from discriminating on the basis of race, color, religion, or national origin. 42 U.S.C. §§ 2000a(a)–(b) (2012).

"deeply concerning," especially where 1) website owners could block access "on the basis of race or gender;" 2) political campaigns could block "selected news media, or supports of rival candidates;" and 3) companies "could prevent competitors or consumer groups from visiting their websites to learn about their products or analyze pricing."[160]

Second, revocation is non-negotiated: the computer owner has complete control over how much access to revoke and when to do so, putting users entirely at the whim of website owners.[161] Algorithmic auditors and competitors are particularly vulnerable to this factor because a website owner could choose to shut down a project at a moment's notice.[162] Facebook had full authority to determine if and when to cease Power's promotional campaign.[163] Even if Power had already invested significant financial resources or if its entire success was dependent on the campaign, under the revocation paradigm, Facebook's decision had the force of the CFAA.[164] More troubling, this asymmetrical balance of power can deter algorithmic auditors and competitors from even embarking on projects if they suspect that a certain website owner will be less sparing.[165]

160. hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1110 (N.D. Cal. 2017).

161. The unilateral nature of cease and desist letters under the CFAA is analogous to that of cease and desist letters used to enforce trademarks. For an in-depth discussion of abusive trademark letters, *see generally* Leah Chan Grinvald, *Policing the Cease-and-Desist Letter*, 49 U.S.F. L. REV. 411 (2015) (discussing the implications of abusive cease and desist letters and their particularly coercive effect on small businesses and individuals).

162. This problem is exacerbated by the fact that the vast majority of websites reserve "the right to modify their [TOU] *at any time*." Complaint for Declaratory and Injunctive Relief, *supra* note 14, at 20 (emphasis added) (stating that of twenty commonly used housing and employment websites, eighteen explicitly reserved this right). Therefore, even a user who did read the complete TOU at the time she first used the website "could be subjected to criminal liability for conduct that was not prohibited in the [TOU] at the time she read them." *Id.*

163. On the same day that Facebook first became aware of Power's promotional campaign, it sent the cease and desist letter instructing Power to terminate its activities. Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1063 (9th Cir. 2016).

164. Facebook sent the cease and desist letter on December 1, 2008—two years after Power began developing its product. *Id.* In April 2011, during the peak of litigation before the district court, Power ceased doing business altogether, *see id.*, and Steve Vachani attempted to file for bankruptcy. Aarti Shahani, *The Man Who Stood Up To Facebook*, NPR (Oct. 13, 2016), https://www.npr.org/sections/alltechconsidered/2016/10/13/497820170/the-man-who-stood-up-to-facebook [https://perma.cc/4534-N9ZQ].

165. *See* Grinvald, *supra* note 161, at 414 ("[W]hen abusive cease-and-desist letters are sent to small businesses and individuals, it is almost certain that such targets will immediately capitulate[.]"). *See also* William McGeveran, *Four Free Speech Goals for Trademark Law*, 18 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1205, 1206–07 (2008) (noting that cease and desist letters are frequently effective).

Finally, revoking authorization is cheap and easy to execute. In *Facebook,* Facebook needed only send a cease and desist letter.[166] In *Nosal II*, K/F simply removed Nosal from the company database of authorized users.[167] Both of these options are much cheaper and quicker than preventative measures under the code-based theory, where computer owners must erect technological barriers to protect their information.[168] This feature of revocation also raises concerns about encouraging overprotective behavior in the form of boilerplate revocation letters. That is, because cease and desist letters are minimally burdensome to send, computer owners can generously send form letters to potentially problematic users. Then, if they decide to bring a CFAA claim against a user *ex post*, the form cease and desist letter can serve as the legal hook under the revocation paradigm.[169]

B. DETERRING ALGORITHMIC AUDITORS

The dangers of singling-out are exacerbated for algorithmic auditors because the computer owner has an inherent incentive to guard against external scrutiny. In the same way that any organization might be wary of auditors or journalists poking around, a website owner will naturally want to discourage an auditor from examining their business practices.

Consider our introductory hypothetical. If an algorithmic auditor discovered that MBAHired was giving users like Michelle systematically inferior results because of her race, they could tarnish MBAHired's reputation in the online hiring industry by publicly disclosing that data. Naturally, to maintain control over its public relations, MBAHired has an incentive to protect its data.

