PREVENTING UNINTENDED INTERNET DISCRIMINATION: AN ANALYSIS OF THE COMPUTER FRAUD AND ABUSE ACT FOR ALGORITHMIC RACIAL STEERING

BRADLEY WILLIAMS*

Recently, a number of high-profile Internet researchers have come under fire for potentially violating the Computer Fraud and Abuse Act ("CFAA"). Their stories highlight many flaws of the CFAA when it comes to protecting researchers that data-scrape websites to investigate activity that may be illegal. Using the case example of the housing website Zillow and investigation into possible violations of the Fair Housing Act on the site, this Note examines the lack of, and need for, greater protections for researchers under the CFAA. After delving into the history of the CFAA and data scraping and analyzing how courts would likely apply the CFAA to modern researchers scraping websites to test for racial discrimination, this Note argues for a two-part, nonlitigation solution to protecting researchers. The Author's proposal consists of legislative and regulatory improvements that would narrow the scope of the CFAA as well as nonregulatory solutions that would privately incentivize compromise between researchers and website owners.

TABLE OF CONTENTS

* J.D. Candidate 2018, University of Illinois College of Law. First, I would like to thank Professor Kurt T. Lash for his guidance and insight at the initial stages of the writing process. Thank you also to the editors, members, and staff of the *University of Illinois Law Review*, especially Sam Quast. Third, thank you to my family and fiancée, Kirsten, who supported me every step of the way and scrupulously reviewed my work.

I. INTRODUCTION

In 2014, Jonathan Hall, the president of the security firm Future South Technologies, spent weeks researching a computer vulnerability called Shellshock.[1] The vulnerability allowed for hackers to execute commands remotely and, in 2014, affected many web applications.[2] Hall established a honeypot environment[3] vulnerable to Shellshock and tracked attacks leveraged at the environment.[4] Hall discovered that these attacks originated from an unlikely place: servers and computers owned by Yahoo, WinZip, and Lycos Internet.[5] Two Romanian hackers exploited these companies' servers and used their infrastructure to take advantage of other computers, including Hall's honeypot.[6] After his discovery, Hall responded quickly by executing a "kill command" on WinZip's servers to terminate the malicious program.[7] He also published his findings on his blog, after emailing the companies and the Federal Bureau of Investigation ("FBI").[8]

FBI special agents visited Hall at his New Orleans house to investigate his actions.[9] While Hall claimed that killing Shellshock's malicious code was a "justified trespass," Yahoo portrayed Hall's actions as potentially illegal under the Computer Fraud and Abuse Act ("CFAA" or "the Act")—America's anti-hacking law.[10]

1. Robert McMillian, *FBI Pays Visit to Researcher Who Revealed Yahoo Hack*, WIRED (Oct. 8, 2014, 6:30 AM), https://www.wired.com/2014/10/shellshockresearcher/.

2. *Id.*; Pavan Thorat & Pawan Kinger, *Bash Vulnerability Leads to Shellshock: What It Is, How It Affects You*, TREND MICRO (Sept. 25, 2014, 8:01 AM), http://blog.trendmicro.com/trendlabs-security-intelligence/shell-attack-on-your-server-bash-bug-cve-2014-7169-and-cve-2014-6271/.

3. A honeypot is a "system that's put on a network so it can be probed and attacked. Because the honeypot has no production value, there is no 'legitimate' use for it. This means that any interaction with the honeypot, such as a probe or a scan, is by definition suspicious." John Harrison, *Honeypots: The Sweet Spot in Network Security*, COMPUTERWORLD (Nov. 20, 2003, 12:00 AM), http://www.computerworld.com/article/2573345/security0/honeypots--the-sweet-spot-in-network-security.html.

4. McMillian, *supra* note 1.

5. *Id.*

6. *Id.*

7. *Id.* (internal quotations omitted).

8. *Id.*

9. *Id.*

10. *Id.*

Hall is not a stranger to hacking allegations,[11] and other researchers have experienced similar prosecution: For example, a judge sentenced Andrew Auernheimer and Daniel Spitler to 3.5 years in prison after writing a program that collected iPad owners' email addresses, which were publicly available from AT&T's website at the time.[12] Similarly, the United States indicted Aaron Swartz, who pled guilty to wire fraud, computer fraud, and two CFAA violations, and later committed suicide, for mass downloading articles from JSTOR—content he was permitted to access.[13] Controversial cases like these exemplify "highly criticized prosecutions of security researchers who have been charged with serious computer crimes under the [CFAA] . . . ."[14]

The data collection programs that Auernheimer and Spitler used to collect public information are expanding rapidly.[15] In 2013, data scrapers accounted for 18% of all website visitors and 23% of all Internet traffic.[16] These numbers are likely growing, as data-scraping technology becomes more efficient and widely available through open-source and proprietary technologies.[17] Following the upward trend in data-scraping technologies, courts are likely to see a rise in CFAA prosecutions.[18] Aaron Rubin and Tiffany Hu, attorneys specializing in technical-transactions litigation, agree, predicting that "in an era when data is expensive to collect, valuable to have[,] and cheap to take, the CFAA, when properly used, remains a viable tool to combat scrapers."[19]

In the wake of the Democratic National Committee hack and Russia's alleged involvement,[20] the ever-growing threat of cybercrime is a serious concern for Americans.[21] During one average day on the Internet, computer users send 500 million tweets, upload over 4 million hours of YouTube videos, "like" 5.77 billion Facebook posts, and search Google 6 billion times.[22] On that same day,

11. *See* Kevin Poulsen, *FBI Busts Alleged DDos Mafia*, SECURITYFOCUS (Aug. 26, 2004), http://www.securityfocus.com/news/9411.

12. Kim Zetter, *AT&T Hacker 'Weev' Sentenced to 3.5 Years in Prison*, WIRED (Mar. 18, 2013, 11:57 AM) [hereinafter Zetter 1], https://www.wired.com/2013/03/att-hacker-gets-3-years/.

13. *See* Larissa MacFarquhar, *Requiem for a Dream*, NEW YORKER (Mar. 11, 2013), http://www.newyorker.com/magazine/2013/03/11/requiem-for-a-dream; Noam Scheiber, *The Inside Story of Why Aaron Swartz Broke into MIT and JSTOR*, NEW REPUBLIC (Feb. 13, 2013), https://newrepublic.com/article/112418/aaron-swartz-suicide-why-he-broke-jstor-and-mit.

14. Zetter 1, *supra* note 12.

15. *See* Tom Starner, *Big Issues Surrounding Big Data*, HUM. RES. EXEC. (Nov. 3, 2016), http://www.hreonline.com/HRE/view/story.jhtml?id=534361392.

16. Aaron Rubin & Tiffany Hu, *How Website Operators Use CFAA to Combat Data-Scraping*, LAW360 (Aug. 25, 2014, 10:01 AM), https://www.law360.com/articles/569325/how-website-operators-use-cfaa-to-combat-data-scraping.

17. *See id.*; *see, e.g.*, Kyle Vanhemert, *This Simple Data-Scraping Tool Could Change How Apps Are Made*, WIRED (Mar. 4, 2014, 6:30 AM), https://www.wired.com/2014/03/kimono/.

18. *See* James Hendler, *It's Time to Reform the Computer Fraud and Abuse Act*, SCI. AM., https://www.scientificamerican.com/article/its-times-reform-computer-fraud-abuse-act/ (last visited Jan. 16, 2018).

19. Rubin & Hu, *supra* note 16.

20. Eric Lipton et al., *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.*, N.Y. TIMES (Dec. 13, 2016), https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0.

21. Karl Thomas, *The Sad Stats on State of Cybersecurity: 70% Attacks Go Unchecked*, WELIVESECURITY (Sept. 9, 2015, 1:24 PM), http://www.welivesecurity.com/2015/09/09/cybercrime-growing-concern-americans/.

22. Jeff Schultz, *How Much Data Is Created on the Internet Each Day*?, MICROFOCUS BLOG (Oct. 17, 2017), https://blog.microfocus.com/how-much-data-is-created-on-the-Internet-each-day/.

malicious actors infect 30,000 websites with malware,[23] steal 24,658 identities,[24] and hack 301,370 devices.[25] Up to 210,000 of these attacks will go undetected or unchecked.[26] Emphasizing electronic threats and national security, both Democratic nominee Hillary Clinton and Republican nominee Donald Trump addressed cybersecurity on the campaign trail during the 2016 presidential election.[27]

The CFAA could implicate researchers who data scrape websites to investigate activity that may be illegal. In April 2016, a Bloomberg investigation found that Amazon's same-day delivery service avoided predominantly African American zip codes when routing packages.[28] In July 2015, researchers at Carnegie Mellon University showed that "significantly fewer women than men were shown online ads promising them help getting jobs paying more than $200,000, raising questions about the fairness of targeting ads online."[29] More alarming, according to ProPublica, and outside the realm of cybercrime activity, the criminal justice system's sentencing algorithms may systematically overstate the likelihood of African American defendants committing repeat offenses.[30]

The CFAA has been called "the worst of the statutes Congress has passed or debated as ways to address what is vaguely shoveled into a bin labeled 'computer crime.'"[31] Originally enacted by Congress in 1984, the law was intended to protect computers owned and operated by law enforcement against unauthorized access.[32] On average 8.2% of Americans used computers in their house in 1984, and few users connected these computers to the Internet.[33] In 2011, however, 75.6% of Americans used computers in their house, and 71.7% of those users connected their computers to the Internet.[34]

Today, researchers are tempted to data scrape websites to see if algorithms are discriminating against protected classes of individuals.[35] Website owners,

23. James Lyne, *30,000 Web Sites Hacked a Day. How Do You Host Yours?*, FORBES (Sept. 6, 2013, 9:25 AM), http://www.forbes.com/sites/jameslyne/2013/09/06/30000-web-sites-hacked-a-day-how-do-you-host-yours/#28cb46263a8c.

24. *Identity Theft*, CRIME MUSEUM, https://www.crimemuseum.org/crime-library/silent-crimes/identity-theft/ (last visited Jan. 16, 2018).

25. *Staggering Figures: Half of All US Adults Hacked in Last 12 Months*, RT (May 29, 2014, 11:47 PM), https://www.rt.com/usa/162376-47-percent-americans-hacked-year/.

26. Thomas, *supra* note 21.

27. Thorin Klosowski, *Hillary Clinton and Donald Trump's Cybersecurity Platforms, Compared*, LIFEHACKER (Aug. 4, 2016, 11:00 AM), http://lifehacker.com/hillary-clinton-and-donald-trumps-cybersecurity-platfor-1784790979.

28. David Ingold & Spencer Soper, *Amazon Doesn't Consider the Race of Its Customers. Should It?*, BLOOMBERG (Apr. 21, 2016), http://www.bloomberg.com/graphics/2016-amazon-same-day/.

29. Byron Spice, *Questioning the Fairness of Targeting Ads Online*, CARNEGIE MELLON U.: NEWS (July 7, 2015), http://www.cmu.edu/news/stories/archives/2015/july/online-ads-research.html.

30. Jeff Larson et al., *How We Analyzed the COMPAS Recidivism Algorithm*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm.

31. Michael Hiltzik, *Congress' Horse-and-Buggy Computer Laws*, L.A. TIMES (Feb. 6, 2013), http://articles.latimes.com/2013/feb/06/business/la-fi-hiltzik-20130206.

32. *See* H.R. Rep. No. 98–894, at 6 (1984).

33. THOM FILE, U.S. DEP'T OF COMMERCE, ECON. & STAISTICS ADMIN., COMPUTER AND INTERNET USE IN THE UNITED STATES 1 (2013).

34. *Id.*

35. Kim Zetter, *Researchers Sue the Government Over Computer Hacking Law*, WIRED (June 29, 2016, 10:00 AM) [hereinafter Zetter 2], https://www.wired.com/2016/06/researchers-sue-government-computer-hacking-law/.

however, largely block an Internet user's ability to data scrape in their terms-of-use or service agreements, and some courts allow prosecutors to charge researchers under the CFAA for intentionally violating a website's terms of service.[36] Although the Act has a broad scope and criminalizes many Internet practices, this Note will focus specifically on Congress's impact on researchers uncovering housing discrimination under the CFAA.

This Note will examine the lack of, and need for, greater protections under the CFAA for researchers to data scrape websites. This Note uses the case example of the housing website Zillow to exemplify the issues of, and a potential solution to, the CFAA. Part II of this Note provides a short history of the CFAA, a summary of how algorithms and data scraping work, and a summary of how courts apply the Act in light of modern contract law. Addressing property websites, this Note also discusses the Fair Housing Act.

Part III applies the CFAA to modern researchers scraping websites to test for racial discrimination. Section III.A will analyze modern court enforcement of browse-wrap contracts against Internet users and whether data scraping would be considered an unauthorized access of a protected computer system under the CFAA. Section III.B analyzes Internet users' standing to sue under the Fair Housing Act as testers, whether the CFAA is an unconstitutional delegation of authority to private entities under the Fifth Amendment of the United States Constitution, and how private parties within the protected, discriminated-against class may recover under the Fair Housing Act.

Last, Part IV recommends a two-part, nonlitigation solution to protecting researchers who are combating online racial discrimination and racial steering. Section IV.A addresses the first part: legislative and regulatory improvements that would narrow the scope of the CFAA. Section IV.B addresses the second part: nonregulatory solutions that would privately incentivize compromise between researchers and website owners.

II. BACKGROUND

Congress passed the Computer Fraud and Abuse Act of 1986 as an amendment to preexisting computer fraud laws, which were first passed in 1984.[37] This Part will address the evolution of technology and its relationship to the CFAA. Sections II.A and II.B will briefly summarize the historical amendments and congressional history of the CFAA and provide a simplified description of data scraping and algorithms. Section II.C will address specific areas of contract law that may relate to the Act. Section II.D will overview tester protection under the Fair Housing Act civil rights cases. Section II.E will address the limitation the Constitution imposes on Congress from delegating its legislative authority to private parties such as website owners.

36. *See generally Conditions of Use*, AMAZON (Oct. 3, 2017), https://www.amazon.com/gp/help/customer/display.html?nodeId=508088; *Terms of Service*, YOUTUBE (June 9, 2010), https://www.youtube.com/t/terms.

37. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99–474, 100 Stat. 1213 (providing additional penalties for computer-related fraud).

