YALE LAW & POLICY REVIEW

Protecting Deceptive Academic Research Under the Computer Fraud and Abuse Act

Brian Z. Mund[*]

INTRODUCTION

Professors Alan Mislove and Christo Wilson wanted to test a number of housing and employment website algorithms for the presence of hidden

* Yale Law School, J.D. 2018; University of Pennsylvania, B.A., 2013. I am grateful to Professor Frederick Lawrence for his feedback on early drafts of this Comment. Many thanks to Jacob van Leer, Stephanie Garlock, and Simon Zhen at the *Yale Law & Policy Review* for their insightful comments and careful editing. All errors are mine alone.

discrimination.[1] While algorithms do not have any predisposition against any group, faulty programming can create deplorable discriminatory effects.[2] Without testing, it can be difficult to tell which algorithms discriminate and on what grounds. Mislove and Wilson devised an "audit testing" model where researchers designed the profiles of two groups of paired individuals that are equally qualified in the market being studied.[3] Under the "audit testing" model, one group consists of legally-protected minority members, and the other consists of individuals without those minority characteristics.[4] Mislove and Wilson thought the same method could work to test online discrimination: by observing the website's treatment of each individual's advertisements and application success, the researchers could assess whether the minority group received systematically inferior treatment.[5]

However, Mislove and Wilson quickly ran into a big problem: conducting their online research might violate the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030. The CFAA criminalizes a person's behavior when he or she "intentionally accesses a computer without

---

1. *See* Adam Weintraub, *"Landlords Needed, Tolerance Preferred": A Clash of Fairness and Freedom in* Fair Housing Council v. Roommates.com, 54 VILL. L. REV. 337, 338 (2009) (describing "housing discrimination through the use of online housing advertising"); *see also* Anne-Marie G. Harris, *Shopping While Black: Applying 42 U.S.C. § 1981 to Cases of Consumer Racial Profiling*, 23 B.C. THIRD WORLD L.J. 1, 55 n.259 (2003) ("Testing by the Equal Rights Center in Washington, D.C. revealed that consumer racism exists in cyberspace too.").

2. For example, a study demonstrated that an algorithmic software deployed in the criminal justice context had significant racial biases when accounting for criminal risk. *See* Julia Angwin et al., *Machine Bias*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [https://perma.cc/WX7K-N65P].

3. John Yinger, *Audits for Discrimination, in* INTERNATIONAL ENCYCLOPEDIA OF THE SOCIAL SCIENCES (William A. Darity, Jr., ed., 2d ed. 2007).

4. *Id.*

5. *Id.* The offline analog involves researchers posing as members of different groups to test for bias in the job and housing markets. *See* Daniella Kehl, Sandvig v. Lynch*: ACLU Challenges Constitutionality of CFAA Provision That Threatens Online Discrimination Research*, JOLT DIGEST, HARV. J. L. & TECH. (July 13, 2016), http://jolt.law.harvard.edu/digest/aclu-challenges-constitutionality-of-cfaa-provision-that-threatens-online-discrimination-research [https://perma.cc/ZSL7-FTX3].

authorization or exceeds authorized access."[6] If the targeted websites conditioned access on truthful disclosures of personal information, any fake user profile would violate the website's terms and conditions and would arguably amount to "unauthorized access" under the CFAA. In response, Mislove and Wilson preemptively challenged the constitutionality of the CFAA.[7]

This Comment addresses the CFAA's potentially stifling effects on important academic research and explores academics' violations of a website's access conditions through deceptive consent. Scant scholarship has explored academic deception in the online context,[8] and no previous work has considered academic freedom arguments within light of the CFAA. After identifying the "line" where violations of website terms of agreement likely transgress the CFAA, this Comment argues that researchers should receive greater latitude under the CFAA to obtain deceptive consent for website access. The Comment analogizes the interests in academic investigation to those in law enforcement operations and further contends that public university researchers, like government law enforcement agents, should be able to obtain valid consent through misrepresentation in limited circumstances. The Comment concludes that,

---

6. 18 U.S.C. § 1030(a)(2) (2018). *See* Musacchio v. United States, 136 S. Ct. 709, 713 (2016) (noting that the CFAA "provides two ways of committing the crime of improperly accessing a protected computer: (1) obtaining access without authorization; and (2) obtaining access with authorization but then using that access improperly").

7. Complaint for Declaratory and Injunctive Relief at 37, Sandvig v. Sessions, 315 F. Supp 3d 1 (D.D.C. 2018) (No. 1:16-cv-01368) ("The freedom to conduct academic research . . . [is] of paramount public importance and entitled to full protection under the First Amendment."). *See* Kim Zetter, *Researchers Sue the Government Over Computer Hacking Law*, WIRED (June 29, 2016, 10:00 AM), https://www.wired.com/2016/06/researchers-sue-government-computer-hacking-law [https://perma.cc/W29R-34BA].