Compounded with the dangers of singling-out, these misaligned incentives create an intimidating deterrent for algorithmic auditors. Even if an auditor's study is almost complete, the website owner can revoke that auditor's access with a simple cease and desist letter. This can be detrimental for a research

166. *Facebook*, 844 F.3d at 1068.

167. United States v. Nosal, 844 F.3d 1024, 1035–36 (9th Cir. 2016).

168. The Software Alliance has expressed its disapproval of any legislation that would narrow the scope of the CFAA because "it would compel many companies to erect new technical protection measures throughout their networks and support systems, reversing a trend that has contributed the growth of cloud computing, software as a service, and on-demand support." Press Release, BSA, 'Aaron's Law' is Flawed, Says BSA (June 20, 2013).

169. The Ninth Circuit in *Facebook* explicitly refrained from grappling with this question. *Facebook*, 844 F.3d at 1067 n.1 ("One can imagine situations in which . . . for example, an automatic boilerplate revocation follows a violation of a website's terms of use—but we need not address or resolve such questions on the stark facts before us.").

organization that invests significant financial resources or a PhD candidate whose academic career may depend on completion of the study. Upon receiving a cease and desist letter, both would be out of luck with no legal recourse. As a result, the revocation paradigm forces researchers to think hard about the chances of having their access revoked before committing to a project. [170]

Indeed, under the patchwork of existing paradigms, the lack of clarity in the meaning of "access without authorization" was a deterring factor for algorithmic auditors.[171] The revocation paradigm seems to solve that problem in part by providing a clear and easily administrable framework rooted in actual notice for the user. But when viewed from a policy perspective, the revocation paradigm may simply be switching out one deterrent for an even clearer, stronger one.

C. REVOCATION AS ANTI-COMPETITIVE BEHAVIOR

Similar issues arise in the online competition context. Perhaps even more so, businesses are incentivized to guard rather than share their information with competitors. Data on users and their browsing behavior is becoming increasingly important in the wake of artificial intelligence algorithms. To survive in today's online market, platforms must be able to understand their users and provide information specifically relevant to them. Thus, an incumbent company like Facebook has a strong incentive to prevent competitors from gleaning information about Facebook's platform or its users.

This phenomenon is borne out in the case law. For years, large online platform providers have used the CFAA as a legal hook to sue competitors for scraping information on their websites. In 2013, online platform Craigslist sued 3Taps under the CFAA for scraping and reproducing the contents of its website into a new user interface.[172] Similarly, in 2006 and 2007, Southwest Airlines sued BoardFirst.com and LoveCheckIn.org, two apps that provided automated check-in services built on top of Southwest's online platform.[173] In 2016, Southwest eradicated yet another competitor by sending a cease and

170. *See* note 99 and accompanying text.

171. *See* discussion, *supra* Parts III.A.2, III.B.2 and III.C.2 (discussing agency theory, the code-based approach, and the text-based approach for researchers and competitors).

172. Craigslist Inc. v. 3Taps Inc., 964 F.Supp.2d 1178, 1180 (N.D. Cal. 2013); *see also* Clark Splichal, *Recent Development: Craigslist and the CFAA: The Untold Story*, 67 FLA. L. REV. 1845, 1845–46 (2016) (describing how Craigslist has used CFAA litigation to "tak[e] on its would-be competitors in court" and prevent these competing companies from "trying to enhance and augment the Craigslist model").

173. *See* Gordon, *supra* note 100.

desist letter to Dragon Fare Scanner.[174] Dragon Fare immediately shut down their online tool, which scraped Southwest flight fares and notified customers if prices dropped for a flight they had booked.[175] In 2017, LinkedIn filed its claim against hiQ for scraping information from public LinkedIn profiles to build an analytics product.[176]

In most of these cases, the revocation paradigm would give the plaintiff's claims even more strength.[177] In *Craigslist* and *LinkedIn*, both companies sent cease and desist letters to the defendants demanding that they terminate their products.[178] Therefore, under the revocation two-step,[179] a court could have found that 3Taps and hiQ violated the CFAA when they continued to scrape data from the public websites after they had received the cease and desist letters.