A. Evolution of the Computer Fraud and Abuse Act

Congress introduced and enacted the CFAA to address a "new breed of criminal."[38] These new criminals were "technologically sophisticated criminal[s] who break[] into computerized data files."[39] Representative William J. Hughes addressed the narrow scope of the CFAA when he discussed changing the mens rea requirement from "knowingly" to "intentionally."[40] Justifying this change, Representative Hughes stated that "[i]t is not difficult to envision a situation in which an authorized computer user will mistakenly enter someone else's computer file."[41] He further stated that the new intentionality standard would "focus Federal criminal prosecutions . . . on those who evince a clear intent to enter, without authorization, computer files belong[ing] to another."[42] The congressional record did not indicate that the Act would initially apply to terms-of-use violations.[43]

Congress also conceptualized illegal entry into computerized data files by using terms from physical property law.[44] Representative Hughes described cybercriminals as "electronic trespassers" and characterized hackers as "bright, intellectually curious, and rebellious youth."[45] As related to property law, Congress argued that the CFAA needed to treat hackers as "trespassers, just as much as if they broke a window and crawled into a home while the occupants were away."[46] Even during the introduction of the bill, Congress distinguished between breaking into a computer system (a misdemeanor, titled as "trespassing") and obtaining data files and information (a felony, titled as "theft").[47] Representative Hughes ended by calling for Congress to provide the "locks" against cybercriminals in the future.[48]

1. The Comprehensive Crime Control Act of 1984

In 1984, Congress passed the Comprehensive Crime Control Act of 1984.[49] This Act made it a federal crime for someone to "knowingly access[] a computer without authorization, or having accessed a computer with authorization, use[ing] the opportunity such access provides for purposes to which such authorization does not extend . . . ."[50] This law prohibited such actions within three very specific circumstances: (1) obtaining secrets about national security; (2) misusing computers to retrieve personal financial records; and (3) entering

38. 132 CONG. REC. 9160 (1986) (statement of Rep. William J. Hughes).
39. *Id.*
40. *Id.*
41. *Id.*
42. *Id.*
43. *Id.* at 9159–61.
44. *Id.* at 9160.
45. *Id.*
46. *Id.*
47. *Id.*
48. *Id.*
49. Comprehensive Crime Control Act of 1984, Pub. L. No. 98-473, 98 Stat. 1976.
50. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, ch. 21, sec. 2101, § 1030(a), 98 Stat. 2190, 2191.

United States government computers without authorization.[51] As its first attempt to broaden criminal statutes beyond mail fraud and wire fraud, Congress focused on crimes related to national security.[52] Two years later, however, Congress amended the law to address the "crime wave of the new decade."[53]

2. The Computer Fraud and Abuse Act of 1986

Congress dramatically expanded the Comprehensive Crime Control Act, amending it through what is now known as the Computer Fraud and Abuse Act of 1986.[54] This amendment added three more computer-related crimes: (1) accessing a computer without authorization with intent to defraud; (2) prohibiting access to a computer without authorization and altering information which causes $1,000 or more in damage or misdiagnosis; and (3) trafficking with computer passwords.[55] For the first two of the three new crimes, Congress strictly limited the crimes to "[f]ederal interest computer[s]," defined narrowly as the following:

> (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects the use of the financial institution's operation or the Government's operation of such computer; or
> (B) which is one of two or more computers used in committing the offense, not all of which are located in the same State.[56]

Subsequent statutes refined these six activities to allow for nongovernmental persons to seek civil damages if the total damages were greater than $5,000.[57]

Notably, Congress added this new limitation to apply to computers in different states at a time when few computers were connected to interstate networks.[58] Congress included this language to ensure it had enumerated authority to pass the proposed amendment. At the time of enactment, Congress was concerned with "areas where there is a compelling Federal interest in the prevention and punishment of computer crimes," especially "computer crimes affecting the Federal Government itself and . . . activities in which there is unique Federal interest."[59] The scope of this amendment was, in part, cybercrimes involving

51. *Id*; *see* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1564 (2010).

52. *See* Kerr, *supra* note 51, at 1564.

53. 132 CONG. REC. 9160 (1986) (statement of Rep. William J. Hughes).

54. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213.

55. 18 U.S.C. § 1030(a)(4)–(6) (1988).

56. *Id.* § 1030(e)(2) (limiting the scope of this new criminal activity to federally operated computers or multiple, interstate computers at a time when merely hundreds of personal computers were connected to the Internet).

57. *See, e.g.*, Computer Abuse Amendments Act of 1994, Pub. L. No. 103-322, 108 Stat. 2097 (applying § 1030(a)(5) to any computer damage incurred accidentally and allowing for individuals to seek civil damages).

58. Tellingly, now the number of networks that were connected to some form of ARPANET could be quantified in one drawing. *See* Marty Lyons, *Primary Internet Gateways–1985 June 18*, LIVING INTERNET, http://www.livingInternet.com/i/ii_arpanet_gateways.htm (last visited Jan. 16, 2018).

59. 132 CONG. REC. 9160 (1986) (statement of Rep. William J. Hughes).

domestic interstate communication, but it was primarily motivated by crimes involving foreign criminals infiltrating government computers.[60]

3. The National Information Infrastructure Protection Act of 1996

Further amendments and new legislation expanded the CFAA to effectively control all Internet users. In 1996, at the beginning of the popularization of personal computing and the Internet,[61] Congress dramatically expanded the CFAA under "the Economic Espionage Act in a subtitle labeled the National Information Infrastructure Protection Act of 1996."[62] The legislation was a part of the Economic Espionage Act because it did not originally make it past the Judiciary Committee.[63] It was later signed into law by President Bill Clinton under larger espionage and financial protection legislation.[64]

Importantly, the second enumerated crime under the CFAA, computer misuse to retrieve financial records, was no longer limited to "financial record[s] of a financial institution . . . card issuer . . . [or] a consumer reporting agency on a consumer" or "information from any department or agency of the United States."[65] After this amendment, a computer user that "intentionally access[ed] a computer without authorization or exceed[ed] authorized access, and thereby obtain[ed] . . . information from any protected computer" violated Federal law.[66]

Contrary to the broad language of the statute, though, Congress was focused on protecting national security when passing the National Information Infrastructure Protection Act.[67] The CFAA, when first enacted in 1986, was passed to "protect[] . . . computerized credit records and computerized information relating to customers' relationships with financial institutions."[68] The 1996 amendment was similarly proposed in response to a growing concern that American corporations would suffer financial harm from hackers infiltrating their computer systems.[69]

4. Congress Expands Actions Governed by the CFAA

In 1994, in response to the increase in civil computer injuries against other individuals, Congress expanded the CFAA to include any unauthorized access and obtaining of information.[70] Senator Patrick Leahy emphasized that the CFAA encouraged Congress to "use speedier domestic procedures in support of

60. David Thaw, *Criminalizing Hacking, Not Dating: Reconstructing the CFAA Intent Requirement*, 103 J. CRIM. L. & CRIMINOLOGY 907, 927 n.81 (2013).

61. *See generally World Wide Web Timeline*, PEW RES. CTR. (Mar. 11, 2014), http://www.pewInternet.org/2014/03/11/world-wide-web-timeline/.

62. Economic Espionage Act of 1996, Pub. L. No. 104-294, tit. II, 110 Stat. 3488, 3491.

63. Christine D. Galbraith, *Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites*, 63 MD. L. REV. 320, 330 n.80 (2004).

64. *Id.*

65. 18 U.S.C. §§ 1030(a)(2)(A)–(B) (2012).

66. *Id.* § 1030(a)(2)(C).

67. George Roach & William J. Michiels, *Damages Is the Gatekeeper Issue for Federal Computer Fraud*, 8 TUL. J. TECH. & INTELL. PROP. 61, 72 (2006).

68. S. Rep. No. 99–432, at 6 (1986).

69. Galbraith, *supra* note 63, at 330.

70. *Id.* at 329.

international hacker cases, and create the option of prosecuting such criminals in the United States."[71] Moreover, he stated that this new provision would "ensure that [the United States] government w[ould] be able to conduct domestic investigations and prosecutions against hackers from this country who hack into foreign computer systems and against those hacking through the United States to other foreign venues."[72]

By expanding the CFAA's language pertaining to unauthorized access, Congress intended to broaden the scope of computer crimes to include private hackers that did not directly affect federal computing.[73] When amending the Act, however, the sponsors of the legislation did not intend to "open the floodgates to frivolous litigation."[74]

5. Congress Expands Computers Governed by the CFAA

Congress also expanded the scope of computers governed by the CFAA. As previously stated, Congress amended the CFAA to broadly criminalize users who "intentionally access a computer without authorization or exceed[] authorized access, and thereby obtain[] . . . information from any protected computer."[75] The CFAA defines "protected computer" as one of two types of computers: (1) "a computer – exclusively for the use of a financial institution or the United States Government ";[76] or (2) "a computer . . . which is used in or affecting interstate or foreign commerce or communications . . . ."[77]

Congress's expansive authority under the Interstate Commerce Clause[78] allows it to effectively control any computer connected to the Internet today. Under the Commerce Clause, Congress is permitted broad authority to regulate the channels, instrumentalities, and activities that substantially affect interstate commerce.[79] Courts have held that the Internet is an instrumentality of interstate commerce[80] and that, under the CFAA's protected computer definition, all Internet of Things ("IoT") devices[81] connected to the Internet are subject to the

71. 146 CONG. REC. S10915 (daily ed. Oct. 24, 2000) (statement of Senator Patrick Leahy).

72. *Id.*

73. Galbraith, *supra* note 63, at 329.

74. *Id.* (citing 136 CONG. REC. S4614 (daily ed. Apr. 19, 1990) (statement of Sen. Leahy).

75. 18 U.S.C. § 1030(a)(2012) ("Whoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer . . . shall be punished as provided in subsection (c) of this section.").

76. *Id.* § 1030(e)(2)(A).

77. *Id.* § 1030(e)(2)(B).

78. U.S. CONST. art. I, § 8, cl. 3.

79. United States v. Lopez, 514 U.S. 549, 558–59 (1995).

80. United States v. Hornaday, 392 F.3d 1306, 1311 (11th Cir. 2004) ("Congress clearly has the power to regulate the Internet, as it does other instrumentalities and channels of interstate commerce, and to prohibit its use for harmful or immoral purposes regardless of whether those purposes would have a primarily intrastate impact.").

81. Internet of Things devices are devices that are connected to the Internet. These devices include computers and cellphones as well as "coffee makers, washing machines, headphones, lamps, wearable devices and almost anything else you can think of" that has access to the Internet. *See* Jacob Morgan, *A Simple Explanation of 'The Internet of Things,'* FORBES (May 13, 2014, 12:05 AM), http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-Internet-things-that-anyone-can-understand/#14c579068284.

CFAA.[82] The Act could, hypothetically, apply to approximately 6.4 billion devices today that have access to the Internet.[83]

B. How Algorithms and Data Scraping Work

It is critical to be familiar with the technology powering research today to understand the potential liability for data scrapers under the CFAA. When the Advanced Research Projects Agency Network ("ARPANET"), a predecessor to the World Wide Web, was created and released commercially in 1974,[84] Congress could not have fathomed the technological advancements and societal reliance on the Internet today.[85] Since 1974, the Internet has dramatically expanded, and Internet communications are much more complex.[86] In 1976, Apple introduced the first window-style personal computer, which included an astounding four KBz of memory and 1.023 MHz of processing speed.[87] Today, the average computer has four GHz of memory[88] (1,000,000 times larger than in 1976) and 2 GHz of processing speed[89] (2,000 times faster than in 1976). Faster computers with more memory have radically transformed how society understands the world and how modern courts apply antiquated computer laws.[90]

With increased speed and storage, new research innovations allow for mass data harvesting. Researchers today use algorithms and complex software to collect data from the Internet.[91] These technologies can lead to researchers accessing information the website owner explicitly does not authorize.[92] Consequently,

82. *See* United States v. Kramer, 631 F.3d 900, 903 (8th Cir. 2011) (applying the CFAA's unauthorized access and obtaining restriction to cellular phone calls and text messages); United States v. Trotter, 478 F.3d 918, 921 (8th Cir. 2007) (applying the CFAA to computers).

83. Press Release, Gartner, Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent from 2015 (Nov. 10, 2015), http://www.gartner.com/newsroom/id/3165317 (estimating that the number of connected devices will accumulate to 20.8 billion devices by 2020).

84. Kim Ann Zimmerman & Jesse Emspak, *Internet History Timeline: ARPANET to the World Wide Web*, LIVE SCI. (June 27, 2012, 10:46 AM), http://www.livescience.com/20727-Internet-history.html.

85. Sandra F. Chance & Christina M. Locke, *Struggling with Sunshine: Analyzing the Impact of Technology on Compliance with Open Government Laws Using Florida as a Case Study*, 21 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1, 3 (2010) ("Technologies such as the Internet, cell phones and laptop computers were not contemplated when many government entities formulated their laws governing access to records and meetings.").

86. Zimmerman & Emspak, *supra* note 84 (spanning from 1973, when the University College of London connected to the Royal Radar Establishment in Norway using ARPANET, to today, where a single website like Facebook can have over 400 million active users).

87. *Apple I*, APPLE MUSEUM, http://applemuseum.bott.org/sections/computers/a1.html (last visited Jan. 16, 2018).

88. *How Much Memory or RAM Should My Computer Have?*, COMPUTER HOPE (Apr. 26, 2017), http://www.computerhope.com/issues/ch001189.htm.

89. *What Affects a Computers Performance*, LEHIGH, https://www.lehigh.edu/~inimr/computer-basics-tutorial/computersperformance.htm (last visited Jan. 16, 2018).

90. Jeff Hawkins, *The Terminator is Not Coming. The Future Will Thank Us*, RECODE (Mar. 2, 2015, 7:00 AM), http://www.recode.net/2015/3/2/11559576/the-terminator-is-not-coming-the-future-will-thank-us.

91. Mylynn Felt, *Social Media and the Social Sciences: How Researchers Employ Big Data Analytics*, BIG DATA & SOC'Y, Jan.–June 2016, at 1–2.

92. *See, e.g.*, Tiffany Hu & Aaron Rubin, *Data for the Taking: Using the Computer Fraud and Abuse Act to Combat Web Scraping*, SOCIALLY AWARE (July 21, 2014), http://www.sociallyawareblog.com/2014/07/21/data-for-the-taking-using-the-cfaa-to-combat-web-scraping/.

researchers may inadvertently open themselves to criminal and civil liability under the CFAA.[93]

1. Algorithms

The term "algorithm" is defined as "a process or set of rules to be followed in calculations or other problem-solving operations, especially by a computer."[94] An algorithm is a mathematical formula implemented in a computer program that has three distinct characteristics: (1) "it must stop at a certain point"; (2) "it must have well-defined instructions with specific steps"; and (3) "it must be effective in solving the problem it was designed to solve."[95] Website developers and software programmers implement many popular algorithmic functions in their programs today, such as RSA, Merge Sort, Quick Sort, Heap Sort, and Proportional Integral Derivative (among other functions).[96]

Algorithms determine the top posts users see on Facebook, the news that is prioritized for users on Google, and the apartment listings recommended to buyers on websites.[97] Algorithms also compress data files to make systems cheaper, more efficient, and easier to transfer.[98] These digital recipes power our world.[99]

2. Data Scraping

One way to analyze websites that use algorithms is by data scraping, or "extracting information from a local machine, a database, or even . . . from the Internet."[100] A similar concept is data mining, or "the process of analyzing data from different perspectives and summarizing it into useful information . . . ."[101] A web-scraping software "automatically load[s] and extract[s] data from multiple pages of websites based on [a] requirement.[102] These programs are difficult to set up and use[103] but are incredibly powerful tools for collecting and eventually analyzing data from websites.[104]

93. *Id.*

94. *What are Algorithms?*, FUTURISM, https://futurism.com/images/what-are-algorithms/ (last visited Jan. 16, 2018).

