ARTICLE

# CYBERCRIME LITIGATION

JONATHAN MAYER†

*Cybercrime is, undoubtedly, a growing problem. Scarcely a week goes by without reports of massive online misconduct. The primary federal legislative response so far has been to impose computer abuse liability on network attackers. Every state has enacted a similar statute.*

*But do these cybercrime statutes actually punish and deter hackers? Members of Congress and Department of Justice prosecutors think so—and have repeatedly sought to expand the scope and consequences of liability. Meanwhile, scholars, advocates, and some judges have argued that computer abuse legislation is overbroad and ineffective. Law and policy debate has proceeded from these dueling narratives, not from data.*

*This Article presents the first comprehensive empirical analysis of litigation under the federal cybercrime statute, the Computer Fraud and Abuse Act. Drawing on a new dataset compiled from hundreds of civil and criminal pleadings, the Article addresses fundamental and unanswered questions about the on-the-ground function of cybercrime law.*

*The data reflect that there has been a nationwide cybercrime litigation explosion, and most cases look nothing like the hacker archetype. The overwhelming majority of*

† Cybersecurity Fellow, Stanford University; J.D., 2013, Stanford Law School; Ph.D. candidate, 2016, Stanford University Department of Computer Science. The author is currently serving as Chief Technologist of the Federal Communications Commission Enforcement Bureau. All views are solely the author's own and do not reflect the position of the United States Government or the Federal Communications Commission. The author is grateful to Andrew Schlossberg, Markus Brazill, and the editors of the *University of Pennsylvania Law Review*, who provided thoughtful recommendations (and endless patience) throughout the revision process. Participants at the Privacy Law Scholars Conference, and especially session chair Professor David Thaw, provided invaluable feedback on this project. The author also wishes to express gratitude to the many colleagues who contributed insights to this work, including Dan Boneh, Ryan Calo, Cindy Cohn, Hanni Fakhoury, Laura Fong, Jennifer Granick, James Grimmelmann, Anne Hilby, Marcia Hofmann, Orin Kerr, Mark Lemley, Whitney Merrill, John Mitchell, Paul Ohm, Kurt Opsahl, Chris Riley, Barbara van Schewick, Peter Swire, Lee Tien, and George Triantis. The author participated in both the *United States v. Auernheimer* and *United States v. Swartz* litigation.

*civil claims arise from mundane business and employment disputes, not sophisticated computer intrusions. And while federal prosecutors do sometimes charge serious offenders, the plurality fact pattern in criminal litigation involves a low-level government employee mishandling data. What's more, cybercrime law appears to be redundant in civil cases, and there is little reason to believe that it deters the most concerning hackers.*

*The Article closes with normative recommendations. In the near term, I suggest that (1) Congress and state legislatures should repeal civil cybercrime liability, (2) prosecutors should establish enforcement policies that prioritize significant misconduct, and (3) courts should narrowly construe cybercrime statutes to better effectuate legislative intent. As a structural matter, I challenge the net benefit of cybercrime law. An expansive computer abuse construct is a poor fit for modern technology, which is increasingly pervasive and increasingly shared. Policy should emphasize alternative means of protecting computer security and privacy.*

"[T]he majority of [cybercrime] cases still involve 'classic' hacking activities."
*—Pacific Aerospace & Electronics, Inc. v. Taylor*[1]

## INTRODUCTION

Phillip Fadriquela was the archetypal hacker.[2] By day, the twenty-six-year-old labored as a data processing drone; by night, he broke into federal computer systems. "I was just playing," he would later insist to the media.[3] In 1985, Fadriquela earned the first-ever criminal indictment under the primary federal cybercrime statute, the Computer Fraud and Abuse Act (CFAA).[4]

---

1 295 F. Supp. 2d 1188, 1196 (E.D. Wash. 2003); *see also* P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, LLC, 428 F.3d 504, 510 (3d Cir. 2005) (citing *Pacific Aerospace* for the proposition that most CFAA cases are about "classic" hacking); Dresser-Rand Co. v. Jones, 957 F. Supp. 2d 610, 616 n.7 (E.D. Pa. 2013) (citing *P.C. Yonkers* for the same underlying claim); 1st Rate Mortg. Corp. v. Vision Mortgage Servs. Corp., No. 09-C-471, 2011 WL 666088, at *3 (E.D. Wis. Feb. 15, 2011) (same); Guest-Tek Interactive Entm't, Inc. v. Pullen, 665 F. Supp. 2d 42, 45 (D. Mass. 2009) (same); Dudick *ex rel.* Susquehanna Precision, Inc. v. Vaccarro, No. 3:06-CV-2175, 2007 WL 1847435, at *5 (M.D. Pa. June 25, 2007) (same).

2 *See* Joseph B. Tompkins, Jr. & Frederick S. Ansell, *Computer Crime: Keeping Up with High Tech Criminals*, CRIM. JUST., Winter 1987, at 31, 32 (noting that Fadriquela was the only person who had ever been indicted under the 1984 law that CFAA then amended in 1986); Glenn D. Baker, Note, *Trespassers Will Be Prosecuted: Computer Crime in the 1990s*, 12 J. MARSHALL J. COMPUTER & INFO. L. 61, 65-66 (1993) (describing Fadriquela as "a Los Angeles computer hacker"); Mitch Betts, *DP Worker Charged with Hacking*, COMPUTERWORLD, Feb. 11, 1985, at 2 (highlighting the indictment); Paul Korzeniowski, *Agencies' Hacker Troubles Blamed on Bulletin Board*, COMPUTERWORLD, July 8, 1985, at 15 (outlining Fadriquela's actions in further detail).

3 *The Region: Gang Members Aid Landmark Cleanup*, L.A. TIMES, Feb. 11, 1985, at OC2.

4 Tompkins & Ansell, *supra* note 2, at 31-32. Although at the time of Fadriquela's indictment the statute was called "The Counterfeit Access Device and Computer Fraud and Abuse Act," his conviction is properly understood as the first CFAA conviction because Congress renamed the

Dyanne Deuel managed medical technicians for a chintzy chain of surgical clinics.[5] Her "1-800-GET-THIN" employer had already aroused suspicion for unusually frequent complications and misleading advertisements.[6] In 2012, Deuel dropped a bombshell whistleblower lawsuit, alleging that physicians had covered up flagrant malpractice that contributed to a patient's death.[7] In response, Deuel's employers filed their own suit alleging a civil CFAA violation.[8] To blow the whistle, they argued, Deuel had checked the patient's electronic chart.[9] She shouldn't have.

Fadriquela and Deuel bookend a radical transformation in cybercrime law. What began as a tentative legislative response to the archetypal young, rogue hacker has evolved into sweeping doctrine with severe remedies. Read broadly, contemporary cybercrime law does not just address sophisticated hacking. It also imposes worldwide civil and criminal liability that displaces trade secret, property, contract, fraud, and copyright law in the information economy.[10]

---

statute "The Computer Fraud and Abuse Act" as part of the 1986 Amendments. *See generally* Pub. L. No. 99-474, 100 Stat. 1213 (codified as amended at 18 U.S.C. § 1030 (2012)).

5 Complaint at 3, Deuel v. 1 800 GET THIN, LLC, No. BC477064 (Cal. Super. Ct. Jan. 17, 2012).

6 *See* Stuart Pfeifer, *Another Patient Dies After Lap-Band Surgery*, L.A. TIMES (Sept. 23, 2011), http://articles.latimes.com/2011/sep/23/business/la-fi-lap-band-death-20110924 [https://perma.cc/7WD4-XJWK] ("[P]atients' deaths and injuries have led to a series of wrongful-death and personal injury lawsuits against 1-800-GET-THIN, its affiliated surgery centers and doctors who performed the procedures."); Press Release, Food & Drug Admin., FDA Issues Warning Letters for Misleading Advertising of Lap-Band (Dec. 13, 2011), http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm283455.htm [https://perma.cc/7SJK-TZQT] (warning consumers that advertisements for 1-800-GET-THIN "fail to provide required risk information, including warnings, precautions, possible side effects and contraindications").

7 Complaint at 14-16, *Deuel*, No. BC477064 (Cal. Super. Ct. Jan. 17, 2012); Stuart Pfeifer, *Patients Allege 'Gruesome Conditions' at Lap-Band Clinics*, L.A. TIMES (Jan. 17, 2012), http://articles.latimes.com/2012/jan/17/business/la-fi-get-thin-whistleblower-20120118 [https://perma.cc/445R-GUP7]. The local coroner's expert subsequently described the medical practice as "gross negligence with incompetence." Stuart Pfeifer, *Errors Cited in Lap-Band Operation*, L.A. TIMES (Apr. 19, 2013), http://articles.latimes.com/2013/apr/19/business/la-fi-get-thin-rojeski-20130420 [https://perma.cc/B3DV-BTM7].

8 Complaint at 8-11, Beverly Hills Surgery Ctr., LLC v. Deuel, No. 12-CV-1789 (C.D. Cal. Mar. 2, 2012).

9 *Id.* at 8.

10 *See* 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, 441-51 (explaining how a CFAA claim is both easier to prove than a trade secret claim and less limited by concessions to employee mobility and morality); 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, 340-41 (2004) (noting how CFAA can protect uncopyrightable information without the limitations of contract law); Maureen A. O'Rourke, *Common Law and Statutory Restrictions on Access: Contract, Trespass, and the Computer Fraud and Abuse Act*, 2002 U. ILL. J.L. TECH. & POL'Y 295, 297-310 (comparing contract, copyright, and trespass to chattels protections against CFAA); Thomas E. Booms, Note, *Hacking into Federal Court: Employee "Authorization" Under the Computer Fraud and Abuse Act*, 13 VAND. J. ENT. & TECH. L. 543, 550-51 (2011) (noting that a CFAA claim is easier to prove than a trade secret claim); Katherine Mesenbring Field, Note, *Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 MICH. L. REV. 819, 845-46 (2009) (same);

Proponents of expansive cybercrime law in both the legislative and executive branches have emphasized the government's need to combat online threats that are growing in frequency, impact, and sophistication.[11] Scholars, advocates, and some judges, meanwhile, have argued that computer abuse legislation is overbroad and ineffective.[12] The debate over the appropriate scope and sanctions for cybercrime law has played out for years, based almost exclusively on these dueling narratives and their accompanying anecdotes. Hard data are long overdue.

This Article presents the first comprehensive empirical analysis of cybercrime litigation in the federal courts. Drawing on a new dataset compiled from hundreds of civil and criminal CFAA pleadings, the Article answers foundational questions about the practical function of cybercrime law.

Part I sets the stage, attempting to articulate the two competing viewpoints on cybercrime liability. It also highlights untested factual assumptions that underpin both perspectives. Part II dives into data. It begins by explaining the sources and methodology for this study, then provides quantitative responses to specific unanswered questions at the heart of the cybercrime debate. The data reflect that, in recent years, there has been a nationwide cybercrime litigation explosion—and most of these cases look nothing like hacking. The overwhelming majority of civil claims arise from mundane employment and commercial disputes, not sophisticated computer intrusions. And the most common fact pattern in criminal prosecutions arises from low-level government employees merely misappropriating data. Moreover, cybercrime law appears to be both internally and externally redundant in civil cases, and there is little reason to believe that the law meaningfully deters sophisticated hackers.

Part III offers three workable recommendations for correcting cybercrime law. Congress should repeal civil liability because it is misdirected, unnecessary, and introduces expansionist pressures. The Department of Justice should articulate a cybercrime enforcement policy that focuses resources on serious offenders and differentiates among distinct cybercrime offenses. And, to better fulfill Congressional intent, the courts should narrowly construe cybercrime statutes.

To conclude, I challenge the net benefit of cybercrime liability. I argue that dedicated cybercrime statutes have a sharply limited upside. Information technology has become too pervasive and too shared for computer abuse to

---

Garrett D. Urban, Note, *Causing Damage Without Authorization: The Limitations of Current Judicial Interpretations of Employee Authorization Under the Computer Fraud and Abuse Act*, 52 WM. & MARY L. REV. 1369, 1390-91 (2011) (arguing that CFAA threatens to displace state contract and trade secret law).

11 *See infra* Section I.A.

12 *See infra* Section I.B.

remain an expansive legal construct. Congress should focus on alternative mechanisms for promoting cybersecurity.

## I. COMPETING PERSPECTIVES ON CYBERCRIME LAW

Initially, cybercrime law was not very controversial.[13] When the state and federal legislatures began dabbling in the area in the 1970s and 1980s, they were bolstered by contemporaneous, sensationalized media reports of youthful hacking escapades.[14] Prosecutors requested new tools for investigating and combating electronic misconduct, and lawmakers were quick to equip them.[15] While a handful of commenters questioned the need for dedicated computer abuse statutes and expressed hypothetical concerns about overbreadth, they posed scant political opposition. Congress enacted CFAA in 1984, and by 2000, *every* state had a cybercrime law on the books.[16]

---

13 *See* Richard C. Hollinger & Lonn Lanza-Kaduce, *The Process of Criminalization: The Case of Computer Crime Laws*, 26 CRIMINOLOGY 101, 106-07 (1988) (recounting that media attention in the early 1980s "ensured that both the public and its elected representatives 'knew' that computer crime was a major problem and that something had to be done quickly").