8. For recent scholarship on academic deception in the digital context, see Karen Levy & Solon Barocas, *Designing Against Discrimination in Online Markets*, 32 BERKELEY TECH. L.J. 1183, 1231-32 (2017), which describes the CFAA's potential chilling effect on online academic research; Komal S. Patel, *Testing the Limits of the First Amendment: How Online Civil Rights Testing Is Protected Speech Activity*, 118 COLUM. L. REV. 1473 (2018); and Bradley Williams, *Preventing Unintended Internet Discrimination: An Analysis of the Computer Fraud and Abuse Act for Algorithmic Racial Steering*, 2018 U. ILL. L. REV. 847 (2018).

under limited conditions, academic researchers may achieve valid consent through behavior that might otherwise amount to willful code-based violations of a website's terms of service.

I. GENERAL SCOPE OF THE COMPUTER FRAUD AND ABUSE ACT

When Congress passed the CFAA, it enacted an intentionally broad statute criminalizing computer hacking. The CFAA prohibits both unauthorized use and activities that "exceed authorized use,"[9] and many commentators have expressed concerns that the expansive language regulates constitutionally protected activities that go far beyond computer hacking.[10]

In *United States v. Nosal* ("*Nosal I*"), the Ninth Circuit noted that "Congress enacted the CFAA in 1984 primarily to address the growing problem of computer hacking."[11] Both the government and the defendant agreed that the CFAA targets computer hacking, but disagreed as to the scope of the criminal prohibition on unauthorized use.[12] In *Nosal I*, Judge Kozinski warned that on its face, the CFAA's criminalization can reach as far as "g-chatting with friends, playing games, shopping or watching sports highlights."[13] As a result, the court applied the rule of lenity and defined "exceeds authorized access" as limited to violations of access restrictions and to not include use restrictions.[14]

At least one court has held that, in terms of the creation of a misdemeanor offense for an intentional violation of a website's terms of service, the CFAA is void for vagueness.[15] However, the Ninth Circuit

9. 18 U.S.C. § 1030 (2018).

10. *See, e.g.*, Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1563 (2010) ("The CFAA has become too broad to apply without careful attention to the vagueness doctrine."); 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, 1670 (2016) (offering a narrow interpretation of the CFAA to combat the CFAA's "ambiguous and broad" statutory text).

11. 676 F.3d 854, 858 (9th Cir. 2012).

12. *Id.*

13. *Id.* at 860.

14. *Id.* at 863-64.

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

sitting en banc in *Nosal II* held that the CFAA's meaning of "without authorization" had an unambiguous plain meaning and therefore refused to find the CFAA void for vagueness.[16]

A. Public Access

Since *Nosal II*, courts and scholars have agreed that merely accessing a public website, even when transgressing the website's terms of service, does not amount to a violation of the CFAA. Otherwise, the CFAA would create expansive criminal liability. For example, a website could forbid the use of a Virtual Private Network ("VPN"), and every visitor who opened the page while using a VPN would have committed a federal crime. Leading computer crime expert Orin Kerr analogizes access to a public website as akin to visiting a storefront:

> You can approach the store and peer through the window. If you see no one inside, you can try to enter through the front door. If the door is unlocked, you can enter the store and walk around. The shared understanding is that shop owners are normally open to potential customers.[17]

In a recent decision, a federal district court relied upon Kerr's analysis. In *hiQ Labs v. LinkedIn*, the court distinguished prior unauthorized use cases under the CFAA from cases that involved access to "public data."[18] The court rejected as absurd the notion that "merely viewing a website in contravention of a unilateral directive from a private entity would be a crime, effectuating the digital equivalence of Medusa."[19] Noting that the CFAA was "not intended to police traffic to publicly available websites on the Internet," the court limited 'unauthorized access' to include only instances where the website has imposed a password authentication

16. United States v. Nosal ("*Nosal II*"), 844 F.3d 1024 (9th Cir. 2016), *cert. denied*, 138 S. Ct. 314 (2017).

17. Orin S. Kerr, Essay, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1151 (2016).

18. 273 F. Supp. 3d 1099, 1109 (N.D. Cal. 2017) ("Each of these cases is distinguishable in an important respect: none of the data in *Facebook* or *Nosal II* was *public* data.").

19. *Id.* at 1110.

system to regulate access.[20] Thus, under *hiQ Labs*, online researchers could freely misrepresent information on public access websites.

B. Anyone Can Register

However, researchers might face a website that requires password authentication but is open to all through free registration. At first glance, dicta in *hiQ Labs* suggests that this sort of "password authentication system to regulate access" would be protected under the CFAA. However, Orin Kerr, whose scholarship the *hiQ Labs* court cites, argues that "[w]hen anyone can open an account, there is an implicit delegation to anyone who registers for a new account."[21] According to Kerr, in the context of public websites, the grant of website access authorizes account use for any reason. Thus, researchers should be able to use a website to create misleading and even false profiles where anyone can open an account.