95. *Id.*

96. *Id.*

97. Will Rinehart, *Primer: Why Algorithms are Important to Public Policy*, AM. ACTION F. (Oct. 5, 2016), https://www.americanactionforum.org/insight/primer-algorithms-important-public-policy/.

98. *What Are Algorithms?*, *supra* note 94.

99. Rinehart, *supra* note 97.

100. Arpan Jha, *Web Crawling: Data Scraping vs. Data Crawling*, PROMPT CLOUD (May 30, 2012, 6:51 PM), https://www.promptcloud.com/data-scraping-vs-data-crawling.

101. *Data Mining: What is Data Mining*, CDA INST., http://www.data-analysts.org/view/48.html (last visited Jan. 16, 2018).

102. *What is Web Scraping?*, WEBHARVY, https://www.webharvy.com/articles/what-is-web-scraping.html (last visited Jan. 16, 2018).

103. *Id.*

104. *Advantages and Disadvantages of Data Mining*, ZENTUT, http://www.zentut.com/data-mining/advantages-and-disadvantages-of-data-mining/ (last visited Jan. 16, 2018).

For website owners, attempting to limit data scrapers from crawling through their website is very difficult.[105] Website owners cannot block IP addresses[106] because data scrapers use numerous addresses when scraping.[107] To protect their data, website owners attempt to protect themselves through copyright protection, browse-wrap agreements, and click-wrap agreements.[108]

C. Contract Law and Website Terms of Use

Since the population of online contracts, courts have been developing contract law to determine whether an individual computer user has agreed to a website's terms of use.[109] Website managers are free to determine their terms of use and define what constitutes an unauthorized access of data that is publicly available on their websites.[110] These terms and services are usually not read by the average Internet user and are subject to change without notifying the user.[111] Previously, the United States Courts of Appeals have held that a website's terms of use were contractual agreements.[112] Some courts have reasoned, however, that these terms of use are not legally binding.[113]

States will need to consider both policy implications as the law continues to develop.[114] Proponents of browse-wrap agreements may argue that browse-wrap contracts, which are contracts users accept through implied consent when using a website, should be enforceable because they allow users adequate notice of the existence of the terms and provide users a meaningful opportunity to review the terms.[115] Additionally, browse-wrap agreements provide users adequate notice and require a specific action to manifest assent, and users voluntarily assent to the terms.[116] Policy implications, however, favor not enforcing browse-wrap agreements: The terms are generally preprinted, provide no bargaining power to consumers, and are rarely read or understood by consumers.[117]

105. Lisa Allen, *Data Scraping and the Importance of Well-Drafted Website Terms of Use*, SAND HILL (Oct. 15, 2014), http://sandhill.com/article/data-scraping-and-the-importance-of-well-drafted-website-terms-of-use/.

106. "IP" stands for Internet Protocol. An IP address consists of four numbers, between zero and 255, separated by periods. An IP address functions as an identity for Internet communication. *See What Is an IP Address? What Does It Do?*, WHATISMYIPADDRESS.COM, http://whatismyipaddress.com/ip-address (last visited Jan. 16, 2018).

107. Allen, *supra* note 105.

108. *Id.*; *see also infra* Section II.C.

109. Woodrow Hartzog, *Website Design as Contract*, 60 AM. U. L. REV. 1635, 1645 (2011) ("Fundamentally, contracts exist to bind parties to promises by creating legal obligations. On a website, these promises can be made in nearly any form and can appear anywhere. Promises made as part of a negotiation can be more attractive for users; negotiation is typically deliberative, thus negotiated terms are presumably understood and satisfactory to contract adherents.").

110. Samantha Jensen, *Abusing the Computer Fraud and Abuse Act: Why Broad Interpretations of the CFAA Fail*, 36 HAMLINE L. REV. 81, 108 (2013).

111. *Id.* at 108–09.

112. *See, e.g.*, ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1453 (7th Cir. 1996).

113. *See, e.g.*, Sprecht v. Netscape Commc'ns Corp., 306 F.3d 17, 25 (2002).

114. Cheryl B. Preston, *"Please Note: You Have Waived Everything": Can Notice Redeem Online Contracts?*, 64 AM. U. L. REV. 535, 565 (2015).

115. *See* Juliet M. Moringiello & William L. Reynolds, *From Lord Coke to Internet Privacy: The Past, Present, and Future of the Law of Electronic Contracting*, 72 MD. L. REV. 452, 461 (2013).

116. *Id.* at 466–67.

117. *Id.* at 479.

Subsection II.C.1 discusses adhesion contracts and how corporations rely on this method of contracting. Subsections II.C.2 and II.C.3 provide examples for how courts interpret one type of adhesion contract used online—browse-wrap agreements.

1. Adhesion Contracts

This issue stems from the evolution of adhesion contracts and their use in online platforms.[118] An adhesion contract is a "standard-form contract prepared by one party, to be signed by another party in a weaker position, usu[ally] a consumer, who adheres to the contract with little choice about the terms."[119] The standard-form contracts allow businesses to complete contracts without the assistance of an attorney.[120] Beginning in the 1960s, adhesion contracts became very popular in specific markets, like insurance markets, to allow corporations to quickly draft contracts.[121] Unfortunately, these contracts significantly reduce the possibility of consumers negotiating for a specific good.[122]

Companies use adhesion contracts (most notably, for website activity) to force consumers to agree to terms which are likely not in their best interest.[123] Consumers assent to these terms on a take-it-or-leave-it basis, creating the false impression that consumers have fully read and understood the terms of the contract before agreeing to them.[124] Fundamentally, these contracts do not require the same type of mutual assent that would be provided in nonadhesion contracts, and consumers typically will agree to harsh terms favoring the drafter of the contract.[125] Courts have generally held, however, that these contracts are enforceable based on the premise that both parties willingly agreed to and understood the terms.[126] These adhesion contracts exist in two forms: online browse-wrap contracts and click-wrap contracts.[127] This Note only addresses browse-wrap contracts because they primarily relate to data-scraping restrictions.

2. Browse-wrap Contracts Under Specht

A browse-wrap agreement is a contract "typically presented at the bottom of the web site where acceptance is based on 'use' of the site."[128] These agreements give users a conspicuous notification of a contract, usually appearing as a hyperlink on the website under the "guise" of a terms of use or terms-of-use

118. Aaron E. Ghirardelli, *Rules of Engagement in the Conflict Between Businesses and Consumers in Online Contracts*, 93 OR. L. REV. 719, 722 (2015).

119. *Adhesion Contract*, BLACK'S LAW DICTIONARY (10th ed. 2014).

120. Ghirardelli, *supra* note 118.

121. W. David Slawson, *The New Meaning of Contract: The Transformation of Contracts Law by Standard Forms*, 46 U. PITT. L. REV. 21, 50 (1984).

122. *See id.* at 32.

123. *See id.* at 34.

124. *Id.* at 31.

125. *Id.*

126. *See, e.g.*, CompuCredit Corp. v. Greenwood, 565 U.S. 95, 104 (2012).

127. Ghirardelli, *supra* note 118, at 728.

128. Ian Rambarran & Robert Hunt, *Are Browse-Wrap Agreements All They Are Wrapped Up to Be?*, 9 TUL. J. TECH. & INTELL. PROP. 173, 176 (2007).

agreement.[129] The terms of the agreement "do not usually appear on the same page as the original hyperlink but are connected to another page . . . incorporated by reference."[130] Users are usually unaware of the terms of use of a contract, even after supposedly assenting to them.[131]

In some cases, courts have rejected browse-wrap agreements because both parties have not mutually assented to the terms.[132] In *Specht v. Netscape Communications Corp.*, the browse-wrap contract in question concerned free software downloaded on Netscape's website.[133] After clicking a link on the website to download the free software, the plaintiff went to a screen asking whether the user wanted to "[d]ownload with [c]onfidence [u]sing SmartDownload!"[134] After clicking the link, the software prompted the plaintiff to install another piece of software, titled "Communicator," which required the plaintiff to agree to the terms of use. Users would be directed to start the download, and by clicking the download, the plaintiff assented.[135]

Unbeknownst to the user, though, Netscape installed two pieces of software on the plaintiff's computer after clicking the link: the aforementioned Communicator software and SmartDownload.[136] The terms and conditions of SmartDownload were inaccessible to the plaintiff unless the plaintiff opened an additional website hidden at the bottom of the page.[137] To review the contractual terms, the plaintiff had to scroll all the way down to the bottom of the page.[138] Upon learning about SmartDownload's installation, the plaintiff brought a class action lawsuit against Netscape, claiming the SmartDownload software violated his privacy.[139] Netscape moved to compel arbitration based on SmartDownload's terms of use, and the district court denied the motion because a contractual relationship between the plaintiff and the website did not exist.[140]

The Second Circuit held that this browse-wrap agreement was invalid.[141] It reasoned, in part, that website users downloading software did not assent when the terms of use only appeared after the download.[142] In agreements like this, the court further reasoned that two parties could not have mutually agreed, or assented, to the terms of use.[143] Tellingly, the court stated that a "reasonably prudent" Internet user would not have known they accepted the terms and service of SmartDownload if they were required to scroll to the bottom of a hidden window.[144]

129. *Id.*
130. *Id.*
131. *Id.*
132. *See, e.g.*, Specht v. Netscape Commc'ns Corp., 306 F.3d 17, 40 (2d Cir. 2002).
133. *Id.* at 21.
134. *Id.* at 22.
135. *Id.* at 23.
136. *Id.*
137. *Id.*
138. *Id.* at 23–24.
139. *Id.* at 25.
140. *Id.* at 21.
141. *Id.* at 40.
142. *Id.* at 23.
143. *Id.* at 28–30.
144. *Id.* at 35.

3. Browse-wrap Contracts Under Register.com, Inc.

While some courts have invalidated contracts based on a "reasonably prudent" Internet user standard, many courts have not been so forgiving, upholding browse-wrap contracts as enforceable contracts.[145] Revisiting this holding, the Second Circuit addressed this issue in *Register.com, Inc. v. Verio, Inc*.[146] The plaintiff, Register.com, is a company that registers and issues domain names to others preparing to establish websites.[147] The defendant, Verio, Inc., would download the registration names of new users submitted by Register.com.[148] When completing the download, Verio, Inc. would receive an email from Register.com, Inc. and the terms of use Verio, Inc. agreed to by downloading this information.[149] Verio, Inc. began using this downloaded information to solicit to new domain owners by direct mail and telephone, which was against Register.com's policy.[150] Verio, Inc. refused to stop this practice after Register.com demanded that they cease.[151] The court granted Register.com's preliminary injunction, and Verio, Inc. appealed.[152]

Clarifying *Specht*, the Second Circuit affirmed the district court's order and held that a browse-wrap contract may be enforceable.[153] It reasoned that a browse-wrap contract was valid even if the website provider disclosed the terms of the contract at a later time, and if parties had adequate notice of the terms (in this case, behavior that implies an awareness of the terms and actions manifesting assent to the terms).[154] When adequate notice exists, a reasonably prudent Internet user should be aware of the contractual terms and is deemed to have mutually assented to the agreement.[155]

While the same circuit decided these cases, many federal circuit courts are similarly clarifying when browse-wrap contracts are enforceable against the consumer.[156] Some judges enforce browse-wrap contracts when a user assents to a website's terms of use and reasonably implies assent based on his or her conduct (such as continued use after the user received notice of the terms of use).[157] Some judges refuse to enforce browse-wrap contracts, however, when the user does not see the terms-of-use agreement, even if the terms explicitly say

145. *See, e.g.*, Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 402 (2d Cir. 2004).
146. *Id.*
147. *Id.* at 395.
148. *Id.* at 396.
149. *Id.*
150. *Id.*
151. *Id.* at 397.
152. *Id.* at 395.
153. *Id.* at 402.
154. *Id.* at 401 ("Verio's argument might well be persuasive if its queries addressed to Register's computers had been sporadic and infrequent. If Verio had submitted only one query, or even if it had submitted only a few sporadic queries, that would give considerable force to its contention that it obtained the WHOIS data without being conscious that Register intended to impose conditions, and without being deemed to have accepted Register's conditions. But Verio was daily submitting numerous queries, each of which resulted in its receiving notice of the terms Register exacted.").
155. *Id.* at 401–02.
156. *See, e.g.*, Nicosia v. Amazon.com, Inc., 834 F.3d 220, 233 (2d Cir. 2016); Nguyen v. Barnes & Noble, Inc., 763 F.3d 1171, 1176 (9th Cir. 2014); Schnabel v. Trilegiant Corp., 697 F.3d 110, 125 (2d Cir. 2012).
157. Preston, *supra* note 114, at 575.

that using a website constitutes acceptance and adherence to the website's terms.[158] Based on market reliance on this method of contracting to control consumer's conduct, however, these seemingly unilateral statements are still enforceable today, regardless of whether consumers see, read, understand, or want to change the terms of use.[159]

D. The Fair Housing Act

In its current form, the CFAA broadly applies to any unauthorized access or use of a protected property affecting interstate commerce.[160] Theoretically, a hacker testing a website may violate the terms of use of a website under the Act, even if their tests were intended to root out violations against protected classes of individuals.[161] The legislative, executive, and judiciary branches have largely resolved this issue for tangible property rights, under the Fair Housing Act.[162] By nature of its subject matter, however, the CFAA applies to intangible—not tangible—actions.[163]

1. Early History

The Thirteenth Amendment to the United States Constitution bans racial discrimination, both privately and publicly, in the sale and rental of property.[164] In 1968, President Lyndon B. Johnson enacted Title VIII and Title IX of the Civil Rights Act of 1968 (hereinafter referred to as "the Fair Housing Act")[165] under the Thirteenth Amendment's broad authority "to enforce [the Amendment restricting slavery] by appropriate legislation."[166] Courts liberally construe the Fair Housing Act's language to be "broad and inclusive" and "give [a] generous construction to effectuate its stated policies."[167]

The Fair Housing Act broadly prohibits, for example, discrimination against people based on race, color, religion, sex, familial status, or national origin in renting or purchasing housing.[168] For this Note, I will focus on three types of discrimination, all violations based on the aforementioned protected classes of individuals. First, the Fair Housing Act makes it unlawful to "discriminate against any person in the terms, conditions, or privileges of sale or rental of a dwelling, or in the provision of services or facilities in connection

158. Mark A. Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 460 (2006).
159. *Id.*
160. 18 U.S.C. § 1030(e)(2)(B) (2012).
161. *See, e.g.*, United States v. Drew, 259 F.R.D. 449, 466 (C.D. Cal. 2009).
162. *See* Gladstone Realtors v. Vill. of Bellwood, 441 U.S. 91 (1979).
163. Deborah F. Buckman, Annotation, *Validity, Construction, and Application of Computer Fraud and Abuse Act (18 U.S.C.A. § 1030)*, 174 A.L.R. Fed. 101, 113 (2001).
164. *See* U.S. CONST. amend. XIII; Jones v. Alfred H. Mayer Co., 392 U.S. 409, 439–40 (1968).
165. 42 U.S.C. § 3601–3619 (1968).
166. U.S. CONST. amend. XIII, § 2.
167. 93 AM. JUR. 3D *Proof of Facts* 429 (2007) (citing Samaritan Inns, Inc. v. District of Columbia, 114 F.3d 1227 (D.C. Cir. 1997)). The policy of the Fair Housing Act, in part, is to provide fair housing throughout the United States in accordance with an individuals' constitutional rights. *See* Trafficante v. Metro. Life Ins. Co., 409 U.S. 205, 210–11 (1972).
168. 42 U.S.C. § 3604 (2012).

therewith . . . ."[169] Second, it is unlawful to steer individuals in housing based on race, or "intention[ally] to make any such preference, limitation, or discrimination . . . ."[170] Third, it is unlawful to restrict housing based on race, or to "represent to any person . . . that any dwelling is not available . . . ."[171] Thus, landlords that racially steer applicants or refuse to rent properties to specific individuals based on race violate the Fair Housing Act.[172]

2. The Fair Housing Act Protects Testers

To ensure landlords provide the same information and availability to all individuals, the Supreme Court has uniformly allowed for testers to expose racial discrimination and representation.[173] Early in the Fair Housing Act's history, the Supreme Court tackled this problem in *Gladstone Realtors v. Village of Bellwood*,[174] addressing testers' standing to sue when realtors racially "steer" or "channel" purchasers depending on their race.