14 *See id.* (describing media fixation on "juvenile hackers and the perceived threat of computer crime" in the early 1980s); Reid Skibell, *Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act*, 18 BERKELEY TECH. L.J. 909, 910, 917-18 (2003) (noting that CFAA was passed in part due to the movie *WarGames*, which reinforced a public fear of computer crime); Mary M. Calkins, Note, *They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-Hacking Regulatory Models*, 89 GEO. L.J. 171, 175-77 (2000) (emphasizing that *WarGames* strongly influenced the public's stereotype of what a hacker looks like); Declan McCullagh, *From 'WarGames' to Aaron Swartz: How U.S. Anti-Hacking Law Went Astray*, CNET (Mar. 13, 2013, 4:00 AM), http://news.cnet.com/8301-13578_3-57573985-38/from-wargames-to-aaron-swartz-how-u.s-anti-hacking-law-went-astray/ [https://perma.cc/UC55-DL2L] (describing political and media focus on The 414s, a group of young hackers that accessed sensitive government and private computer systems around the time that *WarGames* was released); *see also* Greg Pollaro, Note, *Disloyal Computer Use and the Computer Fraud and Abuse Act: Narrowing the Scope*, 2010 DUKE L. & TECH. REV. 12, ¶ 4 ("*War Games* introduced much of the country to the 'hacker,' and its influence was not lost on members of Congress, who already were trying to decide what to do about . . . network trespassers . . . ."); Tompkins & Ansell, *supra* note 2, at 31 ("[M]any [legal] practitioners probably consider computer crime to be the light-hearted, glamorous avocation of whiz kids.").

15 *See* OFFICE OF TECH. ASSESSMENT, OTA-CIT-297, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: MANAGEMENT, SECURITY, AND CONGRESSIONAL OVERSIGHT 89-91 (Feb. 1986) (providing an overview of computer crime legislative proposals in the 98th and 99th Congresses); Robin K. Kutz, Note, *Computer Crime in Virginia: A Critical Examination of the Criminal Offenses in the Virginia Computer Crimes Act*, 27 WM. & MARY L. REV. 783, 785-88 (1986) (observing that law enforcement in the 1970s realized that federal criminal law did not easily cover computer crime, so Congress intervened to pass new legislation).

16 *See Computer Crime Statutes*, NAT'L CONF. ST. LEGISLATURES (June 12, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx [https://perma.cc/96WE-3P88] (collecting state computer abuse statutes); *see also* Hollinger & Lanza-Kaduce, *supra* note 13, at 101-04 (reviewing how state law evolved to address computer crime); Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1017 (2001) ("[W]hen Vermont enacted a statute proscribing computer crime in 1999, it became the fiftieth state to devote specific legislation to computer crimes."); John Montgomery, *Computer Crime*, 24 AM. CRIM. L. REV. 429, 430 (1987) (noting the proliferation of state computer crime statutes by 1987); Douglas M. Reimer, *Judicial and Legislative Responses to Computer Crimes*, 53

Beginning in the mid-2000s, the cybercrime law debate took on new vitality—and became more heated. Prosecutors and their allies in Congress continued to request expanded authority, emphasizing the increasing frequency, magnitude, and sophistication of online attacks.[17] Section A attempts to articulate the best arguments in favor of this expansionist perspective on cybercrime law.

Scholars and advocacy organizations, meanwhile, began to press for a rollback.[18] The law had become too broad and too ambiguous, they argued. Courts started to agree, adopting narrower interpretations of statutory scope and, in one high-profile case, concluding that a criminal offense was unconstitutionally vague.[19] Section B explains this critical perspective on cybercrime, drawing on policy arguments and anecdotes of litigation abuse.

Section C closes with an explanation of why empirical analyses are overdue. Evaluating these two perspectives is impossible in the abstract, because they depend upon particular factual assumptions about the function of cybercrime law. Policymakers and the judiciary require an understanding of the law on the ground.

### A. *The Expansionist Perspective*

At one pole of the cybercrime litigation debate, proponents argue in favor of sweeping liability and stringent remedies.[20] Online malfeasance is spiraling out of control, the reasoning goes. Consumers are increasingly at risk for online fraud, identity theft, harassment, and worse. Sophisticated

---

INS. COUNS. J. 406, 419-30 (1986) (surveying computer crime statutes in twenty-three states); Michael P. Dierks, Note, *Computer Network Abuse*, 6 HARV. J.L. & TECH. 307, 322-25 (1993) (reviewing the evolution of state computer crime law); Kutz, *supra* note 15, at 789-90 (describing the varying computer crime statutes in fourty-five states by 1986).

17 ERIC A. FISCHER, CONG. RESEARCH SERV., R42114, FEDERAL LAWS RELATING TO CYBERSECURITY: OVERVIEW AND DISCUSSION OF PROPOSED REVISIONS 1 (2013).

18 *See infra* notes 32–34 and accompanying text.

19 *See infra* notes 38–39 and accompanying text.

20 The perspective in this Section is, necessarily, a synthesis of myriad viewpoints. For detailed arguments in favor of expanding cybercrime law, see generally Frank P. Andreano, *The Evolution of Federal Computer Crime Policy: The Ad Hoc Approach to an Ever-Changing Problem*, 27 AM. J. CRIM. L. 81 (1999); Richard Warner, *The Employer's New Weapon: Employee Liability Under the Computer Fraud and Abuse Act*, 12 EMP. RTS. & EMP. POL'Y J. 11 (2008); Peter A. Winn, *The Guilty Eye: Unauthorized Access, Trespass and Privacy*, 62 BUS. LAW. 1395 (2007); Sarah Castle, Note, *Cyberbullying on Trial: The Computer Fraud and Abuse Act and* United States v. Drew, 17 J.L. & POL'Y 579 (2009); Joseph P. Daly, Note, *The Computer Fraud and Abuse Act—A New Perspective: Let the Punishment Fit the Damage*, 12 J. MARSHALL J. COMPUTER & INFO. L. 445 (1993); Graham M. Liccardi, Note, *The Computer Fraud and Abuse Act: A Vehicle for Litigating Trade Secrets in Federal Court*, 8 J. MARSHALL REV. INTELL. PROP. L. 155 (2008); Matthew Aaron Viana, Note, *Aaron's Law: Reactionary Legislation in the Guise of Justice*, 10 U. MASS. L. REV. 214 (2015); Scott Zambo, Note, *Digital La Cosa Nostra: The Computer Fraud and Abuse Act's Failure to Punish and Deter Organized Crime*, 33 NEW ENG. J. ON CRIM. & CIV. CONFINEMENT 551 (2007).

intruders are ransacking businesses and universities for their intellectual property. Foreign powers are pilfering government secrets.

The usual legal mechanism for addressing misconduct is, of course, imposing liability. Businesses should have legal recourse to protect their property-like rights in information technology and intellectual assets.[21] And prosecutors should have effective legal tools for investigating and addressing online misconduct.

There are some high-profile criminal litigation successes to report. The Department of Justice effectively dismantled LulzSec, a hacker collective that breached or disabled over a dozen online services.[22] Federal prosecutors have also knocked major botnets and malware vendors offline.[23]

But because the status quo still involves an unacceptable level of cybercrime, the thinking goes, *broader* authorities and *tougher* sanctions are needed.[24] Otherwise, would-be hackers will remain insufficiently deterred (ex ante) or punished (ex post).

---

21 *See* O'Rourke, *supra* note 10, at 308 ("The CFAA essentially functions like a federal claim for trespass."); Winn, *supra* note 20, at 1397-1403 (viewing CFAA as a property right in information technology).

22 Press Release, U.S. Attorney's Office, S. Dist. of N.Y., Leading Member of the International Cybercriminal Group "Lulzsec" Sentenced in Manhattan Federal Court (May 27, 2014), http://www.justice.gov/usao-sdny/pr/leading-member-international-cybercriminal-group-lulzsec-sentenced-manhattan-federal [https://perma.cc/DV5P-4B6P]; Press Release, U.S. Attorney's Office, Cent. Dist. of Cal., Second Member of Hacking Group Sentenced to Over Year in Prison for Stealing Customer Information from Sony Pictures Computers (Aug. 8, 2013), http://www.justice.gov/usao-cdca/pr/second-member-hacking-group-sentenced-over-year-prison-stealing-customer-information [https://perma.cc/7EFZ-N6YZ]; Press Release, U.S. Attorney's Office, S. Dist. of N.Y., Manhattan U.S. Attorney Announces Guilty Plea of Jeremy Hammond for Hacking into the Stratfor Website (May 28, 2013), http://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-guilty-plea-jeremy-hammond-hacking-stratfor-website [https://perma.cc/F8N3-5PYJ]; Press Release, U.S. Attorney's Office, Cent. Dist. of Cal., Member of LulzSec Hacking Group Sentenced to Over Year in Federal Prison for 2011 Intrusion into Sony Pictures Computer Systems (Apr. 18, 2013), http://www.justice.gov/usao-cdca/pr/member-lulzsec-hacking-group-sentenced-over-year-federal-prison-2011-intrusion-sony [https://perma.cc/YAS7-3X9R]; *see also* GABRIELLA COLEMAN, HACKER, HOAXER, WHISTLEBLOWER, SPY: THE MANY FACES OF ANONYMOUS 237-75 (2014) (describing the LulzSec group).

23 *E.g.*, David B. Fein, *Major Achievements in the Courtroom: Coreflood Botnet Takedown & Civil Action*, U.S. DEP'T OF JUSTICE (July 9, 2015), http://www.justice.gov/usao/priority-areas/cyber-crime/major-achievements-courtroom-coreflood-botnet-takedown-civil-action [https://perma.cc/ZY9B-KZ73]; Press Release, U.S. Dep't of Justice, Major Computer Hacking Forum Dismantled (July 15, 2015), http://www.justice.gov/opa/pr/major-computer-hacking-forum-dismantled [https://perma.cc/5TVH-F6UF]; Press Release, U.S. Dep't of Justice, Pakistani Man Indicted for Selling 'StealthGenie' Spyware App (Sept. 29, 2014), http://www.justice.gov/opa/pr/pakistani-man-indicted-selling-stealthgenie-spyware-app [https://perma.cc/5SDQ-9ZEE]; Press Release, U.S. Dep't of Justice, U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator (June 2, 2014), http://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware [https://perma.cc/9632-DD55]; Press Release, U.S. Dep't of Justice, Cyber Criminal Pleads Guilty to Developing and Distributing Notorious SpyEye Malware (Jan. 28, 2014), http://www.justice.gov/opa/pr/cyber-criminal-pleads-guilty-developing-and-distributing-notorious-spyeye-malware [https://perma.cc/YD66-5DCZ].

24 *See, e.g.*, *Cyber Crime: Modernizing Our Legal Framework for the Information Age: Hearing Before the Subcomm. on Crime & Terrorism of the S. Comm. on the Judiciary*, 114th Cong. 5 (2015) (statement

The expansionist perspective has manifested itself in several federal legislative proposals. In 2011, the White House and the Department of Justice drafted a high-profile CFAA reform package that would have expanded the scope of liability, increased prison sentences, provided civil forfeiture authority, and added a RICO predicate offense.[25] The 2011 package has been the basis for more recent proposals, including a 2013 discussion draft that was circulated by the House Judiciary Committee staff,[26] an early 2015 White House pitch in conjunction with the State of the Union,[27] and a mid-2015 draft Senate bill.[28]

The expansionist perspective on cybercrime law is, to be sure, not an absolutist perspective. Department of Justice officials have acknowledged concerns about statutory overbreadth and have emphasized the limiting role of prosecutorial discretion.[29] More recent legislative proposals have also

---

of David M. Bitkower, Deputy Assistant Att'y Gen., U.S. Department of Justice) (describing court decisions that narrowly construe CFAA as "unfortunate") [hereinafter Bitkower statement]; *Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks: Hearing Before the Subcomm. on Crime & Terrorism of the S. Comm. on the Judiciary*, 113th Cong. 9 (2014) (statement of Leslie R. Caldwell, Assistant Att'y Gen., U.S. Department of Justice) (arguing that CFAA is not "up to date" and must "keep up with rapidly evolving technologies and uses"); *Cybercrime: Updating the Computer Fraud and Abuse Act to Protect Cyberspace and Combat Emerging Threats: Testimony Before the S. Comm. on the Judiciary*, 112th Cong. 3-4 (2011) (statement of James A. Baker, Associate Deputy Att'y Gen., U.S. Department of Justice) (arguing that federal law must "more effectively deter" computer crime and setting forth a proposal to amend the law to "increase the maximum penalties").