This presumption of access should override most embedded terms of use phrased as access restrictions. Put otherwise, the mere presence of terms of access within a website's "terms and conditions" page should not be considered access restrictions. As Kerr points out, "terms of use may be drafted by lawyers to read like limitations on access. But companies do not actually expect the many visitors to otherwise-public websites to comply with the terms by keeping themselves out."[22] The Ninth Circuit has affirmed Kerr's view, holding that the "violation of the terms of use of a website—without more—cannot be the basis for liability under the CFAA."[23] One might justify this presumption through a notification model that emphasizes the defendant's intent to knowingly disregard clear access

20. *Id.* at 1109-12. Orin Kerr argues that "[t]he authorization line should be deemed crossed only when access is gained by bypassing an authentication requirement." Kerr, *supra* note 17, at 1161.

21. Kerr, *supra* note 17 at 1177.

22. *Id.* at 1165-66.

23. Facebook, Inc. v. Power Ventures, Inc., 828 F.3d 1068, 1077 (9th Cir. 2016); *see* Cvent, Inc. v. Eventbrite, Inc., 739 F. Supp. 2d 927, 933 (E.D. Va. 2010). Several Members of Congress also attempted to prevent a breach of contract from becoming a criminal violation through Aaron's Law, H.R. 2454, 113th Cong. § 4; S. 1196, 113th Cong. § 4. However, the bill died in committee. *See* Tiffany Curtiss, *Computer Fraud and Abuse Act Enforcement: Cruel, Unusual, and Due for Reform*, 91 WASH. L. REV. 1813, 1833 (2016).

limitations.[24] Under such a test, intentional misrepresentation would only amount to an unauthorized access if a website explicitly notified those creating fake profiles of a requirement that all accounts must contain accurate information.

C. Willful Violation

A more challenging case for deceptive online research concerns those cases where the website does not permit unrestricted access and the defendant intentionally violated those access restrictions through a "violation of code."[25] Consider, for example, a website that does not permit users under the age of twenty-one and requires registrants to fill in their birthdate. Suppose that the website's code denies registration to those who input birth dates that do not meet the minimum age requirements. Or, for the case most relevant for online discrimination researchers, the website might require that users provide truthful information upon registration. For example, Airbnb.com verifies profiles through the use of government-issued driver's licenses and passports. Such access restrictions can be analogized to entrance into a bar. While bars are public establishments, most will not allow access without proof of age.

Under the norms proposed by Orin Kerr and the standards articulated by the *hiQ Labs* court, willful deception of this kind would amount to unauthorized access in violation of the CFAA.[26] Here, the distinction between general terms of agreement and clear registration requirements

24. *See* Josh Goldfoot & Aditya Bamzai, *A Trespass Framework for the Crime of Hacking*, 84 GEO. WASH. L. REV. 1477, 1490-91 (2016) ("So long as there is sufficient proof that this notification reached the defendant, and that the defendant read it or otherwise knew of the access limitation it conveyed, the defendant's access contrary to these limitations was unauthorized.").

25. Ryan H. Niland, *Do Not Read this Article at Work: The CFAA's Vagueness Problem and Recent Legislative Attempts to Correct It*, 15 N.C. J.L. & TECH. 205, 220 (2014); Danielle E. Sunberg, *Reining in the Rogue Employee: The Fourth Circuit Limits Employee Liability Under the CFAA*, 62 AM. U. L. REV. 1417, 1429 (2013).

26. Kerr, *supra* note 17, at 1171 ("Authentication requirements should be understood as the basic requirement of a trespass-triggering barrier on the Web. By limiting access to a specific person or group, the authentication requirement imposes a barrier that overrides the Web default of open access.").

is an important one. The Second Circuit has interpreted the standard for legal enforceability of online contracts to turn on "whether a reasonably prudent offeree" would be on notice of the term at issue.[27] When terms of service are found to be otherwise enforceable, the Supreme Court has been reticent to invalidate them on First Amendment grounds. For example, when a newspaper breached an agreement protecting the anonymity of a source, the Supreme Court found that "the First Amendment does not confer on the press a constitutional right to disregard promises that would otherwise be enforced under state law."[28] Under this logic, a researcher would not be able to breach the terms of a legally enforceable agreement governing the terms of use for a website. However, as I argue below, under limited circumstances, even violations of code-based restrictions should confer effective access consent and not amount to a violation of the CFAA.