In this case, Village of Bellwood residents sued real estate personnel and brokers at Gladstone for two reasons: (1) realtors allegedly "steered prospective Negro home buyers toward an integrated area of Bellwood approximately 12 by 13 blocks in dimension and away from other, predominately white areas"[175] and (2) realtors allegedly steered "[w]hite customers . . . away from the integrated area of Bellwood."[176] Residents from the Village of Bellwood uncovered Gladstone's racially discriminatory practices by employing "testers," or individuals alleging, falsely, to Gladstone that they wanted to purchase homes when their true purpose was to "determine whether petitioners were engaging in racial steering . . . ."[177] Gladstone moved for summary judgment, arguing that the defendants did not have standing to sue under the Fair Housing Act.[178] The district court granted the motion, and the court of appeals reversed.[179]

Upon reaching the Supreme Court, a seven-Justice majority held that the Village of Bellwood's residents had standing to sue.[180] The Court stated that tester standing under the Fair Housing Act is as broad as Article III of the Constitution permits,[181] which extends to circumstances where testers expose landlords that racially steer and channel applicants to particular properties.[182] Further, depriving Village of Bellwood residents the "social and professional

169. *Id.* § 3604(b).
170. *Id.* § 3604(c).
171. *Id.* § 3604(d).
172. *Id.* §§ 3604(b)–(d).
173. *See* Havens Realty Corp. v. Coleman, 455 U.S. 363, 373–75 (1982) ("Section 804(d) states that it is unlawful for an individual or firm covered by the Act '[t]o represent to *any person* because of race, color, religion, sex, or national origin that any dwelling is not available for inspection, sale, or rental when such dwelling is in fact so available' . . . .") (quoting 42 U.S.C. § 3604(d)) (emphasis in original).
174. Gladstone Realtors v. Vill. of Bellwood, 441 U.S. 91, 99 (1979).
175. *Id.* at 95.
176. *Id.*
177. *Id.* at 94 (quotations omitted).
178. *Id.* at 95.
179. *Id.* at 95–98.
180. *Id.* at 116.
181. U.S. CONST. art. III, § 2.
182. *Gladstone Realtors*, 441 U.S. at 109–15.

benefit[] of living in an integrated society" was a sufficient injury to support standing.[183] While testers are not "genuinely interested in purchasing homes" and lack standing if they do not live in the affected area, residents are "entitled to prove that the discriminatory practices documented by their testing deprived them, as residents of the adversely affected area . . . ."[184]

This decision, which the Supreme Court has followed since 1982, is limited to the Fair Housing Act and does not address racial discrimination claims under 42 U.S.C. § 1982 or any other civil rights laws.[185]

3. Courts Apply Tester Protection Under the Fair Housing Act to Hackers

The Fair Housing Act serves two critical purposes: (1) "to eliminate housing discrimination and segregation" and (2) "to promote integration nationwide."[186] While the Fair Housing Act has traditionally applied in the physical solicitation and purchase of housing,[187] many similarities exist between physically buying property and finding housing online. It is also not uncommon to invoke the Fair Housing Act for research purposes.[188] For example, the Department of Housing and Urban Development has conducted three surveys—in 1977, 1989, and 2000—to research and document racial discrimination against protected classes of individuals.[189] While the historical background of the CFAA and browse-wrap agreements may potentially criminalize certain activity,[190] the Fair Housing Act may provide a nontraditional, yet effective, solution to online housing discrimination.

With standing to sue, researchers would be considered testers under the Fair Housing Act. Under the Fair Housing Act, it is unlawful to "make, print, or publish, or cause to be made, printed, or published any notice, statement, or advertisement, with respect to the sale or rental of a dwelling that indicates any preference, limitation, or discrimination based on race . . . ."[191] Website owners, however, are not liable for all discriminatory activity on their websites under the Communications Decency Act of 1996, which provides immunity for discriminatory information provided by website users and other third parties.[192]

Courts have been willing to extend unlawful housing actions to discrimination occurring online.[193] For example, the Ninth Circuit stated in *Fair Housing*

183. *Id.* at 114 (quoting the complaint).

184. *Id.* at 97–98.

185. *See* Havens Realty Corp. v. Coleman, 455 U.S. 363, 367 n.2 (declining to examine tester standing under § 1982). For a longer explanation of the circuit split on this matter, see Washington v. Krahn, 467 F. Supp. 2d 899, 901–04 (E.D. Wis. 2006).

186. Jorge Andres Soto & Deidre Swesnik, *The Promise of the Fair Housing Act and the Role of Fair Housing Organizations*, AM. CONST. SOC'Y 5 (January 2012), https://www.acslaw.org/sites/default/files/Soto_and_Swesnik_-_Promise_of_the_Fair_Housing_Act.pdf.

187. *Id.* at 4.

188. *See, e.g.*, *id.* at 7.

189. *Id.*

190. *See supra* Section II.B–C.

191. 42 U.S.C. § 3604(c) (2012).

192. 47 U.S.C. § 230(c)(1) (2012).

193. *See, e.g.*, Fair Hous. Council v. Roommate.com, LLC, 521 F.3d 1157, 1172–75 (9th Cir. 2008) (holding that Roommate.com was liable when it was designed to force subscribers to divulge protected characteristics and discriminatory preferences prohibited under the Fair Housing Act).

Council of San Fernando Valley v. Roommates.com, LLC that "[i]f such questions are unlawful when posed face-to-face or by telephone, they don't magically become lawful when asked electronically online" when a website collected answers in a questionnaire that violated the Fair Housing Act.[194] The court further stated that a website owner does not have immunity when it "design[s] its search system [to] . . . steer users based on the preferences and personal characteristics that [the website owner] itself forces subscribers to disclose."[195] Courts have not determined at this time, however, whether the Ninth Circuit's reasoning may extend beyond questionnaires and to websites that algorithmically discriminate and steer individuals.

E. Due Process and Restrictions on Delegating Legislative Powers

While the Constitution does not explicitly restrict legislative power, the Supreme Court has held that private entities cannot create legislation unilaterally. Article I of the United States Constitution vests "[a]ll legislative Powers" in Congress.[196] The Court has held that Congress cannot delegate its legislative authority to private parties.[197] The Court justifies this limitation on Congress's legislative power by invoking the doctrine of separation of powers.[198] Justice Brandeis aptly described the separation of powers doctrine in his dissent in *Myers v. United States*:

> The doctrine of the separation of powers was adopted by the Convention of 1787 not to promote efficiency but to preclude the exercise of arbitrary power. The purpose was not to avoid friction, but, by means of the inevitable friction incident to the distribution of the governmental powers among three departments, to save the people from autocracy.[199]

The Court limits its analysis to Article I of the Constitution when Congress delegates authority to public actors but applies the Fifth Amendment's Due Process Clause when Congress delegates authority to private actors.[200]

Courts restrict Congress from delegating authority to private actors based on the Fifth Amendment's Due Process Clause. The Fifth Amendment protects individuals from being "deprived of life, liberty, or property, without due process of law . . . ."[201] Since ratified in 1868, the Fourteenth Amendment has applied due process rights to the states as well.[202] The Supreme Court established delegations to private parties as unconstitutional in *Carter v. Carter Coal Co.*, describing it as "legislative delegation in its most obnoxious form[,] for it is . . .

194. *Id.* at 1164.

195. *Id.* at 1167.

196. U.S. CONST. art. I.

197. *See* Carter v. Carter Coal Co., 298 U.S. 238, 311 (1936) (holding that delegating authority to a private entity to fix maximum hours of labor and to fix minimum wages for a district was unconstitutional).

198. Ira P. Robbins, *The Impact of the Delegation Doctrine on Prison Privatization*, 35 UCLA L. REV. 911, 915 (1988).

199. 272 U.S. 52, 293 (1926) (Brandeis, J., dissenting).

200. *Carter*, 298 U.S. at 311 ("The delegation is so clearly arbitrary, and so clearly a denial of rights safeguarded by the [D]ue [P]rocess [C]lause of the Fifth Amendment, that it is unnecessary to do more than refer to decisions of this court which foreclose the question.").

201. U.S. CONST. amend. V.

202. *Id.* at amend. XIV.

delegation . . . to private persons whose interests may be and often are adverse to the interest of others in the same business."[203] Since the New Deal era, however, the Supreme Court has avoided addressing legislative delegation to private parties by holding laws unconstitutional on separate grounds.[204] While the Supreme Court does not have a consistent framework when applying the delegation doctrine, it has held that Congress may delegate authority to private parties when a statute is specific and definite.[205]

III. ANALYSIS

In its current form, the Computer Fraud and Abuse Act is too broad to justly protect individuals, including the United States government, from unauthorized computer attacks. While current court interpretations allow litigants to seek damages for violating a website's terms of use,[206] the Constitution may protect researchers that data scrape to investigate discrimination and other legislative violations.[207]

This Part will analyze a recent issue researchers experience when data-scraping websites involving racial discrimination. First, Section III.A will address the criminal and civil liability of researchers under the CFAA. Section III.B will discuss how researchers data-scraping websites to investigate discrimination may protect themselves.

For this Note, I will look specifically at Zillow.com as an example.[208] I do not intend to accuse Zillow of intentional or unintentional wrongdoing. Instead, Zillow represents one of many websites that actively restrict researching their algorithms' potentially discriminatory consequences through data scraping and data mining.

A. Researcher Liability Under the CFAA

Researchers wanting to investigate online discrimination face a catch-22.[209] Either researchers (1) refrain from researching discrimination online and refrain from uncovering practices that harm protected classes of citizens, or (2) data scrape websites and potentially subject themselves to liability under the CFAA. This Section addresses the relationship between electronic contracting and data scraping, as well as how electronic contracting relates to researcher liability under the Act.

---

203. *Carter*, 298 U.S. at 311.

204. *See* Robbins, *supra* note 198, at 919 n.44.

205. *See, e.g.*, Sunshine Anthracite Coal Co. v. Adkins, 310 U.S. 381, 397–99 (1940).

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

207. Russell Brandom, *New ACLU Lawsuit Takes on the Internet's Most Hated Hacking Law*, VERGE (June 29, 2016, 10:00 AM), http://www.theverge.com/2016/6/29/12058346/aclu-cfaa-lawsuit-algorithm-research-first-amendment ("The plaintiffs specialize in algorithmic research: bombarding closed algorithms with a range of different inputs to study their hidden biases. Those techniques often involve breaking a websites terms of service, potentially exposing them to prosecution under the CFAA.").

208. ZILLOW, https://www.zillow.com/ (last visited Jan. 16, 2018).

209. A "catch-22" is "a problematic situation for which the only solution is denied by a circumstance inherent in the problem or by a rule[.]" *Catch-22*, MERRIAM-WEBSTER DICTIONARY (11th ed. 2016), https://www.merriam-webster.com/dictionary/catch-22.

Subsection III.A.1 will address how companies such as Zillow, Trulia, and Amazon explicitly ban researchers from data scraping on their websites based on the websites' terms of use. Subsection III.A.2 will address how private website owners could, theoretically, seek damages under the CFAA from researchers who data mine.

1. Websites Restrict Data Scraping under Terms of Use

Likely, and hopefully unintentionally, websites steer certain users to certain content based on their predicted characteristics.[210] Typically, private websites explicitly limit an Internet user's ability to data scrape.[211] These browse-wrap contracts are presumptively valid and enforceable if: (1) the website user has actual or constructive knowledge of the terms;[212] and (2) the use of the website was within the scope of the browse-wrap agreement.[213]

a. A Website User's Actual or Constructive Acceptance to the Terms of Use

First, a browse-wrap agreement may bind a website user to the terms of use if the user expressly or implicitly accepts the terms in writing, orally, or through his or her conduct.[214] To show a breach of contract, the website owner must show a "manifestation of mutual assent on the part of two or more persons" as well as consideration for the mutual assent.[215] A common way to prove mutual assent, or a promise, is the presence of an offer and acceptance.[216] With browse-wrap agreements, courts focus on a user's acceptance of the terms of use offered by the website.[217] To accept, a user must "assent to the terms . . . made by the offeree in a manner invited or required by the offer."[218] A website user may accept terms of use by performance if the terms of use "invite[d] such an acceptance."[219]

When parties challenge website terms-of-use agreements, courts look objectively at the website user's conduct. For example, in *Molnar v. 1–800–Flowers.com, Inc.*, the court found that the consumers assented to the terms of use and the forum selection clause.[220] There, the consumer used the website numerous times before placing the order and was presumptively aware of the terms of use since the consumer's attorney investigated the claim before the consumer's

210. Esha Bhandari & Rachel Goodman, *ACLU Challenges Computer Crimes Law That is Thwarting Research on Discrimination Online*, ACLU (June 29, 2016, 10:00 AM), https://www.aclu.org/blog/free-future/aclu-challenges-computer-crimes-law-thwarting-research-discrimination-online.

211. Brandom, *supra* note 207.

212. Nguyen v. Barnes & Noble, Inc., 763 F.3d 1171, 1176 (9th Cir. 2014).

213. Ward v. TheLadders.com, Inc., 3 F. Supp. 3d 151, 161 (S.D.N.Y. 2014).

214. *See* Hines v. Overstock.com, Inc., 380 F. App'x 22, 24 (2d Cir. 2010).

215. RESTATEMENT (SECOND) OF CONTRACTS § 3 (AM. LAW INST. 1981).

216. *Id.* § 18 cmt. b, § 22.

217. *See Ward*, 3 F. Supp. 3d at 159.