25 *See* GINA STEVENS & JONATHAN MILLER, CONG. RESEARCH SERV., R41941, THE OBAMA ADMINISTRATION'S CYBERSECURITY PROPOSAL: CRIMINAL PROVISIONS 3-6 (2011) (describing the provisions of the reform package).

26 *See* Mike Masnick, *Rather Than Fix the CFAA, House Judiciary Planning to Make It Worse . . . Way Worse*, TECHDIRT (Mar. 25, 2013, 5:43 AM), https://www.techdirt.com/articles/20130324/14342822435/rather-than-fix-cfaa-house-judiciary-committee-planning-to-make-it-worse-way-worse.shtml [https://perma.cc/LS2E-25HM] (describing the unattributed discussion draft and providing a copy).

27 THE WHITE HOUSE, UPDATED ADMINISTRATION PROPOSAL: LAW ENFORCEMENT PROVISIONS (2015), https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-law-enforcement-tools.pdf [https://perma.cc/7Z7Y-AT96]; *see also* Letter from Shaun Donovan, Dir., Office of Mgmt. & Budget, to John A. Boehner, Speaker of the House of Representatives (Jan. 13, 2015), https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cybersecurity-letters-to-congress-house-signed.pdf [https://perma.cc/YP7U-6U36] (presenting and summarizing the Obama Administration's proposed substantive changes to the existing statutory regime); Barack H. Obama, 2015 State of the Union Address (Jan. 20, 2015), https://www.whitehouse.gov/the-press-office/2015/01/20/remarks-president-state-union-address-january-20-2015 [https://perma.cc/CX9A-7WRH] ("I [President Obama] urge this Congress to finally pass the legislation we need to better meet the evolving threat of cyberattacks . . . .").

28 *See* Harley Geiger, *Graham/Whitehouse Draft Bill Would Make CFAA Worse*, CDT BLOG (July 17, 2015), https://cdt.org/blog/grahamwhitehouse-draft-bill-would-make-cfaa-worse/ [https://perma.cc/F5ND-68JC] (explaining the proposed legislation and providing a copy).

29 *See* Bitkower statement, *supra* note 24, at 6 ("These [limiting] judicial decisions stemmed from the concern that the relevant provision of the CFAA could potentially make relatively trivial conduct a federal crime—such as checking the baseball scores . . . in violation of an employer's strict Internet use policy. The department has no interest in prosecuting such harmless acts."); Leslie R. Caldwell, *Prosecuting Privacy Abuses by Corporate and Government Insiders*, U.S. DEP'T OF JUST.:

included (very modest) protections for ordinary Internet users.[30] But the core of the viewpoint remains that cybercrime law is a valuable and effective tool, and litigation abuses are and will be rare and manageable.

JUST. BLOGS (Mar. 16, 2015), http://www.justice.gov/opa/blog/prosecuting-privacy-abuses-corporate-and-government-insiders [https://perma.cc/4LNL-PXN2] ("We understand these [overbreadth] concerns. The Department of Justice has no interest in prosecuting harmless violations of use restrictions like these.").

30 The 2015 Obama administration proposal would introduce a new monetary threshold for CFAA liability. *See* THE WHITE HOUSE, *supra* note 27 (triggering liability under CFAA only if the value of the illegally-acquired information exceeds $5000). Given how easily litigants have pled around CFAA's existing monetary threshold, it is not apparent that this provision would meaningfully constrain liability.

### B. *The Critical Perspective*

A competing view of cybercrime liability has gained traction,[31] particularly among scholars,[32] policy advocates,[33] and members of the

31 While this Article endeavors to objectively assess cybercrime litigation in the federal courts, in the interest of complete transparency, I fall firmly within the school of thought that criticizes cybercrime law. That view is informed as much by policy and legal considerations as it is by the empirical assessment presented here.

32 A voluminous academic literature has criticized cybercrime law, and especially CFAA, as overbroad or overly punitive. *See, e.g.*, Brenton, *supra* note 10, at 440-56 (explaining that CFAA presents inconsistencies with trade secret law); Galbraith, *supra* note 10, at 361-66 (arguing that courts have improperly construed CFAA to permit website owners to enforce restrictions on access to and use of copyrightable information); Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1617-32 (2003) (explaining how courts have expansively interpreted the concepts of "access" and "authorization" under CFAA to capture undesirable behavior, and arguing that such a broad sweep is normatively undesirable); Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1575-78 (2010) (arguing that a broad construction of "authorization" under CFAA may amount to unconstitutional vagueness); Andrea M. Matwyshyn, *The Law of the Zebra*, 28 BERKELEY TECH. L.J. 155, 182-208 (2013) (criticizing CFAA for permitting both criminal and civil liability for contractual breaches); O'Rourke, *supra* note 10, at 308 ("Congress likely did not intend the [CFAA] statute to become the potent weapon that it now is 'against employees, former employees, competitors and others.' Unanticipated uses of the Act have arisen because its language is not limited to cases of hacking but instead is broad enough to encompass a wide range of conduct." (footnote omitted)); Skibell, *supra* note 14, at 922-43 (arguing that CFAA mistakenly treats the crime of trespass and the crime of fraud or theft identically, imposes unfair punishments on some individuals, has done little to slow the growth of computer crime, and imposes unnecessarily high penalties that do not serve proper deterrent or retribution purposes). *See generally* Booms, *supra* note 10; Sarah Boyer, Note, *Computer Fraud and Abuse Act: Abusing Federal Jurisdiction?*, 6 RUTGERS J.L. & PUB. POL'Y 661 (2009); Cyrus Y. Chung, Note, *The Computer Fraud and Abuse Act: How Computer Science Can Help with the Problem of Overbreadth*, 24 HARV. J.L. & TECH. 233 (2010); Dierks, *supra* note 16; Katherine Mesenbring Field, Note, *Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 MICH. L. REV. 819 (2009); Andrew T. Hernacki, Note, *A Vague Law in a Smartphone World: Limiting the Scope of Unauthorized Access Under the Computer Fraud and Abuse Act*, 61 AM. U. L. REV. 1543 (2012); Haeji Hong, Note, *Hacking Through the Computer Fraud and Abuse Act*, 31 U.C. DAVIS L. REV. 283 (1997); Nicholas R. Johnson, *Recent Developments, "I Agree" to Criminal Liability: Lori Drew's Prosecution Under § 1030(a)(2)(C) of the Computer Fraud and Abuse Act, and Why Every Internet User Should Care*, 2009 U. ILL. J.L. TECH. & POL'Y 561; Caroline G. Jones, Note, *Computer Hackers on the Cul-de-Sac: MySpace Suicide Indictment Under the Computer Fraud and Abuse Act Sets Dangerous Precedent*, 17 WIDENER L. REV. 261 (2011); Ryan Patrick Murray, Note, *MySpace-ing Is Not a Crime: Why Breaching Terms of Service Agreements Should Not Implicate the Computer Fraud and Abuse Act*, 29 LOY. L.A. ENT. L. REV. 475 (2009); Warren Thomas, Note, *Lenity on Me:* LVRC Holdings LLC v. Brekka *Points the Way Toward Defining Authorization and Solving the Split over the Computer Fraud and Abuse Act*, 27 GA. ST. U. L. REV. 379 (2011); Garrett D. Urban, Note, *Causing Damage Without Authorization: The Limitations of Current Judicial Interpretations of Employee Authorization Under the Computer Fraud and Abuse Act*, 52 WM. & MARY L. REV. 1369 (2011); Note, *The Vagaries of Vagueness: Rethinking the CFAA as a Problem of Private Nondelegation*, 127 HARV. L. REV. 751 (2013).

33 *See, e.g.*, Letter from Internet Infrastructure Coalition (i2Coalition) et al., to Rep. Jim Sensenbrenner et al. (Mar. 12, 2013), https://www.eff.org/files/cfaa_innovators_letter_3-12-13_final.pdf [https://perma.cc/4QQR-YFW8] (urging Congress to reform CFAA due to its chilling effects on innovation and economic growth in the technology field).

judiciary.[34] This perspective emphasizes how broad, vague cybercrime law poses grave legal peril for innocuous—and often desirable—computer-related conduct.[35]

Articulations of this critical viewpoint tend to invoke the following at-risk categories of computer users.

### 1. Consumers

Under expansive cybercrime liability, run-of-the-mill online conduct could become a criminal offense. In Judge Kozinski's memorable phrasing, ordinary consumers would "have to live at the mercy of [their] local prosecutor."[36] He added, "[P]osting for sale an item prohibited by Craigslist's policy, or describing yourself as 'tall, dark and handsome,' when you're actually short and homely, will earn you a handsome orange jumpsuit."[37]

The prosecution of Lori Drew is an oft-invoked anecdote in support of this critical perspective. Drew's cybercrime liability rested on breaching the social network MySpace's terms of use.[38] The district court concluded that Drew had committed a statutory offense, but set aside the jury conviction as unconstitutionally void for vagueness.[39]

More recently, federal prosecutors brought cybercrime charges against gamblers who discovered a glitch in slot machine payouts.[40] The case was dropped only after a magistrate judge recommended dismissal on statutory grounds.[41]

### 2. Employees

Surveys have consistently found that many, if not most, employees breach corporate information technology policies.[42] They shirk at work, swap

---

34 For a particularly sharp critique offered by then–Chief Judge Alex Kozinski, see United States v. Nosal, 676 F.3d 854, 862-63 (9th Cir. 2012) (rejecting an expansive interpretation of CFAA on statutory, constitutional, and policy grounds). *See also* United States v. Valle, 807 F.3d 508, 523-28 (2d Cir. 2015) (following *Nosal*); WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 203-07 (4th Cir. 2012) (same).

35 In the interest of brevity, this Article focuses on policy perspectives and empirical analysis rather than legal synthesis. For present purposes, it is sufficient to note that nearly all online conduct that is conceivably objectionable could plausibly fall within the scope of civil and criminal sanctions. *See supra* note 32.

36 *Nosal*, 676 F.3d at 862.

37 *Id.*

38 United States v. Drew, 259 F.R.D. 449, 452 (C.D. Cal. 2009); *see also Nosal*, 676 F.3d at 862 (discussing *Drew* as a poor exercise of prosecutorial discretion).

39 *Drew*, 259 F.R.D. at 464.

40 Report and Recommendation of United States Magistrate Judge at 1-2, United States v. Kane, No. 2:11-cr-00022 (D. Nev. Oct. 15, 2012), ECF No. 86.

41 *Id.* at 9.

42 *See, e.g.*, CISCO SYS. INC., DATA LEAKAGE WORLDWIDE: COMMON RISKS AND MISTAKES EMPLOYEES MAKE 1-7 (2008), http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-499060.pdf [https://perma.cc/8XXG-EW2Y] (giving numerous

passwords, take files home, and keep data when they exit the firm. All of these routine indiscretions could be criminal under a broad interpretation of cybercrime law: federal appellate courts have sustained liability merely for browsing a work database (in violation of employer policy)[43] and taking files to a competitor (in violation of fiduciary responsibilities).[44] Employers also would be equipped with a powerful civil cudgel against their former employees, enabling retaliation for exercising legal rights or whistleblowing.[45]

### 3. Entrepreneurs

Many online startups are iterative, built atop another business's technology and data.[46] A broad cybercrime law would encompass these innovation models such that failure to obtain a "platform" business's permission would result in civil and criminal liability.[47] This concern is no hypothetical—Craigslist,[48] Facebook,[49] and Oracle[50] have all used CFAA to

examples of employee misuse of information technology); PONEMON INST., DATA LOSS RISKS DURING DOWNSIZING: AS EMPLOYEES EXIT, SO DOES CORPORATE DATA 3-24 (2009), http://eval.symantec.com/mktginfo/enterprise/white_papers/b-data_loss_risks_during_downsizing_study_WP.en-us.pdf [http://perma.cc/47F4-FEU8] (providing in-depth data on misuse of confidential information); SYMANTEC CORP., WHAT'S YOURS IS MINE: HOW EMPLOYEES ARE PUTTING YOUR INTELLECTUAL PROPERTY AT RISK 2 (2013) https://www4.symantec.com/mktginfo/whitepaper/WP_WhatsYoursIsMine-HowEmployeesarePuttingYourIntellectualPropertyatRisk_dai211501_cta69167.pdf [https://perma.cc/43KA-NQHN] (showing the "top reasons" why employees take corporate data).

43 United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010).

44 Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006).

45 *See, e.g.*, Lee v. PMSI, Inc., No. 8:10-cv-2904, 2011 WL 1742028, at *2-3 (M.D. Fla. May 6, 2011) (dismissing a cybercrime counterclaim by a former employer in a wrongful termination suit, which alleged that the former employee was liable for merely checking personal email and social network accounts); *see also* United States v. Nosal, 676 F.3d 854, 860 n.6 (9th Cir. 2012) (citing *Lee* as an example of cybercrime overbreadth risks).