II. PERMITTING CODE-BASED VIOLATIONS: INVESTIGATIVE MISREPRESENTATIONS

Courts should not read the CFAA to criminalize all false misrepresentations made in furtherance of academic research. Courts will sometimes deem fraudulent misrepresentations to effectuate valid consent. While the body of law remains unsettled, I argue that academic researchers, like other government investigators, should have a limited right to secure access consent through deceptive tactics. Thus, I contend that there should be circumstances under which courts will find that even willful violations of online access conditions do not constitute "unauthorized access" under the CFAA.

A. Deception Does Not Necessarily Invalidate Consent

In situations in which a website has bona fide access restrictions, academic researchers might willfully violate that site's terms of use. But even where the researchers intend to knowingly deceive website owners, traditional trespass case law suggests that access terms alone should not

27. Nicosia v. Amazon.com, Inc., 834 F.3d 220, 236 (2d Cir. 2016). The First Circuit has adopted a similar test, noting that "[r]easonably conspicuous notice of the existence of contract terms and unambiguous manifestation of assent to those terms by consumers are essential if electronic bargaining is to have integrity and credibility." Cullinane v. Uber Techs., Inc., 893 F.3d 53, 61 (1st Cir. 2018).

28. Cohen v. Cowles Media Co., 501 U.S. 663, 672 (1991).

prevent online researchers from engaging in misrepresentation. The "online audits" can be analogized to the legitimate deception that occurs in "real world" audit testing. In *Desnick v. American Broadcasting Company*, undercover television reporters carried hidden cameras into eye examination centers, after promising the property owner that they would not engage in undercover reporting.[29] *Desnick* explicitly relies on the notion that "'[t]esters' who pose as prospective home buyers in order to gather evidence of housing discrimination are not trespassers even if they are private persons not acting under color of law."[30] The court grounds its decision in the parallel between discrimination testing and the ability for government agents to accept an invitation to do business and to enter upon the premises for "the very purposes contemplated by the occupant" during the course of an investigation.[31] Importantly for *Desnick*, the defendant's videotaping actions did not intrude upon "any of the specific interests that the tort of trespass seeks to protect."[32] While the line between those cases where deceit vitiates intent and those where it does not may be "fine and sometimes incoherent," the precedent establishes that under some circumstances, deception does not invalidate consent.[33]

Courts have been very permissive in allowing government agents to obtain valid consent based on misrepresentations.[34] In *Hoffa v. United States*, the Supreme Court found that an individual secretly operating as a government informant did not negate the informant's consent to be in another individual's hotel room.[35] Similarly, in *Lewis v. United States*, the Supreme Court reaffirmed the constitutionality of covert information gathering, ruling that an undercover government agent disguised as a willing purchaser of illegal drugs received lawful consent to enter the dealer's home.[36] The Court held that "the Government is entitled to use

29. 44 F.3d 1345, 1348 (7th Cir. 1995).

30. *Id.* at 1353.

31. *See* Lewis v. United States, 385 U.S. 206, 211 (1966); Northside Realty Assocs., Inc. v. United States, 605 F.2d 1348, 1355 (5th Cir. 1979).

32. *Desnick*, 44 F.3d at 1352.

33. Theofel v. Farey-Jones, 359 F.3d 1066, 1073 (9th Cir. 2004).

34. *See* Brian Mund, *Social Media Searches and the Reasonable Expectation of Privacy*, 19 YALE J.L. & TECH. 238, 252 (2017).

35. 385 U.S. 293 (1966).

36. 385 U.S. 206, 210 (1966).

decoys and to conceal the identity of its agents," and to hold otherwise would "severely hamper the Government."[37]

Courts have recognized undercover research as a legitimate means of gathering information. "Undercover work is a legitimate method of discovering violations of civil as well as criminal law."[38] Unless undercover agents could deceitfully disavow their associations, covert operations would be meaningless.[39] The Supreme Court has consistently recognized the government's interest in being able to utilize government deception and has overturned legal constructions that might "potentially threate[n] the use of properly run law enforcement sting operations."[40]

B. Academic Researchers as Government Investigators

Academics at public universities conducting deceptive online research should be viewed akin to government investigators for the purpose of deceptive consent.[41] Just as the government has a strong interest in ensuring that police can investigate crime, the government also has a deep interest in promoting academic research. When state-employed academic researchers engage in deceptive online research, they act in a capacity as government agents.

1. Deep Interest in Promoting Academic Research

The Court has long emphasized the significant government interest in academic freedom. The Court has suggested a special government interest in academic freedom as an integral means of protecting general societal welfare. Academic repression poses a high-stakes risk: "absent the academic freedom to inquire, to study and to evaluate, to gain new

37. *Id.* at 209-10.

38. United States v. Centennial Builders, Inc., 747 F.2d 678, 683 (11th Cir. 1984).

39. *Id.* ("A contrary position would enable individuals suspected of crimes to negate the effects of undercover investigations merely by inquiring of all associates at the outset whether they are government agents.").