218. RESTATEMENT (SECOND) OF CONTRACTS § 50(1) (AM. LAW INST. 1981).

219. *Id.* § 53(1).

220. Molnar v. 1-800-Flowers.com, Inc., No. CV 08-0542 CAS JCX, 2008 WL 4772125, at *8 (C.D. Cal. Sept. 29, 2008).

order.[221] Conversely, in *Nguyen v. Barnes & Noble, Inc.*, the court found that the consumer did not assent to the terms of use and the arbitration clause when the terms-of-use hyperlink[222] was not positioned in a way to provide notice of its existence, and the consumer would not necessarily see it without express notice.[223]

In the context of website terms-of-use agreements and data scraping, many of these websites restrict researchers from data scraping and data mining.[224] Amazon, for example, explicitly bans data mining in its terms of use:

> Subject to your compliance with these Conditions of Use and your payment of any applicable fees, Amazon or its content providers grant you a limited, non-exclusive, nontransferable, nonsublicensable license to access and make personal and noncommercial use of the Amazon Services. This license *does not include* any resale or commercial use of any Amazon Service, or its contents; any collection and use of any product listings, descriptions, or prices; any derivative use of any Amazon Service or its contents; any downloading, copying, or other use of account information for the benefit of any third party; or *any use of data mining, robots, or similar data gathering and extraction tools*.[225]

Housing websites, such as Zillow, implicitly restrict data scraping by restricting users from using the website's content.[226] While not as explicit as Amazon's terms of use, Zillow's terms still broadly ban the collection of information for data-scraping purposes:

> You agree not to impersonate another person or misrepresent your affiliation with another person or entity . . . . Except as expressly stated herein and without limitation, you agree that you will not, nor will you permit or encourage any third party to, reproduce, publicly display, or otherwise make accessible on or through any other web site, application, or service any reviews, ratings, and/or profile information about real estate, lending, or other professionals, underlying images of or information about real estate listings, or other data or content available through the Services.[227]

The terms of use for Zillow's website would likely be an enforceable contract based on its terms-of-use agreement. Zillow's "Terms of Use & Privacy" are prominently displayed on all of the website's webpages—including its homepage and in the footer.[228] When a new user wants to create a new account on Zillow to buy, rent, sell, or mortgage property, they must provide their e-mail address, a user-specific password, and indicate if they are a landlord or industry

221. *Id.* at *1–2.

222. A "hyperlink" is a programmatic command to move to another page in a Web browser. Hyperlinks are embedded in the text of websites to help users move quickly to a targeted Web page. Paul Gil, *What Is a Hyperlink?*, LIFEWIRE (Sep. 30, 2017), https://www.lifewire.com/how-do-hyperlinks-work-2483287.

223. Nguyen v. Barnes & Noble, Inc., No. 8:12-CV-0812-JST RNB, 2012 WL 3711081, at *3–*5 (C.D. Cal. Aug. 28, 2012), *aff'd,* 763 F.3d 1171 (9th Cir. 2014) (reasoning that the plaintiff did not assent to the website's terms when the hyperlink was located in the bottom-left corner of each screen and does not require the user to click on it).

224. Brandom, *supra* note 207.

225. *Conditions of Use*, *supra* note 36 (emphasis added).

226. *Terms of Use*, ZILLOW, https://www.zillow.com/corp/Terms.htm (last updated Mar. 2016).

227. *Id.* (emphasis added).

228. *See generally id.*

professional.[229] When users click the "[s]ubmit" button, immediately to the right of the button is hyperlinked text stating "I accept Zillow's Terms of Use."[230] Explicitly stated in Zillow's internal Wiki,[231] Zillow's data is "licensed to [Zillow] only for use by consumers on the Zillow site . . . mean[ing] that scraping data or distributing it on other Web sites is not allowed, except in the case of permitted search engines."[232]

Following the court's holding in *Nguyen*, Zillow's terms of use would be enforceable against researchers that data scrape Zillow's website. In traditional contract law, Zillow's terms of use would be considered an offer because their terms of use are not unique, and courts "have consistently enforced browse-wrap agreements against both businesses and consumers."[233] Further, users of Zillow's website objectively accept these terms: the browse-wrap agreement is accessible through a hyperlink, Zillow prompts users to review the terms of use, users have to accept these terms to effectuate any transaction, and users must affirmatively agree to the terms before creating an account.[234]

Proponents of civil liberties would argue that this practice still does not form a contract because both parties did not mutually assent to the terms with consideration.[235] The recent case law indicates that the courts find these agreements to be made with consideration, however, because the terms of use are "sought by the [website] in exchange for [its] promise [to use the website's services] and is given by the [user] in exchange for that promise."[236] Ultimately, Zillow's terms of use are binding agreements to which users assent, including researchers.

b. A Website User's Acts are Within the Scope of the Website's Terms of Use

Courts would also consider whether researchers that data scrape Zillow to test its potentially discriminatory behavior are within the scope of the agreement. Challenges to a website's browse-wrap agreements based on scope largely revolve around the agreement's inapplicability to a party's use of the website and the website's alleged claims.[237] As previously stated, however, a researcher attempting to scrape data from a website, like Zillow, would expressly fall under

229. ZILLOW, *supra* note 208.

230. *Terms of Use*, *supra* note 226.

231. A Wiki is a "collaborate community [w]ebsite where anyone can contribute." Wikis are used online to create internal knowledge bases, assemble online communities and manage websites. Wikis are simple to create and edit and are simply organized and may even show recent changes to a Wiki page. Nathan Matias, *What Is a Wiki? Article*, SITEPOINT (Nov. 3, 2003), https://www.sitepoint.com/what-is-a-wiki/.

232. *Privacy and Terms of Use*, ZILLOW (last updated Apr. 20, 2016), http://www.zillow.com/wikipages/Privacy-and-Terms-of-Use/.

233. Nguyen v. Barnes & Noble, Inc., No. 8:12-CV-0812-JST RNB, 2012 WL 3711081, at *3 (C.D. Cal. Aug. 28, 2012), *aff'd,* 763 F.3d 1171 (9th Cir. 2014) (quotations omitted) (quoting defendant's reply).

234. *See id.* at *4; Ticketmaster L.L.C. v. RMG Techs., Inc., 507 F. Supp. 2d 1096, 1107 (C.D. Cal. 2007).

235. *See generally* Russell Korobkin, *The* Borat *Problem in Negotiation: Fraud, Assent, and the Behavioral Law and Economics of Standard Form Contracts*, 101 CALIF. L. REV. 51, 70 (2013).

236. RESTATEMENT (SECOND) OF CONTRACTS § 71(2) (AM. LAW INST. 1981).

237. Kurtis A. Kemper, *Validity, Construction, and Application of Browsewrap Agreements*, 95 A.L.R. 6th 57 § 5 (2014).

Zillow's terms of use, which could constitute unauthorized access of a protected computer in some federal jurisdictions.[238]

Thus, websites explicitly restrict researchers and laypersons from data scraping, potentially opening those individuals to criminal or civil liability under the CFAA.

2. Based on Terms of Use, Data Scraping Breaches the CFAA

The Supreme Court has not spoken regarding whether courts should apply the CFAA broadly or narrowly to website terms-of-use agreements, leaving each circuit to decide whether the CFAA exposes researchers to criminal or civil liability for intentionally violating a website's terms of use. The CFAA makes it illegal to "intentionally access[] a computer without authorization or exceed[] authorized access, and thereby obtain[]. . . information from any protected computer."[239] Violations of the CFAA may result in criminal charges, either misdemeanor or felony charges, as well as civil liability.[240] For civil claims, a plaintiff will likely allege a damage or loss resulting in at least a $5,000 economic loss.[241] The statute is unclear, however, concerning whether violating the CFAA per se imposes liability.[242]

Under the Act, the term "exceeds authorized access" is ambiguous.[243] At this time, the circuit courts of appeals are struggling to determine whether to broadly or narrowly interpret unauthorized access of a protected computer under the CFAA.[244] It is difficult to predict how courts will rule when a researcher intentionally violated a website's terms of use while testing for discrimination because courts are not unified in their approaches.[245] To address this issue, this Note analyzes this activity under case law over the last twenty years.

a. Denying the CFAA as Vague

When courts examine a researcher's testing activities under the CFAA, the applicability of the Act depends on whether the term "unauthorized access" is viewed narrowly or broadly. If "unauthorized access" includes violating a website's terms of use (for example, by data scraping), then the CFAA opens researchers to broad, unilateral criminal or civil liability. This perspective aligns with the Department of Justice's view, which informs prosecutors that it is "rel-

238. *See supra* Subsection III.A.1.a.

239. 18 U.S.C. § 1030(a)(2)(C) (2012).

240. *See generally id.* §§ 1030(c), 1030(g).

241. *Id.* § 1030(g).

242. *See* Clark S. Splichal, *Recent Development: Craigslist and the CFAA: The Untold Story*, 67 FLA. L. REV. 1845, 1851 (2015).

243. United States v. Nosal, 676 F.3d 854, 856–857 (9th Cir. 2012).

244. Shawn E. Tuma, *"What Does CFAA Mean and Why Should I Care?"–A Primer on the Computer Fraud and Abuse Act for Civil Litigators*, 63 S.C. L. REV. 141, 167 (2011).

245. *Compare Nosal*, 676 F.3d at 857, *with* Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1066 (9th Cir. 2016).

atively easy to prove that a defendant had only limited authority to access a computer in cases when the defendant's access was limited by restrictions . . . in writing, such as terms of service [or] a website notice . . . ."[246]

Some courts indicated that it is relatively difficult, however, to succeed in prosecuting defendants under a broad reading of the CFAA. One court went as far as to hold the CFAA unenforceable under the void-for-vagueness doctrine.[247] In *United States v. Drew*, the District Court for the Central District of California held that the CFAA does not apply broadly to a website's terms of service.[248] The defendant, Lori Drew, was charged with violating the Act when she assumed a false identity on Myspace and bullied another student, who later committed suicide.[249] The creation of an account with a fictitious name and a false photograph violated Myspace's Terms of Service.[250] Holding that violating a website's terms of service is not "unauthorized access" under the CFAA, the court reasoned that incorporating these terms into the statute would be "unacceptably vague" and would unknowingly open website users to indefinite liability.[251] The void-for-vagueness doctrine, applied in due process challenges under the Fifth Amendment, requires a statute to "define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement."[252] The court in *Drew* held that the CFAA was unconstitutional on the grounds that the statute's language was so ambiguous that it could be indiscriminately applied to circumstances where a website user unknowingly violated the website's terms of use.[253]

While the void-for-vagueness doctrine was applied by the Central District of California in *Drew*, other courts have rejected that court's reasoning.[254] A website owner may reasonably argue that the criminal offense is definite and understandable when the terms of use are published and obviously available on the website. For example, in *United States v. Lowson*, the court distinguished its holding from *Drew* by limiting *Drew*'s void-for-vagueness application to situations involving only contract violations, and not additional restrictions.[255] As it will be discussed later in this Note, however, distinguishing between types of

246. OFFICE OF LEGAL EDUC., EXEC. OFFICE FOR U.S. ATT'YS, PROSECUTING COMPUTER CRIMES 8–9 (2010), http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf.

247. United States v. Drew, 259 F.R.D. 449, 467 (C.D. Cal. 2009) ("In sum, if any conscious breach of a website's terms of service is held to be sufficient by itself to constitute intentionally accessing a computer without authorization or in excess of authorization, the result will be that section 1030(a)(2)(C) becomes a law that affords too much discretion to the police and too little notice to citizens who wish to use the [Internet].") (quoting City of Chi. v. Moralis, 527 U.S. 41, 64 (1999)) (alternation in original).

248. *Id.*

249. *Id.* at 452.

250. *Id.*

251. *Id.* at 464–65.

252. Kolender v. Lawson, 461 U.S. 352, 357 (1983).

253. *Drew*, 259 F.R.D. at 464–65.

254. *See* United States v. Lowson, Crim. No. 10–114 KSH, 2010 WL 9552416, at *6 (D. N.J. Oct. 12, 2010).

255. *Id.* (distinguishing when the charge involved both a contract violation and a code-based restriction).

restrictions, such as use restrictions, access restrictions, and code-based restrictions, does not resolve the ambiguity of authorized access under the CFAA.[256]

Other courts have not followed the Central District of California's ruling in *Drew*, allowing broad criminal and civil liability for website users that intentionally violate terms of use. Broadly applying the CFAA, the First Circuit previously held in *EF Culture Travel BV v. Explorica, Inc.* that the use of data-scraper software exceeded a website's authorized access based on a contractual agreement made by the parties under the CFAA.[257] Straying from the *Drew* decision, the Ninth Circuit similarly held in *Facebook, Inc. v. Power Ventures, Inc.* that violating Facebook's terms of use may allow Facebook to seek civil damages because Facebook sent a cease and desist letter to the Internet user before suing the defendant.[258]

In the context of researchers testing Zillow for algorithmic discriminatory effects, researchers may be open to criminal or, more likely, civil liability. As previously stated, Zillow's terms of service expressly restrict users from data scraping.[259] The researchers would be doing this act intentionally to test for racial discrimination, which meets the required mens rea under the CFAA.[260] Based on the increased web traffic and misappropriation of resources, the alleged damages could easily exceed the $5,000 threshold under the Act.[261]

Depending on the affirmative action taken by Zillow in response to the researchers data scraping, a website owner would likely be able to sue these researchers under the CFAA, regardless of the vagueness of the Act.[262] Under cases like *Facebook, Inc.*, websites simply need to affirmatively notify the researchers to cease and desist data scraping, an action easily automated by a website owner.[263] Without a congressional amendment, the CFAA appears to open researchers to criminal or civil liability, unilaterally determined by the website owner.

b. Denying the CFAA by Distinguishing "Use" from "Access" Restrictions

Other circuits have followed the ruling of *Drew*—albeit on different grounds—by narrowly applying the CFAA. The Ninth Circuit held in *United States v. Nosal* that the defendant exceeded authorized access because it does not create "criminal liability to everyone who uses a computer in violation of computer use restrictions—which may well include everyone who uses a computer."[264] Nosal convinced a former coworker to retrieve from his former employer's database confidential information, which he later used at a competing

256. *See infra* Subsection III.A.2.b.
257. EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 583 (1st Cir. 2001).
258. Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1069 (9th Cir. 2016).
259. *See supra* Subsection III.A.1.
260. *See* 18 U.S.C. § 1030(a) (2012).
261. *Id.* § 1030(g).
262. *Facebook, Inc.*, 844 F.3d at 1069.
263. *Id.*
264. United States v. Nosal, 676 F.3d 854, 857 (9th Cir. 2012).

company.[265] The government charged Nosal under the CFAA.[266] The court, reconsidering Nosal's denied motion to dismiss in light of *LVRC Holdings LLC v. Brekka*,[267] affirmed the Ninth Circuit's reversal en banc.[268]

Holding for Nosal, the court distinguished between "use" restrictions and "access" restrictions, and the court reasoned that the CFAA only applies to access restrictions, not use restrictions.[269] The court described this distinction by with a useful example:

> Suppose an employer keeps certain information in a separate database that can be viewed on a computer screen, but not copied or downloaded. If an employee circumvents the security measures, copies the information to a thumb drive and walks out of the building with it in his pocket, he would then have obtained access to information in the computer that he is not "entitled so to obtain." Or, let's say an employee is given full access to the information, provided he logs in with his username and password. In an effort to cover his tracks, he uses another employee's login to copy information from the database. Once again, this would be an employee who is authorized to access the information but does so in a manner he was not authorized "so to obtain."[270]

This distinction between use restrictions and access restriction is not helpful, however, in the context of researchers intentionally violating a website's terms of service while testing for discrimination. In the context of Zillow, a website would be the computer system in which users have exceeded authorized use. Zillow, restricting data scraping, could be both an access restriction and a use restriction.[271] It would be an access restriction because the researcher has "some authority [to] access [ ] the website because it is open to the public," and it would be a use restriction because "each webpage is an objective set of data . . . restrict[ing] leveraging the information only for [a] purpose."[272] Further, with the rapid evolution of technology in the last thirty years, determining what qualifies as "use" or "access" under the CFAA remains one of the most "complicated and highly litigated issues" under the CFAA.[273] Depending on the jurisdiction, a researcher may be liable for violating the Act if, like in *Nosal*, the court reasons that a website's terms of use include access restrictions.[274]

265. *Id.* at 856.