46 The in-vogue term for this phenomenon is "platform." *See* Benjamin Edelman, *How to Launch Your Digital Platform*, HARV. BUS. REV., Apr. 2015, at 92 (using the term "platform" to refer to shared technology foundations for new small businesses).

47 *See* ALEXIS OHANIAN, WITHOUT THEIR PERMISSION 199-231 (2013) (arguing that information technology innovation occurs without seeking permission in advance, and laws that require permission necessarily impede innovation).

48 *See, e.g.*, Craigslist Inc. v. 3Taps Inc., 964 F. Supp. 2d 1178, 1180 (N.D. Cal. 2013) (using CFAA against a business that republished classified advertisements); Craigslist Inc. v. 3Taps Inc., 942 F. Supp. 2d 962, 969 (N.D. Cal. 2013) (same); Craigslist, Inc. v. Naturemarket, Inc., 694 F. Supp. 2d 1039, 1049 (N.D. Cal. 2010) (using CFAA against a business that enabled automatic posting of classified advertisements).

49 *See, e.g.*, Facebook, Inc. v. Power Ventures, Inc., 844 F. Supp. 2d 1025, 1027-28 (N.D. Cal. 2012) (using CFAA against a website that aggregated information from multiple social network feeds); Facebook, Inc. v. MaxBounty, Inc., 274 F.R.D. 279, 281 (N.D. Cal. 2011) (using CFAA against a marketing company that created misleading social network pages).

50 *See*, *e.g.*, Oracle Am., Inc. v. TERiX Comput. Co., No. 13-cv-03385, 2014 WL 31344, at *2 (N.D. Cal. Jan. 3, 2014) (using CFAA against an aftermarket service provider for database software); Oracle Am., Inc. v. Serv. Key, LLC, No. 12-cv-00790, 2012 WL 6019580, at *3 (N.D. Cal. Dec. 3, 2012) (same).

shut down derivative ventures. Even the Internet Archive, a nonprofit online library, was targeted with cybercrime litigation on the theory that it impermissibly browsed a public website with an automated crawler.[51]

### 4. Journalists

Investigative reporting often involves assessing obscure and unintended online sources. For instance, in a recent high-profile dispute, journalists at Scripps Howard discovered that FCC-subsidized telecommunications providers had leaked sensitive subscriber information onto the public Internet.[52] One of the telecom firms responded by threatening cybercrime litigation against Scripps on the theory that the reporters lacked authorized access to the subscriber data.[53] The FCC subsequently fined the firms for their deficient security practices.[54]

In another episode, reporters from *Vanity Fair* and a local newspaper used online resources to investigate a "cult-like" executive training firm.[55] The training firm sued, alleging that *Vanity Fair*'s research constituted an actionable violation of cybercrime law.[56] After nearly two years of litigation, its claims were dismissed as untimely.[57]

### 5. Security Researchers

Outside experts routinely evaluate information technology systems for security shortcomings. But the purveyors of those systems tend to get testy when deficiencies in their products and services are unceremoniously exposed.[58] For instance, Sony used cybercrime law to prevent a young

---

51 *See* Healthcare Advocates v. Harding, Earley, Follmer & Frailey, 497 F. Supp. 2d 627, 630-33 (E.D. Pa. 2007) (describing the Internet Archive's Wayback Machine crawler and its alleged cybercrime infraction).

52 Sarah Laskow, *Reporting, or Illegal Hacking: Scripps Reporters Are Accused of Violating the Computer Fraud and Abuse Act*, COLUM. JOURNALISM REV. (June 13, 2013), http://www.cjr.org/cloud_control/scripps_hackers.php [https://perma.cc/RS3W-8S66].

53 *Id*.

54 Notice of Apparent Liability for Forfeiture, TerraCom, Inc. and YourTel America, Inc., No. EB-TCD-13-00009175, at 1 (FCC Oct. 24, 2014), https://apps.fcc.gov/edocs_public/attachmatch/FCC-14-173A1.pdf [https://perma.cc/BTE7-NDWA].

55 *See* William D. Cohan, *How a Strange, Secretive, Cult-Like Company Is Waging Legal War Against Journalists*, NATION (Nov. 18, 2014), http://www.thenation.com/article/how-strange-secretive-cult-company-waging-legal-war-against-journalists/ [https://perma.cc/AQ2L-R6W6].

56 *Id*.

57 NXIVM Corp. v. Foley, No. 14-cv-01375, slip op. at 13 (N.D.N.Y. Sept. 17, 2015)

58 *See, e.g.*, Letter from Alex Stamos et al. to the House and Senate Judiciary Comms. (Aug. 1, 2013), https://www.eff.org/files/dc_bh_letter_f4.pdf [https://perma.cc/ZP38-BDMQ] ("[P]aradoxically, the CFAA currently threatens and chills valuable research in the field by reaching mere violations of terms of use and other acts, such as security research, which cause no real harm and indeed make the public safer.").

researcher from examining its PlayStation 3 video game system;[59] the Massachusetts Bay Transportation Authority prevented MIT students from presenting flaws in its fare payment system;[60] and federal prosecutors won a conviction against a researcher who exposed a vulnerability in AT&T's iPad registration system.[61] Criticism along this line has emphasized that cybercrime liability is, in fact, backfiring: by chilling vital research, cybercrime law actually *reduces* computer security.[62]

Legal scholars have noted how conventional doctrines of trespass, labor law, trade secret, copyright, and contract make concessions to these sorts of public interests.[63] Cybercrime law, however, offers no such limiting principles. There are no implied easements. No employee rights. No secrecy and independent wrongdoing elements. No fair use defense. No limits on contract formation and interpretation. Absence of permission is too often the beginning and the end of a cybercrime liability inquiry.

These are far from the only lines of attack. Critics question the very notion of using criminal law to deter computer intrusions when perpetrators are often difficult to identify or outside the reach of United States law.[64] Some of the worst offenders are *sponsored* by foreign governments: in spring 2014, for instance, the Department of Justice indicted Chinese military officers for cybercrime offenses.[65] The litigation was purely symbolic given that "there is virtually no chance" China would turn over the indicted officers.[66] Similarly, in spring 2016, federal prosecutors indicted hackers working for Iran's Revolutionary

---

59 Sony Comput. Entm't Am. LLC v. Hotz, No. 11-cv-0167, 2011 WL 347137, at *1- 2 (N.D. Cal. Jan. 27, 2011).

60 Temporary Restraining Order at 1-2, Mass. Bay Transp. Auth. v. Anderson, No. 08-cv-11364 (D. Mass. Aug. 9, 2008).

61 United States v. Auernheimer, 748 F.3d 525, 529-30, 532 (3d Cir. 2014). The Third Circuit subsequently vacated the conviction on venue grounds. *Id.* at 529.

62 *See supra* note **Error! Bookmark not defined.** and accompanying text.

63 *See supra* note 10 and accompanying text.

64 *See* Dierks, *supra* note 16, at 332-36 (arguing that deterrence has failed in computer crime law owing to difficulty in detecting breaches, identifying perpetrators, building a case, and encouraging reporting by victims); Skibell, *supra* note 14, at 935-37 ("Deterrence theory needs to account for the empirical evidence that nineteen years under the CFAA has done little to slow the growth of computer crime."); Calkins, *supra* note 14, at 183-84 (noting practical difficulties in enforcing computer crime law).

65 Indictment, United States v. Dong, Crim. No. 14-118 (W.D. Pa. May 12, 2014); *see also* Jonathan Mayer, *Charges Against Chinese, and U.S. Policy on Hacking*, N.Y. TIMES (May 23, 2014), http://www.nytimes.com/2014/05/24/opinion/charges-against-chinese-and-us-policy-on-hacking.html [https://perma.cc/2N6V-GZ69].

66 Michael S. Schmidt & David E. Sanger, *5 in China Army Face U.S. Charges of Cyberattacks*, N.Y. TIMES (May 19, 2014), http://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html [https://perma.cc/29L8-V828].

Guard.[67] There is little reason to believe that the defendants "will ever appear in an American courtroom."[68] Computer security policy should emphasize incentives to protect information technology, the thinking goes, and not be chasing after predictable, persistent, and extraterritorial attackers.

Redundant liability is another category of concern from the critical perspective. Courts were slow at first in adapting conventional legal doctrines to information technology. But as courts have familiarized themselves with navigating computer-related disputes, conventional legal doctrines have caught up with advances in technology. There is, consequently, a lesser need for purpose-built computer causes of action.[69]

A final sticking point is the draconian sentencing regime associated with cybercrime liability, especially at the federal level.[70] This issue gained national prominence when federal prosecutors charged Internet activist Aaron Swartz with CFAA offenses that carried a maximum sentence of decades in prison.[71] Swartz tragically took his own life rather than stand trial.[72]

More recently, a middle school student in Florida logged into his teacher's computer and changed the desktop wallpaper.[73] The local sheriff's department charged him with a felony under the state cybercrime statute, carrying an adult prison sentence of up to five years.[74]

The critical view of cybercrime law has begun to manifest itself in legislative proposals. One example is Aaron's Law, a bipartisan proposal introduced in both houses of the current 114th Congress that would curb

---

67 Indictment, United States v. Fathi, No. 16 Crim. 48 (S.D.N.Y. Jan. 21, 2016).

68 David E. Sanger, *U.S. Indicts 7 Iranians in Cyberattacks on Banks and a Dam*, N.Y. TIMES (Mar. 24, 2016), http://www.nytimes.com/2016/03/25/world/middleeast/us-indicts-iranians-in-cyber attacks-on-banks-and-a-dam.html [https://perma.cc/V845-67AC].

69 *See, e.g.*, Mark Jaycox, *Why the CFAA's Excessive Criminalization Needs Reform*, ELECTRONIC FRONTIER FOUND. (Apr. 2, 2013), https://www.eff.org/deeplinks/2013/04/cfaas-excessive-criminalization [https://perma.cc/XDH3-UZU3] (identifying numerous overlaps between CFAA and other theories of criminal and civil liability).

70 *See* Orin Kerr, *A Question for Supporters of Increasing Maximum Sentences Under the Computer Fraud and Abuse Act*, VOLOKH CONSPIRACY (Mar. 28, 2013, 1:59 PM), http://www.volokh.com/2013/03/28/a-question-for-supporters-of-increasing-maximum-sentences-under-the-computer-fraud-and-abuse-act/ [https://perma.cc/SJR3-STB5] ("Congress is considering legislation to increase maximum punishments under the Computer Fraud and Abuse Act . . . . [H]ave there been *any* cases in which judges maxed out the current sentences . . . ?").

71 John Schwartz, *Internet Activist, a Creator of RSS, Is Dead at 26, Apparently a Suicide*, N.Y. TIMES (Jan. 12, 2013), http://www.nytimes.com/2013/01/13/technology/aaron-swartz-internet-activist-dies-at-26.html [https://perma/cc/9BBY-77VM].

72 *Id.*

73 Josh Solomon, *Middle School Student Charged with Cybercrime in Holiday*, TAMPA BAY TIMES (Apr. 9, 2015, 1:05 PM), http://www.tampabay.com/news/publicsafety/crime/middle-school-student-charged-with-cyber-crime-in-holiday/2224827 [https://perma/cc/F8CD-PD8Z].

74 *Id.*

CFAA's scope and penalties.[75] Another bill, proposed in the Senate during the 113th Congress, was a comprehensive data protection bill that included a provision narrowing CFAA's scope.[76]

The critical perspective on cybercrime law is—like the expansionist perspective—not absolutist. Recommendations have centered on reform, rather than total repeal.[77] Cybercrime law does play a legitimate and important role in promoting cybersecurity, the thinking goes. It has just gone too far.

### C. *Why Empirical Analyses Are Necessary*

These competing perspectives on cybercrime law are essentially competing empirical hypotheses. Proponents of the expansionist perspective do recognize the potential for cybercrime litigation abuse. And critics of broad cybercrime liability do acknowledge the value of legal remedies against hackers.