40. United States v. Jimenez Recio, 537 U.S. 270, 276 (2003).

41. In following this analogy, this Comment adopts Grimmelman's approach that "'[a]uthorization' under the CFAA is best understood as incorporating the traditional legal understanding of consent...." James Grimmelmann, *Consenting to Computer Use*, 84 GEO. WASH. L. REV. 1500, 1521 (2016).

maturity and understanding... our civilization will stagnate and die."[42] The Supreme Court continued to stress the critical importance of academic freedom as "so fundamental to the functioning of our society,"[43] but the Court did not clarify the legal status of this valuable concept. Assessed holistically, "[t]he Court has been far more generous in its praise of academic freedom than in providing a precise analysis of its meaning."[44]

The Supreme Court has never formally recognized a constitutional right to academic research distinct from general free speech protections. The Court has, however, repeatedly recognized the important constitutional interests raised by academic freedom. In *Keyishian v. Board of Regents*, the Supreme Court declared that academic freedom "is of transcendent value to all of us" and "a special concern of the First Amendment."[45] Similarly, Justice Powell's majority opinion in *Bakke* declared that "[a]cademic freedom, though not a specifically enumerated constitutional right, long has been viewed as a special concern of the First Amendment."[46] More recently, in *Grutter v. Bollinger*, the Court reaffirmed that "[w]e have long recognized that, given the important purpose of public education and the expansive freedoms of speech and thought associated with the university environment, universities occupy a special

---

42. Sweezy v. State of N.H., 354 U.S. 234, 250 (1957); *see also* JoNel Newman, *Will Teachers Shed Their First Amendment Rights at the Schoolhouse Gate? The Eleventh Circuit's Post-*Garcetti *Jurisprudence*, 63 U. MIAMI L. REV. 761, 763-65 (2009) (tracing the history of Supreme Court jurisprudence on academic freedom).

43. Rust v. Sullivan, 500 U.S. 173, 200 (1991) ("[T]he university is... so fundamental to the functioning of our society that the Government's ability to control speech within that sphere by means of conditions attached to the expenditure of Government funds is restricted by the vagueness and overbreadth doctrines of the First Amendment.") (citation omitted); *see also* Keyishian v. Bd. of Regents, 385 U.S. 589, 603 (1967) (identifying academic freedom as a "transcendent value" and a "special concern of the First Amendment").

44. J. Peter Byrne, *Academic Freedom: A "Special Concern of The First Amendment,"* 99 YALE L.J. 251, 257 (1989).

45. *Keyishian*, 385 U.S. at 603; *see also* Adler v. Bd. of Educ., 342 U.S. 485, 511 (1952) (Douglas, J., dissenting) (arguing that that academic freedom is central to "the pursuit of truth which the First Amendment was designed to protect.").

46. Regents of the Univ. of Cal. v. Bakke, 438 U.S. 265, 312 (1978).

niche in our constitutional tradition."[47] But "[d]espite the Court's many pronouncements hinting at such an individual right, no decision of the Court has depended for its resolution on the existence of such a right."[48] In fact, several circuit and district court decisions considering academic freedom have ruled against an individual right to research and scholarship.[49]

Nevertheless, recent case law suggests that some appellate courts are willing to recognize a distinct constitutional right to academic freedom for state-employed university academics. In *Demers v. Austin*, the Ninth Circuit appeared to find a special First Amendment right to faculty speech.[50] The *Demers* court read the *Keyishian* language that academic freedom is "a special concern of the First Amendment" to distinguish between the speech of academic employees and other public employees—granting special First Amendment consideration to the academic speech of the former. Citing the Fourth Circuit's decision in *Adams v. Trustees of the University of N.C.-Wilmington*[51] as precedent,[52] *Demers* created a circuit split by answering in the affirmative the unsettled question of whether academic freedom constituted a separate and individual right.

Justice Kennedy's majority opinion in *Garcetti v. Ceballos* suggests uncertainty amongst the Court's majority as to whether expression related to academic scholarship implicates a distinct constitutional interest. The *Ceballos* majority recognized that expression related to academic scholarship might implicate additional constitutional interests not fully accounted for by the Supreme Court's customary employee-speech jurisprudence.[53] The jury is still out over whether the Supreme Court will

47. 539 U.S. 306, 329 (2003).

48. Scott R. Bauries, *Individual Academic Freedom: An Ordinary Concern of The First Amendment*, 83 MISS. L.J. 677, 679 (2014).

49. *See* Borden v. Sch. Dist. of E. Brunswick, 523 F.3d 153, 172 (3d Cir. 2008); Emergency Coal. to Defend Educ. Travel v. U.S. Dep't of the Treasury, 545 F.3d 4, 19-20 (D.C. Cir. 2008); Johnson-Kurek v. Abu-Absi, 423 F.3d 590, 593 (6th Cir. 2005); Urofsky v. Gilmore, 216 F.3d 401, 404-05 (4th Cir. 2000); Radolf v. Univ. of Conn., 364 F. Supp. 2d 204, 216 (D. Conn. 2005).