266. *Id.*

267. 581 F.3d 1127, 1135 (9th Cir. 2009) (holding that "without authorization" and "exceeds authorized access" under the CFAA should be narrowly interpreted and not open employees up to civil liability when they email work documents to themselves for use at home).

268. *Nosal*, 676 F.3d at 864.

269. *Id.* at 862.

270. *Id.* at 858.

271. Jonathan Mayer, *The "Narrow" Interpretation of the Computer Fraud and Abuse Act: A User Guide for Applying* United States v. Nosal, 84 GEO. WASH. L. REV. 1644, 1669 (2016).

272. *Id.*

273. Tuma, *supra* note 244, at 171.

274. *Nosal*, 676 F.3d at 864.

B. Protecting Researchers and Protected Classes under the Fair Housing Act

Researchers are only potentially subject to federal liability if they intentionally violate a website's terms of use.[275] To proactively counter this, researchers are suing the DOJ and asking the courts to enjoin the government from enforcing the CFAA.[276] For real estate websites, researchers may assert statutory protections under the Fair Housing Act and the Fifth Amendment's Due Process Clause. If these challenges are successful, the CFAA would be unconstitutionally broad and would require immediate legislative action.

Subsection III.B.1 will determine whether researchers would have standing to sue website owners under the Fair Housing Act. Subsection III.B.2 will argue that researchers should have standing to challenge the CFAA's broad inclusion of a website's terms-of-use agreements as an unconstitutional delegation of legislative authority, banned under the Fifth or Fourteenth Amendment's Due Process Clause. Subsection III.B.3 analyzes how protected groups affected by algorithmic discrimination may also seek a remedy under civil rights laws like the Fair Housing Act.

1. Researchers Would Have Standing to Sue Under the Fair Housing Act

When courts examine whether a certain practice is racially discriminatory under the Fair Housing Act, they must determine whether the individual tester (the researcher) has standing to sue.[277] Standing under the Fair Housing Act is "expanded to the full extent permitted by Article III, so that a plaintiff need only claim to have suffered an actual, redressable injury."[278] Under Article III of the United States Constitution,[279] litigants have standing in United States District Courts even if the alleged racial discrimination is implicit or indirect.[280] For individuals who perform testing protected under the Fair Housing Act, the Supreme Court has allowed these parties to have standing.[281]

Researchers that data scrape for the purpose of collecting evidence against suspected violators of civil rights laws have standing to sue under the Fair Housing Act.[282] The cases involving civil rights tester cases all refer to physical testing, not electronic testing.[283] In traditional property situations, an individual approaches a seller in person and seeks out discrimination face-to-face.[284] The

275. 18 U.S.C. § 1030(a) (2012).

276. Zetter 2, *supra* note 35.

277. Havens Realty Corp. v. Coleman, 455 U.S. 363, 372 (1982).

278. Daniel A. Klein, Annotation, *Standing to Sue Under 42 U.S.C.A. § 1982, Protecting Property Rights*, 79 A.L.R. Fed. 281 (1986).

279. U.S. CONST. art. III.

280. *See* Gladstone Realtors v. Vill. of Bellwood, 441 U.S. 91, 108–09 (1979).

281. *See id.* at 107–08.

282. *See id.* at 115.

283. *See, e.g.*, *id.*

284. *See*, *e.g.*, *id.* at 94 ("[T]he individual respondents and other persons consulted petitioners, stating that they were interested in purchasing homes in the general suburban area of which Bellwood is a part. The individual respondents . . . acting as 'testers' in an attempt to determine whether petitioners were engaging in racial 'steering,' . . . .").

actions of these testers still establish standing to sue, however, because racial steering likely could lead to a sufficient injury or "decline[] as a result of the conduct of another."[285] For example, in *Fair Housing Council of San Fernando Valley v. Roommates.com*, the plaintiff established standing simply by alleging that Roommates.com violated the Fair Housing Act by discriminating in online questionnaires—an action that would be illegal if done either off-line or online.[286] Similarly, researchers that investigate and data scrape websites would only have to plead that, acting as a tester, they experienced indirect racial discrimination from racial steering and racial targeting.[287]

Some may argue that researchers would not have standing in this context. Critics of standing for Internet testers may compare this to the circuit courts of appeals' split on whether consumers that lose personal information in data breaches have standing for harm that is likely to occur in the future.[288] In some circuits, consumers would have standing in a data breach when a high likelihood of future injury exists from identity theft and credit fraud,[289] while other circuits have held that data breaches do not harm consumers until the information stolen has been misused.[290] Data breaches are distinct from violations of the Fair Housing Act, however, because the Supreme Court has expressly ruled that indirect harm under the Fair Housing Act is sufficient.[291]

Although they would have standing, researchers violating the CFAA would still need to challenge the constitutionality of the CFAA to continue their research.

2. The CFAA Unconstitutionally Delegates Legislative Power to Websites

The broad application of the CFAA allows for flexibility in charging cybercrime, but it also may be the statute's ultimate downfall. When courts allow websites to determine what constitutes "exceed[ing] authorized access" by incorporating a website's terms of use, websites have unilateral authority from Congress to create criminal and civil liability.[292] The enforceability of electronic contracts, and the apparently broad scope of the CFAA, inevitably leads to unintended consequences, and this statutory overbreadth will open more Internet users to potential liability—especially Internet researchers.[293]

Under the Fifth Amendment to the United States Constitution,[294] researchers may challenge the CFAA as an unconstitutional delegation of legislative au-

285. *See id.* ("This is a fact subject to proof before the District Court, but convincing evidence that the economic value of one's own home has declined as a result of the conduct of another certainly is sufficient under Art. III to allow standing to contest the legality of that conduct.").

286. Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157, 1162 (9th Cir. 2008).

287. *See* FED. R. CIV. PRO. 8(a) (2012).

288. Clapper v. Amnesty Int'l USA, 568 U.S. 398, 410 (2013).

289. *See, e.g.*, Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015).

290. *See, e.g.*, Reilly v. Ceridian Corp., 664 F.3d 38, 43 (3d Cir. 2011).

291. Gladstone Realtors v. Vill. of Bellwood, 441 U.S. 91, 102 (1979).

292. 18 U.S.C. § 1030(a)(2) (2012); Cyrus Y. Chung, *The Computer Fraud and Abuse Act: How Computer Science Can Help with the Problem of Overbreadth*, 24 HARV. J.L. & TECH. 233, 245 (2010).

293. *See, e.g.*, Brandom, *supra* note 207.

294. U.S. CONST. amend. V.

thority to website owners. It is a principle that "[f]ederal lawmakers cannot delegate regulatory authority to a private entity."[295] Article I defines Congress's regulatory authority and includes legislative powers like the power to "lay and collect taxes,"[296] to "declare war,"[297] and to "regulate commerce with foreign nations[] and among the several states."[298] While the Supreme Court has not announced a comprehensive test to determine when Congress unconstitutionally delegates authority to private entities, the Court has discussed this issue numerous times in the last century.

a. The CFAA Delegates Legislative Authority to Website Owners

The CFAA indirectly delegates legislative authority to website owners by incorporating a website's terms of use into the statute. Courts have incorporated a website's terms of service into the Act to define authorized access to determine what exceeds authorized access.[299] Website owners act like legislators in this context. Under the Supreme Court's broad interpretation of the Interstate Commerce Clause, website owners regulate interstate commerce indirectly by controlling how Internet users, located nationwide, may or may not interact with a commercial website.[300] The CFAA embraces this broad interpretation by explicitly defining protected computers as computers "affecting interstate or foreign commerce or communication . . . ."[301]

The CFAA's language is not sufficiently precise, further supporting the Act's unconstitutionality under the Fifth Amendment. In *Sunshine Anthracite Coal Co. v. Adkins*, the Supreme Court held that Congress defined the term "bituminous coal" with insufficient clarity, making the delegation of authority to the National Bituminous Coal Commission unlawful.[302] Further, the Court worried about reversing a half-century of administrative law by invalidating Congress's delegation of authority.[303] Compared to websites, "[i]t is unclear that every intentional breach of a website's terms of service would be or should be held to be equivalent to an intent to access the site without authorization or in excess of authorization."[304] Also, reversing the enforceability of website terms of use would not reverse a foundational application of contract law, as the electronic contract is a relatively modern development that is still evolving.[305]

295. Ass'n of Am. R.Rs. v. U.S. Dep't of Transp., 721 F.3d 666, 670 (D.C. Cir. 2013), *vacated and remanded sub nom.* Dep't of Transp. v. Ass'n of Am. Railroads, 135 S. Ct. 1225 (2015).

296. U.S. CONST. art. I, § 8, cl. 1.

297. *Id.* at art. I, § 8, cl. 11.

298. *Id.* at art. I, § 8, cl. 3.

299. EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 585 (1st Cir. 2001) ("To parse the words in any other way would not only impair Congress's intended scope of the Act, but would also serve to reward sophisticated intruders.").

300. Adam R. Bialek & Scott M. Smedresman, *Internet Risk Management: A Guide to Limiting Risk Through Web Site Terms and Proactive Enforcement*, 20 INTELL. PROP. & TECH. L.J. 1, 4 (2008).

301. 18 U.S.C. § 1030(e)(2)(B) (2012).

302. Sunshine Anthracite Coal Co. v. Adkins, 310 U.S. 381, 399–400 (1940).

303. *Id.* at 400.

304. United States v. Drew, 259 F.R.D. 449, 467 (C.D. Cal. 2009).

305. *See* Charles L. Knapp, *Contract Law Walks the Plank:* Carnival Cruise Lines, Inc. v. Shute, 12 NEV. L.J. 553, 556 (2012).

Congress's unconstitutional delegation of authority through the CFAA is even more problematic in the context of property rights. Courts recognize the general principle that "the right of the owner of property to fix the price at which he [or she] will sell it is an inherent attribute of the property itself, and . . . is within the protection of the Fifth . . . Amendment[]."[306] When housing websites algorithmically, and likely unintentionally, discriminate when filtering content, Congress's delegation of power would likely face strict scrutiny.[307]

b. Arguing that Congress Delegates Legislative Authority to Websites is Problematic

The Supreme Court has been unwilling in the last seventy years to reconsider the Fifth Amendment's restriction on Congress's delegating legislative authority to private entities.[308] Recently, the Court has avoided the issue, deciding issues on grounds outside of the Fifth Amendment.[309] Researchers may attempt to challenge the CFAA under the Fifth Amendment, but the Supreme Court would likely follow its recent pattern of analysis and not avoid addressing the doctrine, but instead hold on separate, and distinct, grounds.

3. The Fair Housing Act Also Protects Classes Harmed by Discrimination

The Fair Housing Act and the Fifth Amendment protect researchers who data scrape and who have allegedly violated the CFAA.[310] Especially in the context of housing websites, like Zillow, where the websites aggregate a large amount of data and algorithmically provide results based on a person's profile,[311] the Fair Housing Act would provide protection under the Thirteenth Amendment.[312] A tester, such as a researcher data scraping under the false pretext of being an Internet user, suffers injuries precisely in the form the Fair Housing Act expected: discriminatory refusal to sell, steer, or channel property to a protected class of individuals based on race, class, sex, or ethnicity.[313] Under the Fair Housing Act, housing intermediaries screening prospective buyers by race may seek relief.[314]

306. Old Dearborn Distrib. Co. v. Seagram-Distillers Corp., 299 U.S. 183, 192 (1936).

307. *See id.*

308. Robbins, *supra* note 198, at 921.

309. *See* Dep't of Transp. v. Ass'n of Am. R.Rs., 135 S. Ct. 1225, 1227 (2015) (holding that Amtrak was a government entity, rather than an autonomous entity, for determining whether Congress unconstitutionally delegated authority under the Passenger Rail Investment and Improvement Act of 2008).

310. *See, e.g.*, Harris v. Itzhaki, 183 F.3d 1043, 1043–44 (9th Cir. 1999).

311. *See* TRULIA, https://www.trulia.com/ (last visited Jan. 16, 2018); ZILLOW, *supra* note 208.

312. Havens Realty Corp. v. Coleman, 455 U.S. 363, 374 (1982).

313. *Id.* at 375.

314. *See* Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157, 1167 (9th Cir. 2008).

a. The Fair Housing Act Would Protect Individuals in Affected Social Classes

The Fair Housing Act not only applies to housing realtors but also to online services filtering housing results directly or indirectly based on race.[315] Based on testing already performed by the Department of Housing and Urban Development, researchers could show discrimination by pairing two individuals with similar financial situations that experienced disparate effects of racial steering based on their protected-class status.[316] In *Sherman Park Community Ass'n v. Wauwatosa Realty Co*., twenty-three of the thirty-nine plaintiffs alleged that housing agents racially steered African Americans to one geographic area.[317] All twenty-three of these plaintiffs resided in the area, but the sixteen remaining plaintiffs did not.[318] Using *Bellwood*,[319] the Eastern District of Wisconsin held that all thirty-nine plaintiffs had standing to sue as "persons who have been denied the right to live in an integrated community."[320] Under the civil rights cases, "the scope of this country's fair housing laws . . . cannot be used as a device to limit plaintiffs' standing."[321] The holding in *Bellwood* could easily extend to website owners and allow users a legally enforceable claim when denied the right to see geographic-specific content and live in a specific community.