Where the two sides fundamentally part ways is their assessment of the on-the-ground, practical impact of cybercrime law. The expansionist hypothesis is that "the majority of CFAA cases still involve 'classic' hacking activities,"[78] such that cybercrime law primarily functions as a unique and proportional response to the most concerning computer abuses. The critical hypothesis is that most cases involve minor and technically unsophisticated misconduct, and cybercrime law has become redundant and excessively punitive.[79] There is no abstract means of adjudicating the descriptive accuracy of these competing hypotheses. Both sides are facially credible, bolstered by plausible arguments

75 Aaron's Law Act of 2015, H.R. 1918, 114th Cong. (2015); Aaron's Law Act of 2015, S. 1030, 114th Cong. (2015).

76 Personal Data Privacy and Security Act of 2014, S. 1897, 113th Cong. §§ 107, 110 (2014). This effort draws on an earlier reform amendment sponsored by Senators Grassley, Franken, and Lee. *See* Jake Laperruque & Greg Nojeim, *Why Fibbing About Your Age Is Relevant to the Cybersecurity Bill*, CTR. FOR DEMOCRACY & TECH. (July 30, 2012), https://cdt.org/blog/why-fibbing-about-your-age-is-relevant-to-the-cybersecurity-bill/ [https://perma.cc/3V7R-WZDA]. A prior version of Senator Leahy's proposal included a more questionable attempt to narrow CFAA. *See* Orin Kerr, *My Assessment of Senator Leahy's Proposed Amendment to the CFAA*, VOLOKH CONSPIRACY (Nov. 22, 2011, 5:53 PM), http://www.volokh.com/2011/11/22/my-assessment-of-senator-leahys-proposed-amendment-to-the-cfaa/ [https://perma.cc/KM5K-G6KJ] (explaining the prior Leahy proposal and noting that it may be ineffective).

77 *But see* Eric Goldman, *The Computer Fraud and Abuse Act Is a Failed Experiment*, FORBES (Mar. 28, 2013, 4:21 PM), http://www.forbes.com/sites/ericgoldman/2013/03/28/the-computer-fraud-and-abuse-act-is-a-failed-experiment/ [https://perma/cc/Z8XU-E526] (arguing in favor of substantial repeal); Robert Graham, *Aaron's Law: Repeal CFAA Rather Than Amend It*, ERRATA SECURITY (Jan. 17, 2013), http://blog.erratasec.com/2013/01/aarons-law-get-rid-of-cfaa.html#.VtYtC5OzLxM [https://perma.cc/4RER-L5AU] (suggesting that total repeal would not create additional vulnerabilities or remove penalties for other cybercrimes).

78 Pacific Aerospace & Elecs., Inc. v. Taylor, 295 F. Supp. 2d 1188, 1196 (E.D. Wash. 2003); *see also supra* note 1.

79 *See supra* Section I.B.

and effective anecdotes. Only data can determine which hypothesis is more precise—and so far, data have been entirely missing from the debate.

The balance of this Article illuminates these competing hypotheses with data, providing the first comprehensive empirical analysis of cybercrime litigation.[80] I focus on CFAA, since it is the best-known and most frequently litigated cybercrime statute.

## II. AN EMPIRICAL EVALUATION OF CYBERCRIME LITIGATION

Section A opens by explaining data sources and methodology. This Section assumes that readers have rough familiarity with CFAA's structure and individual offenses.

Sections B and C begin the descriptive empirical analysis by examining longitudinal trends in order to understand the scale and severity of cybercrime litigation. Section B reports that civil cybercrime litigation has skyrocketed, while the criminal caseload steadily increased but then leveled off in the past decade. Section C examines criminal penalties, finding that the mean period of incarceration has greatly lengthened, but that the median case still results in no prison sentence.

Section D shifts to detailed latitudinal analysis of fact patterns, categorizing the conduct and party relationships that underlie cybercrime litigation. The data reflect that most civil cases involve technically unsophisticated conduct in the context of a commercial or employment dispute. Among criminal cases, the plurality fact pattern merely involves government employees misappropriating information.

Section E examines whether cybercrime law is redundant. Data on civil claims suggest that CFAA's various provisions substantially overlap with existing causes of action, which alone are sufficient. Criminal charging data are murkier, suggesting that CFAA offenses are somewhat unique—but that prosecutors strategically blur theories of liability where sentencing enhancements are available.

Section F takes up the question of deterrence. I compare the federal cybercrime caseload to the estimated scope of cybercrime harm and find an extraordinary mismatch. There is little cause to believe that cybercrime law meaningfully deters sophisticated misconduct.

---

80 There has been remarkably little quantitative research on cybercrime law. *But see* Anele Nwokoma, *Process Evaluation of the Computer Fraud and Abuse Act of 1986*, 17 PROC. INFO. SYS. EDUC. CONF. § 128 (2000) (reporting Department of Justice statistics on CFAA usage); George Roach & William J. Michiels, *Damages Is the Gatekeeper Issue for Federal Computer Fraud*, 8 TUL. J. TECH. & INTELL. PROP. 61, 62 (2006) (finding that many courts reject civil CFAA claims for insufficient "loss" or "damage"); McCullagh, *supra* note 14 (plotting longitudinal invocation of CFAA in federal opinions).

Section G closes the analysis by comparing the two high-level hypotheses of cybercrime law against the empirical results. I conclude that there is strong support for the critical hypothesis as applied to civil litigation. In criminal cases, though, I find a more complex picture. There is evidence of overbreadth and ineffective deterrence, in line with the critical hypothesis. But there is also some evidence of prosecutorial discretion and charge uniqueness, in accord with the expansionist hypothesis.

### A. *Data Sources and Methodology*

The empirical analysis in this Article draws on data from civil pleadings, criminal charging documents, judicial opinions, sentencing records, and news reports.

Detailed data on civil claims and criminal charges are difficult to obtain. At present, there are no means of searching the text of all federal litigation filings. To build a comprehensive latitudinal dataset of civil pleadings and criminal charging documents,[81] I began with expansive keyword searches on Bloomberg Law and Westlaw for CFAA-related court filings.[82] Next, I augmented the results with charging materials from Department of Justice public announcements. I then manually winnowed the documents, labeling each with CFAA claims/charges,[83] non-CFAA claims/charges, party/victim relationships, and underlying conduct.[84] In total, I reviewed approximately 600 court filings (about 20,000 pages). The complete civil dataset included 325 pleadings and the criminal dataset included 106 charging documents and 133 defendants.[85] Both datasets are open and available online for future research use.[86]

Aggregate longitudinal data on judicial opinions are drawn directly from Westlaw. I used keyword searches to identify CFAA opinions,[87] then extracted Westlaw's ordinary fields for date, court, and parties.

---

81 This project began in mid-2013. I selected 2012 as the last complete calendar year of court filings.

82 Specifically, I used the query: ("computer fraud") OR ("18 U.S.C. 1030") OR ("18 USC 1030") OR ("18 U.S.C. § 1030") OR ("18 USC § 1030") OR ("18:1030") OR ("fraud activity connected with computers") OR ("unauthorized access to a computer"). The latter two phrases are commonly used on criminal dockets involving a CFAA charge.

83 Many filings are imprecise about the specific CFAA cause of action. Where a filing was not explicit, I attempted to infer the relevant subsections by comparing the text of the filing to the text of the statute.

84 There is, to be sure, no neat taxonomy of party relationships and underlying conduct. I made an initial review of the documents to discern the most common fact patterns, then applied those categories in a second review.

85 Given the volume of civil pleadings, I did not filter out multiple filings from the same proceeding. For criminal charging documents, by contrast, I located the latest document for each proceeding.

86 The civil dataset is available at https://perma.cc/5JM2-XQG9 [hereinafter Civil Dataset]. The criminal dataset is available at https://perma.cc/U75B=XHZW [hereinafter Criminal Dataset].

87 Since I did not manually confirm that each opinion concerned a CFAA theory, I used a narrower search query than for pleadings: "computer fraud and abuse." The results under this methodology, to be sure, include false positives and negatives. Aggregate figures on judicial opinions should be considered as estimates, reflective of trends in federal litigation.

Finally, aggregate criminal longitudinal data were obtained from the Department of Justice's Bureau of Justice Statistics and the TRACfed Criminal Enforcement project at Syracuse University.[88]

### B. *What Is the Volume of Cybercrime Litigation?*

Understanding the longitudinal dynamics of cybercrime litigation is a critical first-order matter. First, the volume of litigation is informative as to whether cybercrime statutes merit scholarly, judicial, and policymaker attention. If cybercrime litigation were exceedingly rare, subsidiary issues would largely become moot.

A second reason for beginning with longitudinal analysis is to understand how litigation practices have changed. An abrupt uptick in civil or criminal litigation constitutes a warning sign, suggestive of strategic statutory abuse. And, in criminal cases, a tapering off is suggestive of limited investigatory resources or capabilities.

The following subsections examine longitudinal trends for civil and criminal cybercrime litigation, respectively.

#### 1. Civil Litigation

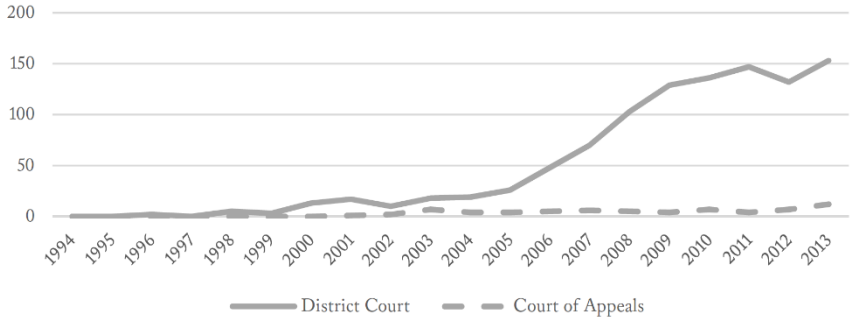
Civil cybercrime litigation has unambiguously exploded. Congress first enacted a private cause of action in 1994; for approximately the first decade of its existence, CFAA lay relatively fallow as a civil recourse. Then, between 2002 and 2012, district court opinions surged by over an order of magnitude.[89] The federal appellate courts have also been reviewing civil CFAA disputes at an increasing rate.[90]

88 *Criminal Enforcement*, TRACFED, http://tracfed.syr.edu/ [https://perma.cc/B2GQ-TS5Z] (last visited Apr. 15, 2016); *Federal Criminal Case Processing Statistics*, BUREAU JUST. STAT., http://www.bjs.gov/fjsrc/ [https://perma.cc/UE5K-AYSD] (last visited Apr. 15, 2016). The two datasets use slightly different means of classifying prosecutions: the DOJ Bureau of Justice Statistics dataset reports all defendants with a CFAA charge, while the TRACFed dataset reports only defendants where prosecutors noted a "lead" CFAA charge. Also, the DOJ BJS dataset only offers annual summary statistics, rather than individual case tracking. In order to associate prosecutions, convictions, and sentences in both datasets, I make the simplifying assumption that all three stages of litigation are contemporaneous.

89 *See infra* Figure 1.

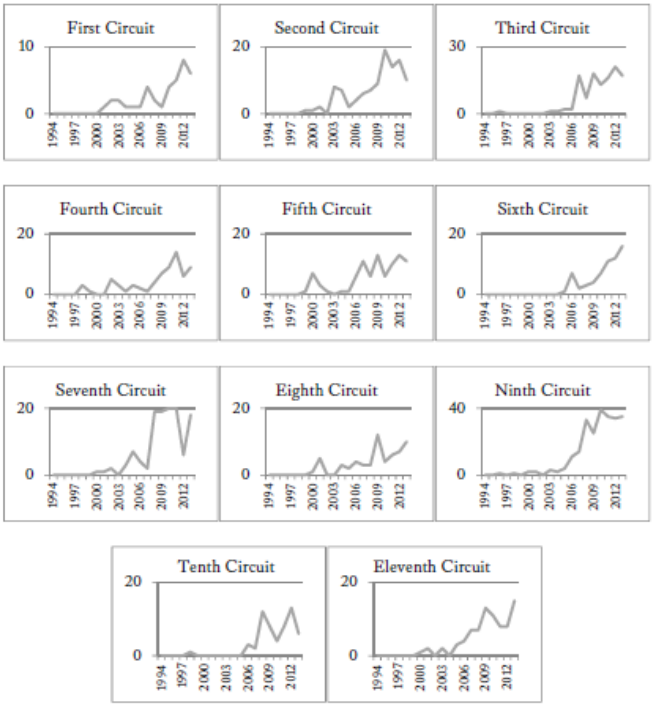
90 *See infra* Figure 1.

**Figure 1: Federal Court Opinions – Civil**




The uptick in civil CFAA litigation is not cabined by geography. Private cybercrime claims are on the rise in federal district courts and in every regional court of appeals, with the sole exception of the D.C. Circuit.[91]

**Figure 2: Federal District Court Opinions – Civil, by Circuit**




91 *See infra* Figure 2.

This sudden surge in civil cybercrime litigation suggests that cases are motivated by shifts in litigation strategy, rather than shifts in the underlying cybercrime problem.[92] Given that cybercrime has also rapidly increased, though, the evidence is hardly conclusive. Section D returns to the issue of civil cybercrime litigation with a detailed latitudinal analysis of pleadings.