50. 746 F.3d 402, 411-12 (9th Cir. 2014).

51. 640 F.3d 550, 557 (4th Cir. 2011).

52. *See Demers*, 746 F.3d at 411.

53. *See* Garcetti v. Ceballos, 547 U.S. 410, 425 (2006).

agree with *Demers* and find a constitutional right for individual academics to speak on matters of public concern.

Regardless of the constitutional determination over a distinct individual right for academic freedom, the long line of case law evinces a profound governmental interest in promoting and developing academic ideas. The consistent judicial homage to academic freedom's "special niche in our constitutional tradition" reflects a fundamental understanding of the critical importance of the free flow of information and the pursuit of research to the maintenance of a healthy society.[54] While academic freedom operates as a protection against government interference with the development of knowledge through a flourishing marketplace of ideas, the special protection afforded to academic freedom simultaneously affirms the government's extraordinary interest in furthering that selfsame knowledge through protecting academic research. Thus, the longstanding constitutional tradition protecting academic freedom reflects a deep-seated state interest in the furtherance of academic research.

2. Academics As Government Agents

Academic researchers at public universities conduct their research in an official capacity and should receive the same endorsement for deceptive investigative tactics granted to government agents.[55] Faculty members employed by public schools are public employees.[56] In *Garcetti v. Ceballos*, the Supreme Court ruled that public employees may only receive First Amendment protection when they speak in their capacity as private citizens and not as part of their job duties as an employee.[57] Given that public university professors "necessarily speak and write "pursuant to . . . [their] official duties,"[58] *Garcetti* threatened to impliedly wipe out First

54. Grutter v. Bollinger, 539 U.S. 306, 329 (2003).

55. This claim does not preclude finding similar interests in other contexts, such as news reporting.

56. *See, e.g.*, Givhan v. W. Line Consol. Sch. Dist., 439 U.S. 410, 415 (1979) (discussing the First Amendment rights of school teachers as public employees).

57. *Garcetti*, 547 U.S. 410.

58. *Id.* at 438 (Souter, J., dissenting) (internal citation omitted).

Amendment protection for public-school faculty.[59] The *Garcetti* majority recognized the threat to faculty researchers in dicta.[60] While *Garcetti* left open the question of whether academic freedom changes the public employee speech calculus, Justice Kennedy's majority opinion clearly situates faculty researchers as government employees.

When government employees speak pursuant to their official duties, they function as agents of their government employer.[61] As the *Garcetti* majority propounded, "[r]estricting speech that owes its existence to a public employee's professional responsibilities... simply reflects the exercise of employer control over what the employer itself has commissioned or created."[62] In other words, "[t]he majority accepts... that any statement made within the scope of public employment is (or should be treated as) the government's own speech."[63]

Academic faculty members conduct their research pursuant to their official duties. Most standard faculty positions include as expected duties teaching, research, and service.[64] As such, when those faculty members

59. *See* Sheldon H. Nahmod, *Public Employee Speech, Categorical Balancing and § 1983: A Critique of* Garcetti v. Ceballos, 42 U. RICH. L. REV. 561, 563 (2008); *see also* Renken v. Gregory, 541 F.3d 769, 775 (7th Cir. 2008) (finding faculty research to constitute employee—not private—speech); Bridget R. Nugent & Julee T. Flood, *Rescuing Academic Freedom from* Garcetti v. Ceballos*: An Evaluation of Current Case Law and a Proposal for the Protection of Core Academic, Administrative, and Advisory Speech*, 40 J.C. & U.L. 115, 136 (2014) ("While the Seventh Circuit was averse to applying the *Garcetti* rule to the academically-unrelated classroom speech in *Piggee*, the *Renken* court applied the *Garcetti* rule to activity related to scholarship.").

60. *See* Garcetti v. Ceballos, 547 U.S. 410, 425 (2006) ("There is some argument that expression related to academic scholarship or classroom instruction implicates additional constitutional interests.... We need not, and for that reason do not, decide whether the analysis we conduct today would apply in the same manner to a case involving speech related to scholarship or teaching.").

61. *Id.*

62. *Id.* at 421-22.

63. *Id.* at 436 (Souter, J., dissenting).