Even in case studies outside of housing, courts may extend other civil rights statutes to protect testers based on the same policy. For example, courts could apply Title VII of the Civil Rights Act of 1964 in cases where website aggregating companies looking to hire certain applicants, discriminate against individuals based on their race, sex, or location.[322] Also, courts could extend the Equal Credit Opportunity Act to protect data scrapers that find credit websites discriminating based on sex, age, or race through preconceived algorithmic profiles.[323]

b. Unique Applications of the Fair Housing Act for Online Activity

Surprisingly, parties have used the Fair Housing Act and other civil rights statutes in nonhousing circumstances. For example, in *Tex*as *Department of Housing & Community Affairs v. Inclusive Communities Project, Inc*., the Supreme Court addressed whether the plaintiffs discriminated by disparate impact when they allocated low-income housing tax credits to African Americans.[324] The Inclusive Communities Project, a nonprofit corporation, argued that Texas and its officers segregated people racially by allocating too many tax credits to

315. *See id.*

316. Ron Leshnower, *What Landlords Need to Know About Fair Housing Testers: How the Government Checks for Housing Discriminaiton*, NOLO, http://www.nolo.com/legal-encyclopedia/what-landlords-need-know-about-fair-housing-testers.html (last visited Jan. 16, 2018).

317. Sherman Park Cmty. Ass'n v. Wauwatosa Realty Co., 486 F. Supp. 838, 842 (E.D. Wis. 1980).

318. *Id.*

319. Vill. of Bellwood v. Gladstone Realtors, 569 F.2d 1013 (7th Cir. 1978).

320. *Sherman Park Cmty. Ass'n*, 486 F. Supp. at 844.

321. *Id.* at 842.

322. 42 U.S.C. § 2000e–2 (2012).

323. 15 U.S.C. § 1691 (2012).

324. Tex. Dep't of Hous. & Cmty. Affairs v. Inclusive Cmtys. Project, Inc., 135 S. Ct. 2507, 2513 (2015).

predominantly black areas and too few tax credits to predominantly white areas, violating the Fair Housing Act.[325] In a five-to-four decision, the Court held for the Inclusive Communities Project.[326] The majority reasoned, in part, that their ruling represents the purpose of the Fair Housing Act: "to eradicate discriminatory practices within a sector of our Nation's economy."[327] The court's holding allows for parties like the defendants to counteract prejudice when it may be hard to prove.[328] Although not a case involving websites, courts may be willing to consider alternative ways to apply the Fair Housing Act beyond the scope of the civil rights cases.[329]

The CFAA is so broad and vague that, as shown above, Internet users may be criminally and civilly liable for violating a website's terms of service. Now, the CFAA is unavoidably vague and needs significant improvements. Without this, the CFAA muddles future litigation for litigators, researchers, and Internet users alike. Researchers that pursue litigation, like what I described above, may win or lose solely based on their jurisdiction's analysis of the CFAA. To prevent creating disincentives for researchers to investigate civil liberty violations, both congressional and corporate action is needed.

IV. RECOMMENDATION

Current researchers and activists, understanding the illegality of data-scraping public websites, must halt their research and preemptively sue to make sure they comply with current CFAA limitations, stifling social progress at the expense of broad government oversight.[330] With algorithms having such a considerable influence on modern society,[331] researchers, and Internet users generally, must seek additional protections outside of litigation to avoid liability under the CFAA. While some Internet users may not be criminally liable (since they do not have the required mens rea), the CFAA may still impose civil liability on an Internet user.[332] A narrower legal framework is required to protect Internet users, researchers, and website owners and to avoid imposing potentially unlimited liability on Internet users.[333]

Part IV makes two recommendations. First, to adequately protect Internet users and researchers, this Note recommends a multi-faceted regulatory solution. Such regulatory improvements include statutory amendments to the CFAA as well as congressional grants of authority to administrative agencies. Second, this Note recommends nonregulatory, private solutions, which include encouraging

325. *Id.* at 2514.
326. *Id.* at 2526.
327. *Id.* at 2521 (citing 42 U.S.C. § 3601 (2012)).
328. *Id.* at 2522.
329. *Id.*
330. Brandom, *supra* note 207.
331. Leo Hickman, *How Algorithms Rule the World*, GUARDIAN (July 1, 2013, 1:32 PM), https://www.theguardian.com/science/2013/jul/01/how-algorithms-rule-world-nsa.
332. 18 U.S.C. § 1030(g) (2012); *see, e.g.*, P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, LLC., 428 F.3d 504, 512 (3d Cir. 2005).
333. Kelsey T. Patterson, *Narrowing It Down to One Narrow View: Clarifying and Limiting the Computer Fraud and Abuse Act*, 7 CHARLESTON L. REV. 489, 531 (2013).

private companies to reward disclosures and encouraging negotiations between website owners and researchers.

A. Statutory and Regulatory Solutions

Researchers and Internet users face a challenging task fighting the CFAA through litigation. Courts, attorneys, and scholars alike continue to struggle with the meaning of authorization under the CFAA without an unambiguous solution.[334] Significant statutory reform is required to clarify the legal framework for future litigation. Amending the CFAA to protect both Internet users and businesses will prevent these conflicts in the future.

1. Partial Exception for Researchers Testing for Civil Rights Violations

Since litigation is uncertain, researchers investigating potentially discriminatory behaviors on websites should lobby for statutory reform. Congress must balance the concerns of businesses as well as the concerns of researchers and Internet users to ensure a long-term solution amenable to technological development.

Scholars have not considered CFAA reform in the context of browse-wrap or click-wrap agreements. Many scholars, however, call for sweeping statutory changes to the CFAA, with some arguing the CFAA should be repealed or amended. Some critics advocate for Congress to remove the subsection making the unauthorized, intentional access of a computer a private right of action.[335] Some scholars, however, have called for a partial exception for employees.[336] For example, Congress could "exempt certain class[es] of cases" from certain types of individuals under the CFAA.[337] Exempting certain classes of individuals would "ha[ve] the effect of obviating the need for enacting a new statute while preserving the existing statute from constitutional infirmity."[338] Some recommend a similar narrowing approach by arguing for a "code-based approach," which would require an Internet user to "circumvent some type of code restriction in order to gain access to particular information on a computer."[339] To be liable under the CFAA, "the user must take affirmative actions to circumvent a code restriction [and] has notice that he is accessing the computer without authorization or is exceeding the bounds of his authorization."[340] This Note does not support these approaches because they do not fully remedy the broad language that would remain in the CFAA.

Both the legislative and executive branches recently proposed legislative reform. Some have argued for a broad interpretation of the CFAA. President

334. *Id.*

335. *See, e.g.*, Kyle W. Brenton, *Trade Secret Law and the Computer Fraud and Abuse Act: Two Problems and Two Solutions*, 2009 U. ILL. J.L. TECH. & POL'Y 429, 457–59 (2009).

336. Obie Okuh, *When Circuit Breakers Trip: Resetting the CFAA to Combat Rogue Employee Access*, 21 ALB. L.J. SCI. & TECH. 637, 669 (2011).

337. *Id.*

338. *Id.*

339. Patterson, *supra* note 333, at 530.

340. *Id.* at 505.

Obama proposed "resolv[ing] the current circuit split by saying that breaching a written restriction on computer use is indeed a crime, but that the scope of liability for such breaches is significantly limited."[341] Senators Lindsey Graham and Sheldon Whitehouse introduced a bill that created civil and criminal liability for unauthorized use or access of a computer except for contractual restrictions like a website's terms-of-use agreement.[342] Some have backed a narrower interpretation of the CFAA: Senators Ron Wyden, Rand Paul, and Zoe Lofgren introduced a bipartisan bill restricting the CFAA from imposing liability for breaches of terms of service and defining "access without authorization" as "gaining unauthorized access to information by circumventing technological or physical controls."[343]

Legislative reform would alleviate many critics' concerns with the CFAA. For example, by clarifying terms such as "authorized access" or "protected computer," and applying a consistent standard of review, courts could reasonably apply the CFAA to the diverse environment of IoT devices.[344] Also, Congress could provide clear notice to Internet users, especially researchers, as to what behaviors constitute misconduct.[345] Finally, by limiting the CFAA to the statute, and not the terms of use for a website, Internet users would not have to research what each website defines as misconduct.[346]

Congress could create research exemptions under the CFAA like in other recent legislation. Under the Digital Millennium Copyright Act ("DMCA"), for example, it is illegal to "circumvent a technological measure that effectively controls access to a [copyrighted] work protected . . . ."[347] The DMCA allows researchers to circumvent such technological measures, however, if they are "security testing." Under the DMCA, Congress defined security testing as:

> [A]ccessing a computer program solely for purposes of good-faith testing, investigation and/or correction of a security flaw or vulnerability, where such activity is carried out in a controlled environment designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices or machines on which the computer program operates, or those who use such devices or machines, and is not used or maintained in a manner that facilitates copyright infringement.[348]

The DMCA's security-testing exemption is not unlimited, as researchers must meet four requirements to qualify: (1) the device must be "lawfully acquired; (2)

341. Orin Kerr, *Obama's Proposed Changes to the Computer Hacking Statute: A Deep Dive*, WASH. POST (Jan. 14, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/01/14/obamas-proposed-changes-to-the-computer-hacking-statute-a-deep-dive/.

342. Connor C. Turpan, *Whistleblower? More Like Cybercriminal: The Computer Fraud and Abuse Act as Applied to Sarbanes-Oxley Whistleblowers*, 42 RUTGERS COMPUT. & TECH. L.J. 120, 140–41 (2016).

343. Press Release, Senator Ron Wyden, Wyden, Lofgren, Paul Introduce Bipartisan Bicameral Aaron's Law to Reform Abused Computer Fraud and Abuse Act (Apr. 21, 2015), https://www.wyden.senate.gov/news/press-releases/wyden-lofgren-paul-introduce-bipartisan-bicameral-aarons-law-to-reform-abused-computer-fraud-and-abuse-act-.

344. Patterson, *supra* note 333, at 531.

345. *Id.* at 530.

346. *Id.* at 531.

347. 17 U.S.C. § 1201(a) (2012).

348. 37 C.F.R. § 201.40(b)(7)(ii) (2016).

during research, researchers must operate "solely for the purpose of good-faith security research"; (3) researchers must not violate the CFAA; and (4) researchers must not have begun researching prior to the exception's enactment.[349]

Enacting an exemption for researchers investigating discriminatory behavior under the CFAA would serve a similar purpose to the DMCA's exemption: to protect testers investigating technological vulnerabilities that would harm the community at large. The Federal Trade Commission ("FTC") commented that the DMCA's exemption "take[s] away a legal hurdle and help[s] protect conduct without fear of legal recourse."[350] Similarly, under the CFAA researchers would no longer have to worry about being subject to unlimited liability for data-scraping websites in carefully controlled testing environments.[351]

Legislative reform takes months, and the president only signs approximately 5% of all proposed bills into law.[352] Moreover, amending the CFAA may raise new, more challenging issues than those that already exist with the current version. Thus, legislative reform should be one aspect of a broad legislative framework.

2. Empower Agencies to Investigate and Police Algorithmic Discrimination

Administrative agencies may exercise their congressional authority to limit website owners from drafting unequal, oppressive terms of use. This Note recommends that the FTC exercise its authority to regulate unfair or deceptive practices and limit website owners from imposing potentially unconscionable terms on Internet users that expose users to CFAA liability.[353] The FTC has great flexibility and may resolve new consumer-protection issues flexibly.[354] If Congress gave the FTC more authority to enforce its regulatory authority against website owners that draft abusive terms of use, it would be an appropriate use of the FTC powers.[355] Also, the FTC has consistently applied its authority to numerous aspects of data collection, tracking, use, disclosure, and processing activities.[356]

The FTC already has a regulatory framework that, if applied to the CFAA, would resolve limitations to data-scraping activity. The "privacy by design" framework provides a "systematic approach to privacy and data security."[357] A

349. *Id.* §§ 201.40(b)(7)(i)–(ii).

350. Aaron Alva, *DMCA Security Research Exemption for Consumer Devices*, FTC (Oct. 28, 2016, 2:12 PM), https://www.ftc.gov/news-events/blogs/techftc/2016/10/dmca-security-research-exemption-consumer-devices.

351. *Id.*

352. Aurelian Braun, *Out of 5,000 Bills in Every Congress, Guess How Many Become Law?*, MIC (Aug. 10, 2013), https://mic.com/articles/59033/out-of-5-000-bills-in-every-congress-guess-how-many-become-law#.0iowYWfeo.

353. Federal Trade Commission Act, 15 U.S.C. § 45(a) (2012).

354. Sarah Cathryn Brandon, *What's Mine Is Yours: Targeting Privacy Issues and Determining the Best Solutions for Behavioral Advertising*, 29 J. MARSHALL J. COMPUTER & INFO. L. 637, 642 (2012).

355. *See, e.g.*, Lesley Fair, *The Lessons of Listening*, FED. TRADE COMM'N (July 23, 2015, 1:32 PM), https://www.ftc.gov/news-events/blogs/business-blog/2015/07/lessons-listening.

356. *Privacy & Data Security Update (2016)*, FED. TRADE COMM'N (Jan. 2017), https://www.ftc.gov/reports/privacy-data-security-update-2016.

357. Edith Ramirez, Comm'r, Fed. Trade Comm'n, Remarks at the Privacy By Design Conference: Privacy by Design and the New Privacy Framework of the U.S. Federal Trade Commission 2 (June 13, 2012),

core principle of privacy by design is simplified choice. The FTC strongly recommends that "[c]ompanies should give consumers clear and simple choices about their data at a relevant time and context, outside of lengthy privacy policies or terms of service" beyond mere notice and consent.[358] Privacy by design is consumer focused because it proposes to stop data collection on websites for "all purposes other than those . . . consistent with the context of the consumer's interaction with a website."[359] While it is a self-regulated framework, privacy by design would inform the FTC when it enforces regulatory authority over private actors.[360]

The same principles that underlie the defunct "Do Not Track" bill, supported by the privacy-by-design framework, would also protect researchers who data scrape websites. The Do Not Track Online Act of 2011 proposed "a mandatory browser-based Do Not Track mechanism that would allow users to opt out of having their information collected online."[361] Similar mechanisms could limit more terms of use outside of collecting, tracking, and using Internet users' activities. Beyond opting out of having information collected online, users should be able to specifically opt in or opt out of other terms-of-use restrictions, such as data scraping. While it has attempted to restrict data scraping in the context of data brokers who collect and sell personally identifiable information for profit,[362] the FTC should not be as concerned with researchers protected by civil rights laws when they scrape for nonprofitable purposes.

Self-regulation, without executive support, is not enough. Without expressed mandates and required, flexible frameworks, corporations may experiment to protect themselves at the expense of Internet users and researchers.[363] The current presidential administration would likely not be supportive of this recommendation, however, and would likely direct the FTC not to exercise its authority to prosecute corporations for drafting and enforcing abusive website terms of use.[364] Regardless, stronger agency regulation and enforcement would support future legislation and prevent online abuses for researchers investigating discrimination.

https://www.ftc.gov/sites/default/files/documents/public_statements/privacy-design-and-new-privacy-framework-u.s.federal-trade-commission/120613privacydesign.pdf.