The trend in civil cybercrime litigation is notably reminiscent of the federal courts' experience with the Racketeer Influenced and Corrupt Organizations (RICO) Act.[93] In the years immediately following its enactment, plaintiffs simply ignored the statute; during the first decade, there were just nine published opinions addressing civil claims under the Act.[94] In the following three years, however, courts published over 200 civil RICO opinions.[95] Strategic litigants recognized that conventional commercial disputes—with no nexus whatsoever to organized crime—could be transmuted into federal claims, with potential for recovering treble damages and attorneys' fees.[96]

### 2. Criminal Litigation

Since federal criminal cases are often resolved without substantial judicial intervention, opinions in criminal CFAA matters are rare. Nevertheless, as with civil litigation, trial and appellate courts are increasingly addressing criminal issues under CFAA, as demonstrated in Figure 3.

92 The growth in CFAA litigation is difficult to attribute to expanded statutory scope. Congress substantially expanded CFAA liability in 1996, nearly a decade before the litigation boom.

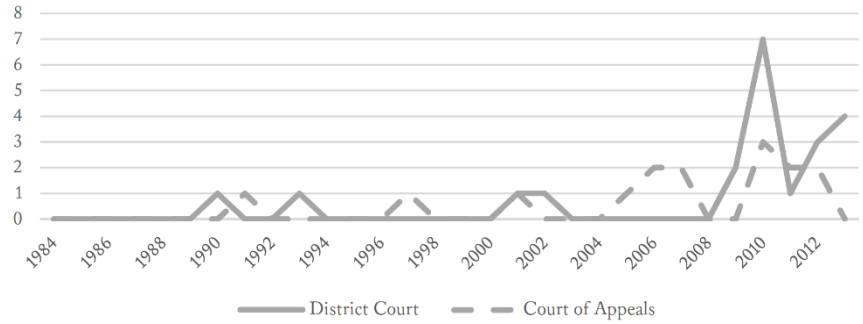
93 *See* Michael Goldsmith & Penrod W. Keith, *Civil RICO Abuse: The Allegations in Context*, 1986 B.Y.U. L. REV. 55, 62-66 (describing the rise in civil RICO litigation and providing data); *see also* Pamela H. Bucy, *Private Justice*, 76 S. CAL. L. REV. 1, 19-23 (2002) (providing more recent data on civil RICO litigation).

94 Goldsmith & Keith, *supra* note 93, at 63, 64 n.38.

95 *Id.* at 64 n.38.

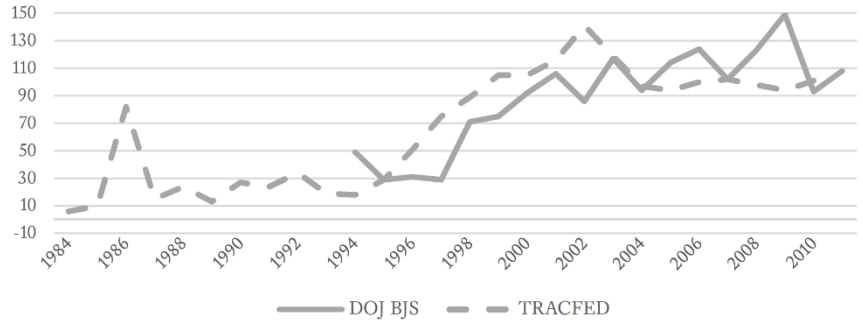
96 *Cf.* Nick Akerman, *CFAA Resembles RICO*, NAT'L L.J. (Aug. 29, 2005), http://www.nationallawjournal.com/id=900005435711/CFAA-Resembles-RICO [https://perma.cc/BQ5B-TSAJ] ("As with civil RICO, litigators can no longer overlook the CFAA. Whenever the evidence reflects that computers are involved in the perpetrating of a wrong, the CFAA should be reviewed for potential claims. The advantages are obvious. Like RICO, the CFAA is a federal statute and thus provides automatic federal jurisdiction, when the only available claims might be based on state law with no diversity jurisdiction. The CFAA also has certain advantages over using RICO (albeit without the treble damages and attorney fees mandated by RICO).").

**Figure 3: Federal Court Opinions – Criminal**




Longitudinal datasets on prosecutorial practice confirm a brisk upswing in cybercrime charging, between the late 1990s and early 2000s. Then, from the mid-2000s on, cybercrime charging leveled off.[97]

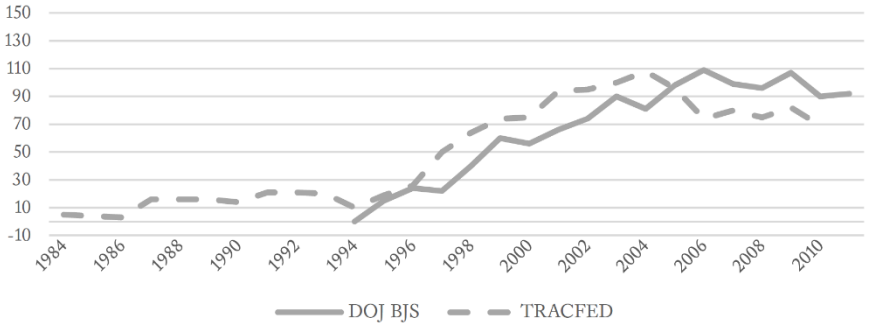
**Figure 4: Federal Criminal Prosecutions**




Data on convictions closely parallel the trends in data on charging—rapid growth from the 1990s to 2000s, then little change.[98]

97 *See infra* Figure 4.
98 *See infra* Figure 5.

**Figure 5: Federal Criminal Convictions**




The increase in criminal prosecutions and convictions, while significant, is not nearly as abrupt or substantial as the apparent increase in civil litigation. The data, therefore, provide little basis on which to assess the charging practices of federal prosecutors. Understanding the dynamics of criminal litigation instead requires exploration of further case detail, as provided in the following Parts.

Several additional observations warrant mention. First, the surge in criminal litigation predated the surge in civil litigation by about a decade. The differing sources of longitudinal data can explain a year or two of discrepancy—the civil data are drawn exclusively from opinions, not preliminary filings—but not so wide a span. This result suggests that prosecutors initially paved the way for broad applicability of cybercrime law, and civil litigants only later took advantage.[99]

Another significant result is that the volumes of cybercrime prosecutions and convictions have remained nearly constant for almost a decade. Given that the cybercrime problem has continued to grow, this trend suggests that prosecutors have reached the limit of their capacity for pursuing cybercrime cases. The longitudinal data do not lend insight, though, into whether that limit arises from fundamental challenges in investigating and prosecuting cybercrime, or from artificial personnel and resource constraints.

Finally, there is a persistent gap between cybercrime prosecutions and convictions. Roughly a quarter of filed charges do not result in a successful criminal justice outcome. According to Department of Justice data, a share of these cases can be attributed to acquittal, dismissal, or diversion.[100] The majority, though, appear to result from defendants who are either unidentifiable or outside the reach of the United States criminal justice system.

---

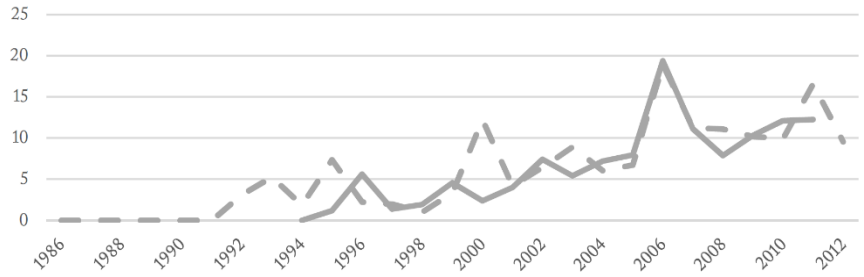
99 *Cf.* Goldsmith & Keith, *supra* note 93, at 62-64 (suggesting that criminal prosecutors took advantage of RICO's broad provisions slightly before civil plaintiffs).

100 *See infra* Figure 7 and accompanying text.

### C. *How Punitive Are Cybercrime Prosecutions?*

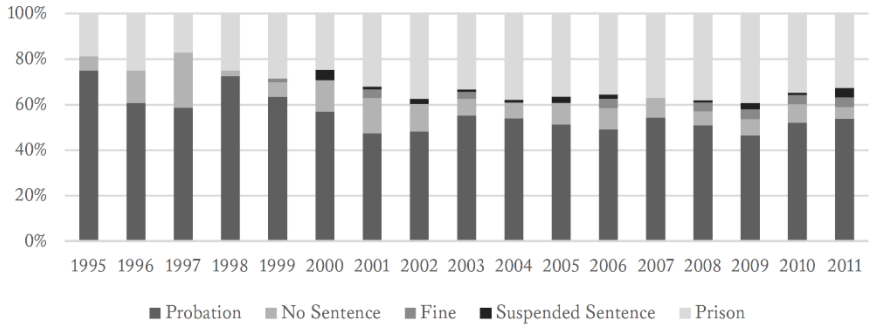
A cursory analysis would suggest that sentencing under cybercrime law has become radically more punitive. A defendant in a concluded prosecution for a federal cybercrime offense in the 2010s will, on average, receive a sentence of incarceration about four to five times longer than a defendant in the 1990s, as shown in Figure 6.

**Figure 6: Mean Prison Sentence in Closed Prosecutions (Months)**



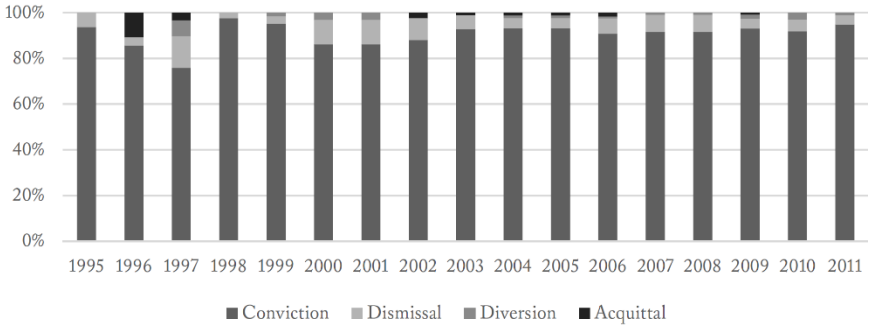

This account, however, proves to be far too simplistic. Most convicted cybercrime defendants do not receive a prison sentence; instead, most receive probation, a fine, a suspended sentence, or no sentence at all.[101] Furthermore, a small fraction of defendants avoid conviction altogether, obtaining dismissal, pretrial diversion, or acquittal.[102]

**Figure 7: Sentencing for Convicted Defendants (DOJ BJS)**




101 *See infra* Figure 8.
102 *See infra* Figure 7.

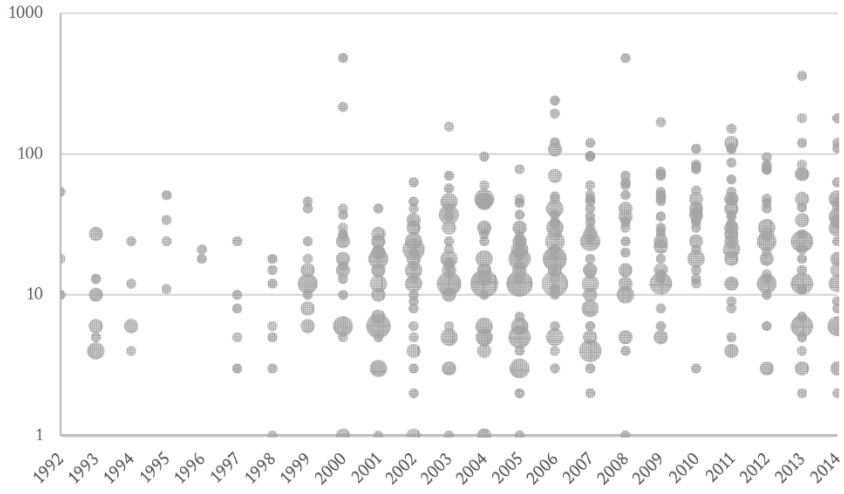
**Figure 8: Outcomes in Closed Prosecutions (DOJ BJS)**




From the mid-1990s to the mid-2000s, the ratio of convicted defendants who received a prison sentence roughly doubled, reaching two in five.[103] But since then, the ratio has remained roughly constant.[104]

So, if the median convicted defendant continues to receive no prison sentence, and if the proportion of convicted defendants who receive a prison sentence has remained steady, why are average cybercrime prison sentences continuing to increase? One possible explanation is that federal prosecutors have been successful at targeting major cybercriminals, such that a small number of outliers are driving up the average.

**Figure 9: Prison Sentence, If Any (TRACFED, Months)**




103 *See supra* Figure 8.
104 *See supra* Figure 8.