64. *See* Jammie Price & Shelia R. Cotten, *Teaching, Research, and Service: Expectations of Assistant Professors*, 37 AM. SOCIOLOGIST 5 (2006); Colleen Flaherty, *So Much to Do, So Little Time*, INSIDE HIGHER ED (Apr. 9, 2014), https://www.insidehighered.com/news/2014/04/09/research-shows-professors-work-long-hours-and-spend-much-day-meetings

conduct their research pursuant to those required duties of their position, they engage as government agents expressing government speech. Thus, when academic researchers at public universities undertake research projects, they act as government employees assigned to augment society's collective knowledge—occasionally through online research tactics.[65]

Academic researchers at public universities should enjoy a similar but limited right to deceptive consent as granted to covert government agents. As detailed in Part 0, courts permit government agents to obtain valid consent based on misrepresentation because of the government's legitimate interest in employing such tactics to ferret out criminal activity, and the fact that disclosure would render such operations meaningless. Here, public university faculty members conduct their research as agents of the government, and their pursuit of academic freedom represents a core state interest. As with government agents seeking to uncover criminal activity, academic researchers seeking to engage in studies like audit testing for hidden discrimination are required to engage in some misrepresentation. Like their criminal investigative counterparts, the disclosure of academic researchers' identities within research settings requiring misrepresentation would severely hamper their ability to effectively further the important state interest of academic research. Therefore, academic researchers serving as government agents should

---

[https://perma.cc/5U9Q-9J47]; *see, e.g.*, *Assistant Professor*, UNIV. KAN., https://employment.ku.edu/assistant-professor/12412br [https://perma.cc/47YC-GNG5] (describing standard workload expectation as forty percent teaching, forty percent research, and twenty percent service).

65. While this analysis applies most directly to academic faculty at state universities, it can arguably extend to all academic researchers that receive government grants to pursue their research. The Fourth Amendment jurisprudence on "government action" for the purposes of a search may prove instructive in this regard. In *Walter v. United States*, 447 U.S. 649 (1980), the U.S. Supreme Court held that the same Fourth Amendment limitations applied to "any official use of a private party's invasion of another person's privacy," because the private party acted as an instrument or agent of the state. 447 U.S. at 657. *See* Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971). Similarly, private academics conducting research projects pursuant to academic research grants might be considered instruments of the state entrusted with the furthering the government interest in academic discovery.

receive the same ability to obtain valid consent through misrepresentation as their law enforcement counterparts.

C. Extending the Deceptive Consent Exception

For many public websites with code-based restrictions, transforming the terms of service to code-based access restrictions should not destroy the availability of consent obtained through misrepresentation. Instead, the traditional deceptive consent theories of tort and criminal procedure should carry over to the CFAA criminal statutory analysis. In the law enforcement context, agents may only "accept an invitation to do business and may enter upon the premises for the very purposes contemplated by the occupant."[66] When terms of service become code-based access restrictions that otherwise permit open access, courts should apply the deceptive consent doctrine to find "authorized access" under the CFAA.[67] A limited class of cases where researchers obtain access pursuant to deceptive misrepresentation should not operate as trespass (carrying criminal implications) but should instead be construed as access pursuant to legitimately authorized consent.

Critically, consent must remain the touchstone of the analysis. Maintaining consent as a required element tethers the consent exception to a limited set of circumstances. Consent also helps maintain the well-reasoned rule that public concern does not justify the unlawful gathering of information.[68] Even the presence of substantial public interest in discovering private information does not justify unlawful investigation methods conducted without consent.

---

66. Lewis v. United States, 385 U.S. 206, 211 (1966).

67. Note that if an academic researcher transgresses beyond the outer bounds of acceptable consent, the researcher would still face civil liability for breach of contract or trespass.

68. *See, e.g.*, Bartnicki v. Vopper, 532 U.S. 514, 528 (2001); *see also* Houchins v. KQED, Inc., 438 U.S. 1, 11, (1978) ("There is an undoubted right to gather news 'from any source by means within the law,' but that affords no basis for the claim that the First Amendment compels others-private persons or governments-to supply information."); Branzburg v. Hayes, 408 U.S. 665, 691 (1972) ("It would be frivolous to assert—and no one does in these cases—that the First Amendment, in the interest of securing news or otherwise, confers a license . . . to violate valid criminal laws."); Zemel v. Rusk, 381 U.S. 1, 17 (1965) ("The right to speak and publish does not carry with it the unrestrained right to gather information.").

Opponents might argue that disambiguating the edge of acceptable deceptive practices for obtaining consent poses a tall order. To be sure, the Ninth Circuit provides the somewhat cryptic test of whether the "invited mistakes go to the essential nature of the invasion [or] are merely collateral."[69] The comments to the Restatement of Torts reframe the test in similarly ill-defined tests: "[i]f the consent is induced by mistake concerning other matters, the rule [invalidating consent] does not apply."[70] Against this context, James Grimmelman's "imputed consent" test offers a helpful framework for considering the extent of acceptable deceptive practices.[71] Courts entertain the legal fiction of "imputed consent" in order to achieve the associated desirable consequences.[72]