The problems that the revocation paradigm brings are admittedly more sympathetic in the algorithmic auditing context. As a society, we are intimately familiar with the value of journalism and academic research as a way to expose and deter questionable behavior. Put simply, it does not seem blatantly unfair to give journalists and academics access to online information in order to root out discrimination. In the competition context, however, the parallel argument that businesses should not be able to use the CFAA to stop their competitors from accessing their computers seems less convincing. The revocation paradigm makes more sense in the competition context because a business should be able to protect their information from their competitors. Undoubtedly, the revocation paradigm enables a business to do so easily, cheaply, and efficiently.[180] Instead of spending resources to erect technological barriers—the cyber equivalent of purchasing locks, installing an alarm system,

174. *Id.*

175. *Id.*

176. hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099 (N.D. Cal. 2017); *see also* Jennifer Granick, *Is Oracle Using Computer Crime Law to Squelch Competition?*, WIRED (Mar. 28, 2017), https://www.wired.com/2007/03/circuitcourt-0328/?currentPage=all [https://perma.cc/5A7R-9H3G].

177. *See* discussion, *supra* Part IV.A (discussing how the revocation paradigm dramatically shifts power from the user to the website owner).

178. Craigslist Inc. v. 3Taps Inc., 964 F. Supp. 2d 1178, 1180 (N.D. Cal. 2013); *hiQ Labs*, 273 F. Supp. 3d at 1099.

179. The revocation two-step consists of two inquiries: 1) whether the computer owner revoked authorization; and 2) whether the user continued to obtain access knowing their authorization had been revoked. *See* discussion, *supra* Part IIII.B ("Clarity and Notice Under a New Paradigm").

180. *See* discussion *supra* Part IV.A ("Dangers of the Singling-Out Power").

or building a fence to protect a home—businesses can rest easy knowing they can revoke an unwanted user's access with a definitive cease and desist letter.

This Note does not attempt to argue that businesses should be forced to leave their information open for competitors to seize. Rather, it aims to persuade the reader that the CFAA is not the right tool to address these concerns. Our legal system has established ways of addressing business competition through unfair competition law and intellectual property law, among others. For a claim under unfair competition law, the plaintiff must prove that the defendant engaged in some unlawful, unfair, fraudulent, or misleading business practice.[181] In all forms of intellectual property law, the court cannot find liability unless there is an act of infringement or misappropriation of another's intellectual property.[182] But under the CFAA interpreted by the revocation paradigm, it becomes unnecessary for businesses to prove any wrongdoing under these other areas of law.[183] Instead, as long as they send a cease and desist letter explicitly revoking authorization, they can bring their claims under the CFAA—simply because there is a computer involved.

V. PROPOSAL: ADDING A SCIENTER REQUIREMENT

Thus far, the discussion in this Note has revolved around court-formulated paradigms for interpreting authorization. This patchwork of standards has created legal uncertainty and fear of prosecution amongst algorithmic auditors and competitors who need access to information to promote fair decision-making on the Internet. The Ninth Circuit's newly-articulated revocation paradigm now puts researchers and competitors in uniquely vulnerable positions to be singled out by incumbent online service providers looking to quash bad press or competing products that may lure users away.[184] This Note highlights that the simultaneous adoption of the revocation paradigm and transformation of the Internet through artificial intelligence algorithms calls

181. *See, e.g.*, CAL. BUS. & PROF. CODE § 17200 ("[U]nfair competition shall mean and include any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising.").

182. 17 U.S.C. § 501 (2012) (copyright infringement), 35 U.S.C. § 271 (2012) (patent infringement), 15 U.S.C. § 1114 (2012) (trademark infringement), 18 U.S.C. § 1832 (2012) (trade secret misappropriation).

183. *See supra* notes 161–162 (discussing the "deeply concerning" arbitrariness of the singling out power and the potential for abusive behavior under the revocation paradigm analogous to that found in the use of trademark enforcement cease and desist letters).

184. *See* discussion, *supra* Part IV ("Implications of the Revocation Paradigm").

for legislative definition and reform to the meaning of authorization under the CFAA.