The data tell a different story. Since the mid-2000s, prosecutors have occasionally secured convictions against serious offenders. But there is not a burgeoning number of outlier sentences; cybercrime sentencing has remained clustered.[105] Rather, the entire set of cybercrime prison sentences appears to have been indiscriminately shifted upwards over the past decade, roughly tripling the average period of incarceration.[106]

These observations about sentencing practices cut in opposite directions. On the one hand, the data imply that federal prosecutors are exercising meaningful discretion in cybercrime cases. Scholars and practitioners have emphasized how broad felony offenses and elevated sentencing guidelines facilitate imposing incarceration.[107] But the data reflect that prosecutors generally remain willing to accept minimal, nonprison punishments.

On the other hand, cybercrime prosecutorial discretion is increasingly bimodal. Where prosecutors do seek and obtain a prison sentence, the period of incarceration has greatly increased. In the 1990s, a cybercrime prison term of less than one year was customary; now, it is a rarity.

The most surprising result is just how few defendants are sentenced to prison. Incarceration serves as a proxy variable for offense severity; where prosecutors seek and judges impose a nonprison sentence, the underlying computer abuse is likely minimal. This observation suggests that most federal prosecutions arise from minor misconduct, not high-profile, large-scale, or sophisticated hacking.

---

105 *See supra* Figure 9.

106 *See supra* Figure 9.

107 One manner in which a minor CFAA offense can be converted into a felony is by incorporating a violation of state cybercrime law. 18 U.S.C. § 1030(c)(2)(B)(ii) (2012); *see* Orin Kerr, *Obama's Proposed Changes to the Computer Hacking Statute*, VOLOKH CONSPIRACY (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/ [https://perma.cc/2465-PTZ2] (explaining how state cybercrime statutes often overlap with CFAA); Zoe Lofgren & Ron Wyden, *Introducing Aaron's Law, A Desperately Needed Reform of the Computer Fraud and Abuse Act*, WIRED (June 20, 2013), http://www.wired.com/2013/06/aarons-law-is-finally-here/ [https://perma.cc /C8AL-UC26] (noting that "a prosecutor can seek to inflate potential sentences by stacking new charges atop violations of state laws"). Another avenue for converting a minor CFAA offense into a felony is to charge the expansive fraud provision, 18 U.S.C. § 1030(a)(4), or one of the damage provisions, 18 U.S.C. § 1030(a)(5)(A)-(C). For an explanation about how sentencing enhancement factors can easily apply in cybercrime cases, see Hanni Fakhoury, *How the Sentencing Guidelines Work Against Defendants in CFAA Cases*, ELECTRONIC FRONTIER FOUND.: DEEPLINKS BLOG (Apr. 9, 2013), https://www.eff.org/deeplinks/2013/03/41-months-weev-understanding-how-sentencing-guidelines-work-cfaa-cases-0 [https://perma.cc/U3PC-R9YF] (critiquing the use of an enhancement factor targeted specifically at CFAA crimes).

### D. *What Fact Patterns Are Litigated Under Cybercrime Law?*

The longitudinal data are probative of how civil plaintiffs and criminal prosecutors have invoked cybercrime law, but they are certainly not conclusive. In this Section, I turn to a detailed latitudinal analysis, using a new, comprehensive dataset of 2012 federal cybercrime pleadings.

With this novel dataset, it is possible to definitively answer additonal foundational questions about the function of federal cybercrime law: Who invokes CFAA and under what circumstances? The following subsections examine these questions, first for civil litigation, then for criminal prosecutions.

#### 1. Civil Litigation

##### a. *Party Relationships*

Civil defendants appear nothing like the outsider rogues that initially captivated Congress and state legislatures, as demonstrated by Table 1.

**Table 1: Party Relationships in Civil CFAA Filings**

| Relationship Between Plaintiff(s) and Defendant(s) | Number of Filings |
|---|---|
| Employee, Consultant, or Contractor | 162 (50%) |
| Competitor | 97 (30%) |
| Technology Service Provider | 42 (13%) |
| Derivative Business | 29 (9%) |
| Business Partner | 24 (7%) |
| Doe(s) | 22 (7%) |
| No Substantial Relationship | 16 (5%) |
| Customer or User | 8 (2%) |
| Employer | 6 (2%) |

The overwhelming majority of private cybercrime claims arise in business disputes (238, 73%),[108] and of those, most follow from previous employment (168, 52%).[109] Just a small minority of claims (38, 12%) are filed against strangers.[110]

An analysis of party relationship coincidence confirms that cybercrime law most often intermediates routine commercial quarrels. There is scant overlap between categories associated with business and those associated with hacker stereotypes; these are not cases in which former employees or competitors have aligned with unrelated, serial computer abusers. Rather, civil CFAA litigation involves one-off commercial disputes that happen to involve information technology.

**Table 2: Party Relationship Coincidence in Civil CFAA Filings**

| | Employee | Competitor | Technology Service | Derivative Business | Business Partner | Doe(s) | No Relation-ship | Customer | Employer |
|---|---|---|---|---|---|---|---|---|---|
| Employee | | 76 (47%) | 0 (0 %) | 0 (0 %) | 9 (6%) | 0 (0 %) | 0 (0 %) | 0 (0 %) | 0 (0 %) |
| Competitor | 76 (78%) | | 0 (0 %) | 6 (6%) | 4 (4%) | 0 (0 %) | 0 (0 %) | 1 (1%) | 1 (1%) |
| Technology Service | 0 (0 %) | 0 (0 %) | | 0 (0 %) | 0 (0 %) | 0 (0 %) | 0 (0 %) | 0 (0 %) | 0 (0 %) |
| Derivative Business | 0 (0 %) | 6 (21%) | 0 (0 %) | | 0 (0 %) | 0 (0 %) | 0 (0 %) | 0 (0 %) | 0 (0 %) |
| Business Partner | 9 (38%) | 4 (17%) | 0 (0 %) | 0 (0 %) | | 0 (0 %) | 0 (0 %) | 0 (0 %) | 0 (0 %) |
| Doe(s) | 0 (0 %) | 0 (0 %) | 0 (0 %) | 0 (0 %) | 0 (0 %) | | 0 (0 %) | 0 (0 %) | 0 (0 %) |
| No Relationship | 0 (0 %) | 0 (0 %) | 0 (0 %) | 0 (0 %) | 0 (0 %) | 0 (0 %) | | 0 (0 %) | 0 (0 %) |
| Customer | 0 (0 %) | 1 (12%) | 0 (0 %) | 0 (0 %) | 0 (0 %) | 0 (0 %) | 0 (0 %) | | 0 (0 %) |
| Employer | 0 (0 %) | 1 (17%) | 0 (0 %) | 0 (0 %) | 0 (0 %) | 0 (0 %) | 0 (0 %) | 0 (0 %) | |

The data on party relationships, seen in Table 2, reveal a notable trend in litigation: a cybercrime claim against a competitor is often accompanied by a cybercrime claim against a former employee (76, 78%).[111] These cases reflect departed staff who have either established their own firms or joined preexisting competitors. Cybercrime law is merely a novel federal twist in these cases, which have historically been adjudicated under contract, trade secret, or agency law.

### b. *Underlying Conduct*

The overwhelming majority of civil cybercrime claims also look nothing like "hacking," even construed broadly, as shown in Table 3.

---

108 Civil Dataset, *supra* note 86 ((Business Dispute) / (All Civil Filings)). In describing the latitudinal data throughout this Article, I use the following logic notation to reflect operations on the civil and criminal datasets: (1) "$\wedge$" for "and," (2) "$\vee$" for "or," and (3) "$\neg$" for "not." The symbol "/" represents division of the sum of records matching the numerator by the sum of records matching the denominator. The symbol "–" represents the difference between the sum of records matching the minuend and the sum of records matching the subtrahend.

109 *See id.* ((Business Dispute $\wedge$ Employee, Consultant, Contractor, or Distributor) / (Business Dispute)).

110 *See id.* ((Unrelated Parties) / (All Civil Filings)).

111 *See id.* ((Competitor $\wedge$ Employee, Consultant, Contractor, or Distributor) / (Competitor)).

**Table 3: Conduct Alleged in Civil CFAA Filings**

| Conduct | Number of Filings |
|---|---|
| Misappropriating Information | 170 (52%) |
| Editing or Deleting Information | 71 (22%) |
| Invasion of Privacy | 41 (13%) |
| Accessing Another Person's Account | 40 (12%) |
| Financial Misfeasance | 26 (8%) |
| Hijacking Another Person's Account | 26 (8%) |
| Impersonation | 20 (6%) |
| Misappropriating a Computer System | 18 (6%) |
| Mobile Phone Unlocking | 16 (5%) |
| Software Disruption of a Computer System | 14 (4%) |
| Credential Sharing | 11 (3%) |
| Harassment | 11 (3%) |
| Unrelated Website | 9 (3%) |
| Copyright Trolling | 8 (2%) |
| Spam Calls or Email | 7 (2%) |
| Malware | 6 (2%) |
| Reverse Engineering | 6 (2%) |
| Physical Disruption of a Computer System | 5 (2%) |
| Automated Website Interaction | 5 (2%) |
| Modifications to Enterprise Software | 5 (2%) |

Most private claims relate to information misappropriation (170, 52%),[112] or modification or deletion (71, 22%).[113] The categories substantially overlap, and together represent a majority of claims (182, 56%).[114] These findings indicate that civil cybercrime works as a quasi-intellectual property regime, far less concerned with the function and integrity of computer systems than with their information contents.

Only a minority of claims could be reasonably characterized as involving the circumvention of a technical protection measure (99, 30%).[115] Furthermore, even within these cases that involve technical circumvention, the most common avenues for unauthorized access are password theft (53, 54%),[116] mobile phone

112 *See id.* ((Misappropriating Information) / (All Civil Filings)).

113 *See id.* ((Editing or Deleting Information) / (All Civil Filings)).

114 *See id.* ((Misappropriating Information ∨ Editing or Deleting Information) / (All Civil Filings).

115 *See id.* ((Circumvention of a Technical Protection) / (All Civil Filings)).

116 *See id.* ((Circumvention of a Technical Protection ∧ Accessing or Hijacking Another Person's Account – Circumvention of a Technical Protection ∧ Accessing or Hijacking Another Person's Account with a Technical Circumvention Except Credentials) / (Circumvention of a Technical Protection)).

unlocking (16, 16%),[117] and password sharing (11, 11%).[118] Civil cybercrime cases, in short, do not arise from technically sophisticated "breaking and entering."[119]

There is remarkably little commonality in the long tail of fact patterns. Claims present a hodgepodge of theories favoring liability, ranging from online harassment (11, 3%)[120] to hosting an unrelated website (9, 3%)[121] to scraping online material (5, 2%).[122] Cybercrime use in copyright trolling (8, 2%)[123] and bulk mobile phone unlocking cases (16, 5%)[124] suggests the law has been opportunistically seized upon for non-adversarial litigation.[125]

### 2. Criminal Litigation

#### a. *Victim–Defendant Relationships*

Most criminal charges, like most civil claims, arise from a preexisting relationship, as shown in Table 4.

**Table 4: Victim-Defendant Relationships in CFAA Prosecutions[126]**

| Relationship Between Defendant and Victim | Number of Defendants |
|---|---|
| Employee, Consultant, or Contractor | 64 (48%) |
| No Substantial Relationship | 41 (30%) |
| Colleague | 9 (7%) |
| Social or Familial Relation | 5 (4%) |
| Technology Service | 5 (4%) |
| Business Partner | 4 (3%) |
| Customer or User | 3 (2%) |
| Doe(s) | 3 (2%) |

117 *See id.* ((Circumvention of a Technical Protection ∧ Mobile Phone Unlocking) / (Circumvention of a Technical Protection)).

118 *See id.* ((Circumvention of a Technical Protection ∧ Credential Sharing) / (Circumvention of a Technical Protection)).

119 *Contra* H.R. REP. NO. 98-894, at 20 (1984), *as reprinted in* 1984 U.S.C.C.A.N. 3689, 3706 ("The conduct prohibited [in CFAA] is analogous to that of 'breaking and entering' rather than using a computer (similar to the use of a gun) in committing the offense.").

120 *See* Civil Dataset, *supra* note 86 ((Harassment) / (All Civil Filings)).

121 *See id.* ((Unrelated Website) / (All Civil Filings)).

122 *See id.* ((Automated Website Interaction) / (All Civil Filings)).

123 *See id.* ((Copyright Trolling) / (All Civil Filings)).

124 *See id.* ((Mobile Phone Unlocking) / (All Civil Filings)).

125 *See generally* Civil Dataset, *supra* note 86.

126 Criminal Dataset, *supra* note 86.

And, like with civil claims, the majority of criminal charges relate to an employment or commercial dispute (76, 57%).[127]

These findings squarely deflate the myth that most cybercrime defendants align with hacker archetypes (i.e., repeat offenders motivated by sport, profit, or national pride). Instead, most criminal cases arise from one-time misconduct, in which an underlying dispute migrates from the real world to the Internet.