The investigative exception for "imputed consent" to code-based restrictions should operate on two limiting principles. First, the scope of this exception should be limited.to deceptive misrepresentation to secure consent for online access. This exception should not purport to operate beyond the trespass-access context. Second, the exception should forbid the impersonation of authorized persons, at least without the consent of those authorized persons, and should instead require the use of a fictitious persona. This limiting principle serves to enforce the collateral-essential distinction outlined by the Ninth Circuit. If a discrete and bounded number of individuals has authorization to access a website, then the individual's distinct identity plays an essential factor in securing access. In contrast, if the code-based restriction allows entrance for false aliases—even if limited to a specific group—then the misrepresented identity cannot be fundamentally based on that individual's unique identity.[73] While these principles map rough boundaries for the deceptive consent exception,

69. Theofel v. Farey-Jones, 359 F.3d 1066, 1073 (9th Cir. 2004).

70. RESTATEMENT (SECOND) OF TORTS § 892B cmt. g (1979).

71. Grimmelmann, *supra* note 42, at 1515.

72. *Id.*

73. One may conceptualize this distinguishing principle as resting on a form of property interest—when the website owner grants the unbounded group of qualified individuals who meet certain criteria the right to access the site, then that unbounded sub-group receives a presumptive claim of entitlement to access. *See, e.g.*, Bd. of Regents v. Roth, 408 U.S. 564, 577 (1972) (defining property interests as "existing rules or understandings that stem from an independent source"). If an investigator may create a fictitious persona and gain access, then they face a lower bar to access—a hurdle overcome with the help of the compelling state interest.

Grimmelman rightly points out that hammering out the specific boundaries of consent in the computer use space will only arise after extensive judicial engagement with individual factual patterns.[74] In all, extending the deceptive consent exception to some academic investigations would best empower judges to effectuate the important interests enshrined in academic freedom.

CONCLUSION

Courts should not interpret the CFAA to criminalize academic research activities resulting from deceptive consent. Academic researchers at public universities, like other government investigators, should have the limited right to engage in deceptive tactics. Government agents have traditionally enjoyed the leeway to obtain valid access consent based on misrepresentation. Courts have permitted such misrepresentation because of the significant government interest in uncovering criminal activity. Like government agents, academic researchers investigative activities represent the pursuit of an important government interest in academic research. As a result, courts should sometimes deem willful misrepresentations by academic to validly effectuate consent.[75]

The lack of a clear line for deceptive online research weighs against applying the CFAA to online academic research. The CFAA has an ambiguous reach to deceptive online academic research, and the "ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity."[76] Not only are courts concerned with a fair warning requirement,[77] but vague statutes also present the risk that they "may in [themselves] deter constitutionally protected and socially desirable conduct."[78] Under the CFAA, researchers would likely retreat from

74. *See* Grimmelmann, *supra* note 42, at 1521-22.

75. Admittedly, this analogous treatment of academic and government investigations has wide ranging implications beyond the CFAA context and presents a ripe area for further research and scholarship.

76. Yates v. United States, 135 S. Ct. 1074, 1088 (2015).

77. *See, e.g.*, McBoyle v. United States, 283 U.S. 25, 27 (1931) ("[I]t is reasonable that a fair warning should be given to the world in language that the common world will understand, of what the law intends to do if a certain line is passed.").

78. United States v. Nat'l Dairy Prods. Corp., 372 U.S. 29, 36 (1963); *see also* J. Peter Byrne, *Constitutional Academic Freedom After* Grutter*: Getting Real*

exercising the full gamut of their rights due to a desire to avoid inadvertently crossing the uncertain boundaries.[79] Instead, researchers would restrict their scholarship to activity that is unquestionably permitted—such as non-deceptive research. The migration to "safe behavior" leads to the fear that the vague statutory language will quash socially desirable activity such as academic research on hidden discrimination. The First Amendment demands that statutory language "must be carefully drawn or be authoritatively construed to punish only unprotected speech and not be susceptible of application to protected expression."[80] This need for "extreme caution" in criminalizing protected activity is only magnified when confronting the Internet, where "we cannot appreciate yet its full dimensions and vast potential to alter how we think, express ourselves, and define who we want to be."[81] As such, construction of the CFAA should create a clear line permitting some willful circumvention of code-based restrictions. By recognizing the importance of academic investigations, courts can assimilate online technologies and maintain America's timeless commitment to vital academic research.

About the "Four Freedoms" of a University, 77 U. COLO. L. REV. 929, 944 (2006) ("[V]ague and overbroad statutes will inhibit exercise of important freedoms.").

79. *See* Baggett v. Bullitt, 377 U.S. 360, 367 (1964) (noting that a vague loyalty oath forbidding support of "subversive organizations" such as the Communist party may chill constitutionally protected speech, including political support for Communist political candidates).

80. Gooding v. Wilson, 405 U.S. 518, 522 (1972).

81. Packingham v. North Carolina, 137 S. Ct. 1730, 1736 (2017).