Several Congress members have attempted to reform the CFAA through a bill known as Aaron's Law, in honor of Internet activist Aaron Swartz.[185] Their bill calls for a definition of "access without authorization" as "knowingly circumventing one or more technological or physical measures that are designed to exclude or prevent unauthorized individuals from obtaining that information"[186]—drawing an almost direct resemblance to the code-based theory.[187] Thus, as discussed, Aaron's Law brings the familiar difficulty of determining what types of conduct constitute "circumventi[on]" of a "technological or physical measure."[188]

Instead, this Note proposes that Congress add an additional scienter requirement to section 1030(a)(2)(C), the CFAA's catch-all provision.[189] Instead of proscribing any intentional access "without authorization," this Note proposes that intentional access must be done *in furtherance of a larger criminal endeavor* to give rise to CFAA liability. This additional scienter requirement would ensure that algorithmic auditors and competitors would be able to pursue their work with legal certainty and return the statute to its original intention of prosecuting and thwarting malicious hackers.

If the proposed scienter requirement had been applied in *Facebook* and *Nosal II*, Facebook would not have been able to target Power for its promotional campaign, but K/F would likely still have been able to hold Nosal liable for accessing confidential company information through another employee's credentials—both of which would have been the appropriate outcomes. Facebook would not have been able to assert claims of access without authorization under the CFAA because Power's promotional campaign was clearly not "in furtherance of a larger criminal endeavor," but rather to promote its own alternative social media website. The outcome in *Nosal* would have been less certain. To assert a CFAA claim, K/F could not have shown merely that it had revoked Nosal's authorization by removing his

185. *See supra* note 65; Kaveh Waddell, *'Aaron's Law' Reintroduced as Lawmakers Wrestle Over Hacking Penalties*, ATLANTIC (Apr. 21, 2015), https://www.theatlantic.com/politics/archive/2015/04/aarons-law-reintroduced-as-lawmakers-wrestle-over-hacking-penalties/458535/ [https://perma.cc/274S-8Q82].

186. S. 1030, 114th Cong. § 2 (2015); H.R. 1918, 114th Cong. § 2 (2015).

187. *See* discussion, *supra* Part III.B ("Code-Based Approach").

188. *See id.*

189. 18 U.S.C. § 1030(a)(2)(C) (2012) (encompassing whoever "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information *from any protected computer*") (emphasis added).

employee credentials from its internal systems. It would also have needed to prove that Nosal's access through another employee's credentials was "in furtherance of a larger criminal endeavor." Though this may sound like a tall order for K/F, it would likely have been able to prove its case because trade secret theft for commercial or economic purposes is already captured under criminal law.[190] Therefore, even with an added scienter requirement, K/F could have asserted that Nosal was engaged in a "larger criminal endeavor" to steal the company's trade secrets and economically advance his own company at the commercial expense of K/F.

A legitimate concern with adding the proposed scienter requirement is that it would result in an under-inclusive statute that fails to reach all malicious hackers—specifically by letting those who intentionally access a computer without authorization get off scot-free, as long as they are not engaged in a larger criminal endeavor. But even if the proposed scienter requirement were adopted, this would not be the case. The CFAA's other provisions already address the most egregious forms of computer hacking. For example, section 1030(a)(2)(A) and section 1030(a)(3) prohibit hacking into computers owned by financial institutions or the federal government.[191] Section 1030(a)(5) prohibits damaging computers or transmitting harmful software.[192] Section 1030(a)(6) prohibits password trafficking.[193]

Additionally, we have other laws in place to address many of the bad behaviors underlying CFAA claims. For example, trade secret law's prohibition on theft and misappropriation reaches CFAA claims where the behavior underlying the computer access involves theft of confidential information.[194] Other intellectual property and unfair competition laws provide similar legal footings. With these redundancies in place both within and without the CFAA, adding a scienter requirement to the catch-all provision of the CFAA will not

190. *See* Economic Espionage Act, 18 U.S.C. § 1832 (2012) (criminalizing theft of trade secrets for commercial or economic purposes, punishable by fines and up to 10 years in prison).

191. 18 U.S.C. § 1030(a)(2)(A) (encompassing whoever "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information contained in a financial record of a financial institution); § 1030(a)(3) (encompassing whoever "intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such [ ] computer").

192. § 1030(a)(5) (encompassing whoever, "knowingly causes the transmission of a program . . . and as a result . . . intentionally causes damage without authorization").