358. *Id.*

359. *Id.*

360. *Id.*

361. Tanzina Vega, *'Do Not Track' Privacy Bill Appears in Congress*, N.Y. TIMES: MEDIA DECODER (May 6, 2011, 5:01 PM), https://mediadecoder.blogs.nytimes.com/2011/05/06/do-not-track-privacy-bill-appears-in-congress/?_r=0.

362. Mary Graw Leary, Katz *on a Hot Tin Roof-Saving the Fourth Amendment from Commercial Conditioning by Reviving Voluntariness in Disclosures to Third Parties*, 50 AM. CRIM. L. REV. 341, 353 (2013).

363. Brandon, *supra* note 354, at 669.

364. *See President Trump's War on Regulation Results in Near-Record High CEO Confidence*, WHITE HOUSE (Feb. 8, 2017), https://www.whitehouse.gov/blog/2017/02/08/trumps-war-regulation-results-near-record-high-ceo-confidence.

B. Nonregulatory Solutions

Considering the uncertainty of legislative reform and administrative action under the current presidential administration,[365] websites restricting researchers from data scraping to test for discrimination may want to consider alternatives to legal reform.

Website owners could consider additional private measures to prevent costly litigation and legislative reform in the future. Litigation is time consuming compared to the expediency of alternative forms of resolution, with criminal felony trials taking anywhere from 4.7 months to 14.7 months to resolve[366] and civil trials taking anywhere from 16.3 months to 29 months.[367] Parties would also be afforded confidentiality by not resolving their grievances in court. Party filings and court cases are public records and widely available to the public through Internet-based providers.[368] Alternative forms of resolutions, like arbitration and mediation, are confidential to the public.[369] Alternative resolution is also flexible, and parties do not need to conform to the court procedural rules when finding solutions to disputes.[370]

While many benefits exist to implementing alternative resolution to resolve researcher liability under the CFAA, alternative resolution is not perfect. In many cases, especially in arbitration, alternative resolution "too often mutates into a private judicial system that looks and costs like the litigation it [is] supposed to prevent."[371] In fact, many aspects of alternative resolution mimic the structure of litigation, impacting its overall cost for the consumer.[372] Also, the legal community views alternative forms of resolution as just that—an alternative—and not the preferred way of resolving disputes.[373]

The following sections advocate for website owners and researchers to consider two public incentivizing schemes: (1) encouraging private companies to establish compensated disclosure programs; and (2) negotiating and sponsoring researchers to data scrape the website owner's websites and publish the findings after the researchers remedy the situation.

365. *See supra* Section IV.A.

366. Jordan M. Singer & Hon. William G. Young, *Measuring Bench Presence: Federal District Judges in the Courtroom, 2008-2012*, 118 PENN ST. L. REV. 243, 273 (2013).

367. Patrick E. Longan, *The Shot Clock Comes to Trial: Time Limits for Federal Civil Trials*, 35 ARIZ. L. REV. 663, 671 (1993).

368. *See, e.g.*, *Find a Case*, U.S. COURTS, http://www.uscourts.gov/courtrecords/find-case-pacer (last visited Jan. 16, 2018) (providing electronic and paper court records of case filings through PACER).

369. *Is Mediation Confidential*, FREEADVICE, http://law.freeadvice.com/litigation/mediation/mediation_confidential.htm (last visited Jan. 16, 2018).

370. Joan Meier, *The "Right" to A Disinterested Prosecutor of Criminal Contempt: Unpacking Public and Private Interests*, 70 WASH. U. L.Q. 85, 110 (1992).

371. Todd B Carver & Alberta A. Vonda, *Alternative Dispute Resolution: Why It Doesn't Work and Why It Does*, HARV. BUS. REV., May–June 1994, https://hbr.org/1994/05/alternative-dispute-resolution-why-it-doesnt-work-and-why-it-does.

372. *Id.*

373. *Id.*

1. Encourage Private Companies to Reward Disclosure

Website owners could learn from recent public compensated disclosure programs to incentivize reporting discriminatory online activity. One example of this is bug bounty programs, which compensate white-hat hackers for reporting security vulnerabilities.[374] The goal of programs like this is to combat black-market sales of vulnerabilities found in company's security protocols.[375] Corporations may compensate individuals who report bugs as they see fit, providing rewards as extravagant as, for example, 1,000,000 frequent-flyer points.[376] Compensating disclosures from the public provides many incentives for both companies and consumers: bug bounty programs are cost-effective, solicit skillsets and expertise outside of the private company, and encourage stronger security measures.[377] These programs may also have drawbacks, however, as skilled staff members need to examine all bug reports, and the corporation must meet the administrative burden of setting up the program.[378]

Bug bounty programs have been successful for private corporations and public entities. Google paid researchers $3 million in total, with the largest single award totaling $100,000, for reporting vulnerabilities in Google's Chromebook and Android operating system for phones.[379] Yelp, a website and web application for restaurants, shopping, and entertainment recommendations, rewarded researchers $17,000 in the first six months of its bug bounty program and used the program to hire more full-time security employees.[380] Similarly, the United States Army launched its first bug bounty program in November 2016.[381] During the one month the program ran, researchers uncovered and reported 118 security vulnerabilities in the Army's Human Resource Command's website, one of which allowed hackers direct access to a Department of Defense internal network from GoArmy.com, and the Army's program paid out over $100,000.[382]

Websites can establish similar programs for researchers to research their algorithms and report potentially discriminatory outcomes. Researchers would provide a benefit to websites by exposing discriminatory outcomes on websites because uncorrected discrimination, even if unintentional, would "not just [be]

374. Cassandra Kirsch, *The Grey Hat Hacker: Reconciling Cyberspace Reality and the Law*, 41 N. KY. L. REV. 383, 386 (2014).

375. Steven M. Bellovin et. al., *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 NW. J. TECH. & INTELL. PROP. 1, 42 (2014).

376. Mohit Kumar, *Two Hackers Win Over 1 Million Air Miles Each for Reporting Bugs in United Airlines*, HACKER NEWS (Aug. 9, 2016), http://thehackernews.com/2016/08/united-airlines-air-miles.html.

377. Paul Rubens, *How Bug Bounty Programs Bring Big Savings and Better Security*, CIO (July 23, 2013, 8:00 AM), http://www.cio.com/article/2383927/outsourcing/how-bug-bounty-programs-bring-big-savings-and-better-security.html.

378. *Id.*

379. Taylor Hatmaker, *Google's Bug Bounty Program Pays Out $3 Million, Mostly for Android and Chrome Exploits*, TECHCRUNCH (Jan. 31, 2017), https://techcrunch.com/2017/01/31/googles-bug-bounty-2016/.

380. Kate Conger, *Yelp's Bug Bounty Improves Security and Attracts Talent*, TECHCRUNCH (Feb. 13, 2017), https://techcrunch.com/2017/02/13/yelps-bug-bounty-improves-security-and-attracts-talent/.

381. Jared Serbu, *Army's First-Ever Bug Bounty Finds Entry Points to Sensitive DoD Systems*, FED. NEWS RADIO (Feb. 1, 2017, 11:00 AM), http://federalnewsradio.com/on-dod/2017/02/armys-first-ever-bug-bounty-finds-entry-points-to-sensitive-dod-systems/.

382. *Id.*

damaging to [its] reputation, it also raises the unpalatable prospect of vital customer data being compromised."[383] Moreover, by encouraging public participation, website owners encourage its patrons to eradicate discrimination and ensure equal treatment for all website users. For website owners, this would be a strong, cost-efficient strategy to incentivize ethical data scraping.[384]

2. Encourage Negotiations Between Researchers and Website Owners

To avoid litigation, website owners and researchers could negotiate to find a common solution. Negotiation is a "consensual bargaining process in which the parties attempt to reach agreement on a . . . potentially disputed matter . . . without the intervention of third parties."[385] In the United States, negotiations are typically adversarial—where each side has an extreme position and slowly makes concessions until each party finds a middle ground, likely splitting the difference.[386]

Companies already retroactively take these actions when accusations of discrimination emerge. Recently, Susan Fowler, a former engineer at the ride-sharing app Uber, published a blog post alleging Uber's unresponsiveness to discrimination and sexual harassment.[387] In response, Uber's Former Chief Executive Office Travis Kalanick opened an internal investigation and selected Arianna Huffington, an Uber board member, and former attorney general Eric Holder to lead it.[388] When asked about the investigation, Holder made it clear that Uber granted him the independence needed to uncover Uber's unintended discriminatory corporate structure:

> I think I've demonstrated throughout my career the ability to be independent, to not be afraid to express contrary views, and that's what I've told everybody here at Uber. If you are going to ask me to do this, you have to be prepared for me to simply look at the facts as they are, look at the policies as they are, look at the culture as it is and make recommendations, make findings on that basis, without any regard for anything other than that.[389]

Holder performed a similar investigation for Airbnb Inc., an online hospitality service, after customers complained they were racially discriminated against when trying to book rentals.[390]

383. *The Benefits of Bug Bounties*, CYBER SEC. EVENT SERIES (June 6, 2016), http://www.cyber-security.events/benefits-of-bug-bounties/.

384. *See id.*

385. *Negotiation*, BLACK'S LAW DICTIONARY (10th ed. 2014).

386. Harold I. Abramson, *Problem-Solving Advocacy in Mediations*, 59 DISP. RESOL. J. 56, 57 (Aug.–Oct. 2004).

387. *See* Susan J. Fowler, *Reflecting on One Very, Very Strange Year at Uber*, SUSAN J. FOWLER BLOG (Feb. 19, 2017), https://www.susanjfowler.com/blog/2017/2/19/reflecting-on-one-very-strange-year-at-uber.

388. Mike Isaac, *Inside Uber's Aggressive, Unrestrained Workplace Culture*, N.Y. TIMES (Feb. 22, 2017), https://www.nytimes.com/2017/02/22/technology/uber-workplace-culture.html.

389. Eric Newcomer & Brad Stone, *Uber Investigator Eric Holder Asserts His Independence*, BLOOMBERG L. (Feb. 24, 2017), https://bol.bna.com/uber-investigator-eric-holder-asserts-his-independence/.

390. *Id.*

Before trial, negotiation outside of the courtroom "offers another way to resolve some or all remedial issues."[391] Negotiations reduce the role of judges, minimize the intrusiveness of the potential outcome for one party, and enhances the agreement's success.[392] Negotiation outside of trial functions similarly as a public good, allowing both parties to find equitable solutions without the costs of litigation or lobbying.[393]

Private agreements between website owners and researchers could result in an equally successful outcome. Website owners could privately allow for researchers to data scrape their website's algorithmic behavior and resolve any discriminatory outcomes if they exist, on the condition that the researchers may still publish their results. Website owners would prevent potential litigation, and researchers would still be able to publish their findings, with the caveat that the website would remain anonymous and take swift action to remedy the situation. Website owners would have the additional benefit of avoiding bad publicity. While many companies may still avoid litigation to deemphasize negative publicity, even in anonymity, negotiations provide an effective way for both parties to meet their goals without stepping into a courtroom.

V. CONCLUSION

Considering the rapid expansion of technology and Internet activity over the past twenty years, much remains unclear about the scope of the CFAA and its enforceability of browse-wrap and click-wrap contracts.[394] Courts may begin to follow the Ninth Circuit, not criminalizing computer-use restrictions based on website terms-of-use agreements.[395] Within the last year, however, a district court contradicted this holding and criminalized corporate computer use for violating a company website's terms of use.[396] Due to Congress's lack of expediency, "[c]orrecting [the CFAA]—enacted more than a quarter century ago—to work in the Digital Age will take a significant amount of time . . . [and] will require sustained public engagement and support."[397]

391. Robert E. Buckholz, Jr. et. al., *The Remedial Process in Institutional Reform Litigation*, 78 COLUM. L. REV. 784, 809 (1978).

392. *Id.* at 810.

393. Jeffrey Kucik & Krzysztof J. Pelc, *Measuring the Cost of Privacy: A Look at the Distributional Effects of Private Bargaining*, 46 BRITISH J. POL. SCI. 861, 865–69 (2015), https://www.cambridge.org/core/journals/british-journal-of-political-science/article/measuring-the-cost-of-privacy-a-look-at-the-distributional-effects-of-private-bargaining/4572C5E003235E54D5C1C6001D5C952A.

394. *See* Alison S. Brehm & Cathy D. Lee, *From the Chair: "Click Here to Accept the Terms of Service*, 31 A.B.A., http://www.americanbar.org/publications/communications_lawyer/2015/january/click_here.html (last visited Jan. 16, 2018); Eric D. Welsh & Sarah A. Fulton, *Fighting Theft of Company Data Through the CFAA*, LAW360 (July 16, 2010, 1:20 PM), https://www.law360.com/articles/180177/fighting-theft-of-company-data-through-the-cfaa.

395. United States v. Drew, 259 F.R.D. 449, 467 (C.D. Cal. 2009).

396. Aileen Nguyen, *Violating Terms of Use Isn't a Crime, EFF Tells Court—Again*, ELECTRONIC FRONTIER FOUND. (Feb. 6, 2017), https://www.eff.org/deeplinks/2017/02/violating-terms-use-isnt-crime-eff-tells-court-again.

397. Zoe Lofgren & Ron Wyden, *Introducing Aaron's Law, A Desperately Needed Reform of the Computer Fraud and Abuse Act*, WIRED (June 20, 2013, 9:30 AM), https://www.wired.com/2013/06/aarons-law-is-finally-here/.

Under the CFAA, breaching a website's terms-of-use agreements may lead to unilaterally determined liability. Based on its current interpretation, the CFAA is so broad that it does not adequately represent modern users' technological concerns. This issue is no longer hypothetical: researchers from First Look Media Works preemptively sued the Justice Department, claiming that the CFAA violated their Fifth Amendment rights to due process.[398] Christian Sandvig, one of these researchers, stated that "[b]eing able to run socially beneficial studies like ours is at the heart of academic freedom. . . . We shouldn't have to fear prosecution just because we're doing our jobs."[399] Based on President Donald Trump's "Two-for-One" Executive Order, however, legal and regulatory action is not likely to occur in the next four years, even though the current administration claims to strongly support cyber-related protections.[400]

President Abraham Lincoln once stated that "[p]rohibition goes beyond the bounds of reason in that it attempts to control a man's appetite by legislation and make crimes out of things that are not crimes."[401] While not made in the context of a computerized world, President Lincoln's statement is particularly salient in the content of the CFAA. With computers and the Internet, Congress needs to read the terms and update to the newest version—and fast.

398. Zetter 2, *supra* note 35.

399. *Id.* (quotations omitted).

400. *See* Exec. Order No. 13771, 82 Fed. Reg. 9339 (Jan. 30, 2017); Bourree Lam, *Trump's 'Two-for-One' Regulation Executive Order*, ATLANTIC (Jan. 30, 2017), https://www.theatlantic.com/business/archive/2017/01/trumps-regulation-eo/515007/.

401. Wayne Winegarden & Donald Rieck, *Taxing Choice and the Road To Prohibition*, FORBES (Oct. 25, 2016, 9:20 AM), https://www.forbes.com/sites/econostats/2016/10/25/taxing-choice-and-the-road-to-prohibition/#2528ae117285.