193. § 1030(a)(6) (encompassing whoever, "knowingly and with intent to defraud traffics . . . in any password or similar information through which a computer may be accessed without authorization").

194. *See* 18 U.S.C. § 1832 (2012).

render the statute under-inclusive. Instead, computer owners will simply no longer be able to abuse the CFAA and use it as a legal hook when nothing else will stick, simply by virtue of having a computer involved.[195]

Another response to the concern of under-inclusiveness is that the reach of the CFAA will not change significantly because the DOJ already considers the proposed scienter requirement in its charging decisions. In fact, the specific language proposed is taken almost directly from the Attorney General's 2014 memorandum, which included the proposed scienter requirement as one of the factors to be considered before initiating CFAA prosecutions.[196] In the ACLU's case challenging the CFAA, the government's reply brief states that "the Department of Justice (DOJ) has expressly stated that it has no intention of prosecuting harmless terms of service violations that are not in furtherance of other criminal activity or tortious conduct."[197]

One might ask then why this additional scienter requirement needs to be added to the face of the statute. After all, if the DOJ is not prosecuting harmless violations that are not in furtherance of a larger criminal endeavor, then auditors and competitors should not fear liability under the CFAA. However, this Note has shown that a primary concern for algorithmic auditors and competitors under the CFAA is not always criminal prosecution itself, but legal uncertainty and the threat of civil liability. Under the existing paradigms for interpreting authorization, it is nearly impossible for a user to confidently know whether their behavior is culpable under the CFAA. The agency theory, the code-based approach, and the text-based approach all fail to provide clear notice of what types of behavior fall outside the bounds of the law.[198]

195. Before the Defend Trade Secrets Act was passed in 2016, litigators often used the CFAA as a legal hook to bring otherwise state claims of trade secret misappropriation to federal court. *See* Peter Toren, *Computer Fraud and Abuse Act*, 9 No. 5 LANDSLIDE 42, 46–47 (2017) (suggesting under "IP Practice Pointers" that the CFAA "may provide a cause of action even where the information that was misused does not qualify as a trade secret under the DTSA"). *See, e.g.*, WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 204, 206 n.4 (4th Cir. 2012) (plaintiffs brought a case to federal court with 9 state-law claims and 1 federal CFAA claim).

196. Government's Reply Brief in Support of Defendant's Motion to Dismiss at 14, Sandvig v. Sessions (D.D.C. Dec. 24, 2016) (No. 1:16-cv-01368) (citing Mem. from the Att'y Gen. to U.S. Att'ys and Assistant Att'ys Gen. for the Criminal and Nat'l Sec. Divs. (Sept. 11, 2014)).

197. *Id.* at 13.

198. *See* discussion, *supra* Parts III.A.2, III.B.2, III.C.2 (discussing agency theory, the code-based approach, and the text-based approach for researchers and competitors).

With the Ninth Circuit's decisions in *Nosal II* and *Facebook,* the revocation paradigm does add some clarity as to where that line is drawn.[199]But even if revocation provides absolutely clear notice to the user, granting complete power of revocation to the computer owner replaces the uncertainty of the existing paradigms with an even stronger uncertainty of when the computer owner will exercise that power.[200]

For these reasons, the proposed scienter requirement should be lifted from the DOJ's internal policies and included in the face of the statute. Such a provision would provide the necessary notice to the public and ensure that the government sticks to its word.

VI. CONCLUSION

Today's shift towards artificial intelligence algorithms on the Internet makes it a particularly vulnerable time for the courts to adopt the revocation paradigm. The revocation paradigm brings some clarity to the legal minefield of access and authorization by imposing a bright-line concept: if I tell you to stop visiting my website, you can no longer visit my website. At the same time, it creates a powerful ability to single out third parties for revocation, which is particularly dangerous for algorithmic auditors and competitors who need access to information to promote fair decision making on the Internet. As a result, this Note calls for renewed interest in legislative reform of the CFAA. An additional scienter requirement that CFAA claims must be "in furtherance of a larger criminal endeavor" would help ensure that the Internet stays an open exchange of ideas, where bias and unfairness can be rooted out by research or defeated in healthy competition.

199. *See* discussion, *supra* Part IIII.B ("Clarity and Notice Under a New Paradigm").
200. *See* discussion, *supra* Part IV.A ("Dangers of the Singling-Out Power").