The criminal prosecution data reveal, however, one notable departure from civil practice: although still a minority, cases in which there is no relationship between the defendant and victim, or where the defendant is unidentified, occur about three times as often in criminal prosecutions as in civil suits (44, 33%).[128]

b. *Underlying Conduct*

Criminal cases, much like civil cases, tend not to arise from sophisticated hacking, as seen in Table 5.

**Table 5: Conduct Alleged in Criminal CFAA Filings** [129]

| Conduct | Number of Defendants |
|---|---|
| Misappropriating Information | 82 (62%) |
| Accessing Another Person's Account | 47 (35%) |
| Financial Misfeasance | 32 (24%) |
| Editing or Deleting Information | 18 (14%) |
| Malware | 17 (13%) |
| Software Disruption of a Computer System | 14 (11%) |
| Unspecified Breaking In | 13 (10%) |
| Hijacking Another Person's Account | 11 (8%) |

About half of prosecutions do not involve technical circumvention of an access control (65, 49%).[130] And, among those cases that do involve a circumvention of a technological protection, many of the fact patterns do not reflect technical sophistication but rather password theft (32, 47%).[131]

127 *See id.* ((Employee, Consultant, Contractor, or Distributor ∨ Business Partner ∨ Colleague ∨ Customer or User ∨ Competitor) / (All Criminal Defendants)).

128 *See id.* ((Doe(s) ∨ No Substantial Relationship) / (All Criminal Defendants)).

129 Criminal Dataset, *supra* note 86.

130 *See id.* ((All Criminal Defendants – Circumvention of a Technical Protection) / (All Criminal Defendants)).

131 *See id.* ((Circumvention of a Technical Protection – Circumvention of a Technical Protection Except Credentials) / (Circumvention of a Technical Protection)).

These results belie the narrative that federal prosecutors generally reserve cybercrime charges for the worst offenders, namely serial and sophisticated computer hackers.[132] In fact, prosecutors routinely file cybercrime charges for minor misconduct, especially when a current or former employee misappropriates information (51, 39%).[133]

One substantial point of divergence between civil and criminal litigation is the extent to which government computer systems are involved. Nearly all the civil cases in the dataset related to computer systems owned by private individuals or businesses.[134] In the criminal cases, by contrast, roughly a quarter of charges related to a government computer system (38, 29%).[135] Most of the defendants in these cases were current or former government employees who had technically valid credentials for a system, but misused the system (21, 55%).[136] Remarkably, among those cases where a government employee repurposed their access to a workplace computer system, the most common class of defendant consisted of law enforcement personnel (12, 57%).[137]

### E. *Is Cybercrime Law Redundant?*

Cybercrime law is not monolithic. Federal and state legislatures have enacted a diverse array of offenses and have drafted those offenses with a wide range of textual variations.[138] The current CFAA, for instance, contains (depending on how one counts) up to fourteen different statutory offenses.[139]

The structure of cybercrime law generates the potential for two different types of redundancy. First, a cybercrime offense might be internally redundant,

---

132 *But cf.* U.S. Dep't of Justice, *U.S. Attorney for the Western District of Washington Jenny A. Durkan Testifies Before the Senate Judiciary Subcommittee on Crime and Terrorism*, JUST. NEWS (May 8, 2013), http://www.justice.gov/opa/speech/us-attorney-western-district-washington-jenny-durkan-testifies-senate-judiciary [https://perma.cc/25MF-TZCB] (highlighting federal prosecutorial successes in cybercrime cases despite the "increases in the skills of threat actors and the complexity of their organizations").

133 *See* Criminal Dataset, *supra* note 86 ((Employee, Consultant, Contractor, or Distributor ∧ Misappropriating Information) / (All Criminal Defendants)).

134 Civil Dataset, *supra* note 86.

135 *See* Criminal Dataset, *supra* note 86 ((Government Computer System) / (All Criminal Defendants)).

136 *See id.* ((Government Computer System ∧ Misappropriating Information ∧ ¬ (Circumvention of a Technical Protection)) / (Government Computer System)).

137 *See id.* ((Government Computer System ∧ Misappropriating Information ∧ ¬ (Circumvention of a Technical Protection) ∧ Law Enforcement Personnel) / (Government Computer System ∧ Misappropriating Information ∧ ¬ (Circumvention of a Technical Protection)).

138 *See, e.g.*, Facebook, Inc. v. Power Ventures, Inc., No. C 08-05780, 2010 WL 3291750, at *9-12 (N.D. Cal. July 20, 2010) (holding that "permission" under the California cybercrime statute has a different meaning than "authorization" under the federal statute); *see also* United States v. Auernheimer, 748 F.3d 525, 534 n.5 (3d Cir. 2014) (suggesting that "without authorization, or in excess of authorization" under the New Jersey statute has a different meaning than "without authorization or exceeds authorized access" under the federal statute).

139 18 U.S.C. § 1030 (2012).

overlapping with other cybercrime offenses within the same statutory scheme. Second, a cybercrime offense might be externally redundant, overlapping with noncybercrime civil claims or criminal charges.

This Section examines the extent to which cybercrime is both internally and externally redundant. It begins with civil claims before turning to criminal charges.

### 1. Civil Litigation

#### a. *Internal Redundancy*

Many pleadings invoke cybercrime law only generally and fail to identify particular statutory claims (123, 38%).[140] These plaintiffs treat CFAA as a single type of liability, blurring the various offenses. One plausible interpretation is that attorneys simply fail to understand the federal statute's structure. Alternatively, practitioners may view cybercrime law as so internally duplicative that particularized claiming is unnecessary. A more cynical view is that many courts tolerate this vague pleading practice, thus providing little incentive for plaintiffs to furnish detail.

CFAA's structure provides a limited natural experiment for evaluating whether attorneys are confused by the statutory scheme or are pleading strategically. In civil practice, statutory claims for unintentional damage to a computer are *markedly easier* to prove than claims for reckless damage to a computer, and both claims provide *identical* remedies.[141] Nevertheless, a nontrivial share of filings (55, 27%) include a reckless damage claim.[142] Most of these pleadings also include an unintentional damage claim (42, 76%), such that the reckless damage claim is merely duplicative.[143] But a meaningful share of reckless damage pleadings do not include an unintentional damage claim (13, 24%),[144] a result that can only be explained by attorney confusion. So, this much is certain: a fair number of practitioners are befuddled by cybercrime law.

Within the subset of filings that are more precise about statutory claims (202, 62%),[145] a substantial majority reference multiple provisions (142, 70%), as shown in Figure 10.

---

140 *See* Criminal Dataset, *supra* note 86 ((Unspecified Claims / All Civil Claims)).

141 CFAA plaintiffs usually must show $5000 in "loss" under 18 U.S.C. § 1030 (g) and (c)(4)(A)(i)(I). As a result, in civil cases, the reckless "damage" offense in (a)(5)(B) is ordinarily strictly harder to prove than the "damage and loss" offense in (a)(5)(C).

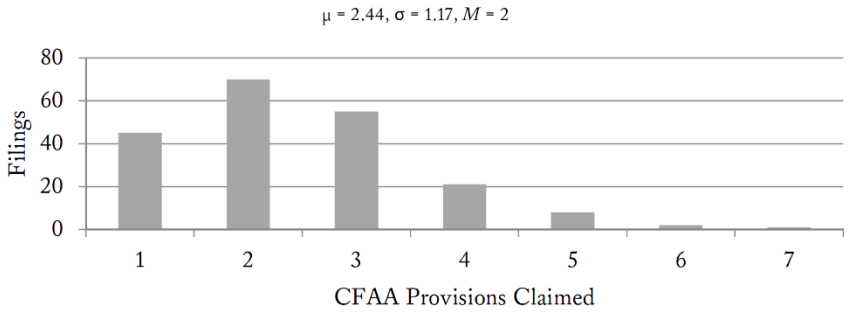
142 *See infra* Table 6 ((1030(a)(5)(B) / (All Civil Claims)).

143 *See infra* Table 7 ((1030(a)(5)(B) ∧ 1030(a)(5)(C) / (1030(a)(5)(B)).

144 *See id.* ((1030(a)(5)(B) ∧ ¬ 1030(a)(5)(C)) / (1030(a)(5)(B).

145 *See* Civil Dataset, *supra* note 86 ((¬ Unspecified CFAA Claims) / (All Civil Claims)).

**Figure 10: Number of Specific CFAA Provisions in Civil Filings**




These findings strongly suggest that CFAA's various provisions greatly overlap. Most plaintiffs who plead with specificity believe their fact pattern could be styled as a violation of more than one statutory offense.

Pleadings most commonly cite CFAA's taking information and fraud offenses, as would be expected given their broad judicial constructions.[146] The unintentional damage and loss provision is also widely invoked, suggesting plaintiffs recognize the broad and overlapping interpretations of "damage" and "loss" that some courts have adopted.

**Table 6: Frequency of Specific CFAA Provisions in Civil Filings**

| Civil Claim | Statutory Provision | Filings with a Claim |
|---|---|---|
| Taking Information | (a)(2)(C) | 136 (67%) |
| Fraud | (a)(4) | 111 (55%) |
| Damage and Loss | (a)(5)(C) | 96 (48%) |
| Reckless Damage | (a)(5)(B) | 55 (27%) |
| Intentional Damage | (a)(5)(A) | 48 (24%) |
| Trafficking in Passwords | (a)(6)(A) | 23 (11%) |
| Unspecified Damage | (a)(5) | 18 (9%) |
| Taking Financial Information | (a)(2)(A) | 4 (2%) |
| Extortion | (a)(7) | 2 (1%) |

146 As an aside, CFAA incorporates an unusual cause of action for password trafficking, and plaintiffs have found a way to put even this to use. Most of these cases arise from mobile phone unlocking (13, 57%) or voluntary password sharing (6, 26%). *Id.* ((1030(a)(6)(A) ∧ Mobile Phone Unlocking) / (1030(a)(6)(A))); *id.* ((1030(a)(6)(A) ∧ Credential Sharing) / (1030(a)(6)(A))).

Claiming coincidence under CFAA lends further credence to the view that the statute is internally redundant, as seen in Table 7. There are extraordinarily high rates of coclaiming across CFAA's broadest provisions.

**Table 7: Coincidence of Specific CFAA Provisions in Civil Filings (18 U.S.C. § 1030(a) (2012))**

| | (2)(C) | (4) | (5)(C) | (5)(B) | (5)(A) | (6)(A) | (5) | (2)(A) | (7) |
|---|---|---|---|---|---|---|---|---|---|
| (2)(C) | | 72 (53%) | 59 (43%) | 39 (29%) | 26 (19%) | 7 (5%) | 16 (12%) | 3 (2%) | 1 (1%) |
| (4) | 72 (65%) | | 51 (46%) | 26 (23%) | 22 (20%) | 20 (18%) | 13 (12%) | 3 (3%) | 1 (1%) |
| (5)(C) | 59 (61%) | 51 (53%) | | 42 (44%) | 32 (33%) | 15 (16%) | | 1 (1%) | 2 (2%) |
| (5)(B) | 39 (71%) | 26 (47%) | 42 (76%) | | 31 (56%) | 2 (4%) | | 1 (2%) | 1 (2%) |
| (5)(A) | 26 (54%) | 22 (46%) | 32 (67%) | 31 (65%) | | 2 (4%) | | 1 (2%) | 1 (2%) |
| (6)(A) | 7 (30%) | 20 (87%) | 15 (65%) | 2 (9%) | 2 (9%) | | 1 (4%) | 1 (4%) | 0 (0%) |
| (5) | 16 (89%) | 13 (72%) | | | | 1 (6%) | | 0 (0%) | 0 (0%) |
| (2)(A) | 3 (75%) | 3 (75%) | 1 (25%) | 1 (25%) | 1 (25%) | 1 (25%) | 0 (0%) | | 0 (0%) |
| (7) | 1 (50%) | 1 (50%) | 2 (100%) | 1 (50%) | 1 (50%) | 0 (0%) | 0 (0%) | 0 (0%) | |

Several areas of claiming coincidence warrant note. First, the taking information and fraud offenses frequently coincide,[147] likely because courts have watered down key elements of CFAA's fraud offense.

Second, the various "damage" claims commonly are coupled with a taking information or a fraud claim.[148] These filings reflect jurisprudence that broadly interprets "damage" to encompass mundane copying or modifying data.[149]

Third, the overwhelming majority of password trafficking claims are paired with fraud claims (20, 87%).[150] Much, but not all, of the overlap arises from copy-and-paste complaints in mobile phone unlocking disputes (13, 65%).[151] The theory of these cases seems to be, in part, that use of another person's password is inherently fraudulent. If viable, this theory renders the password trafficking offense largely redundant as against the fraud offense.

b. *External Redundancy*

Private cybercrime claims are usually bundled with a passel of other causes of action, as shown in Figure 11.

147 *See supra* Table 7.

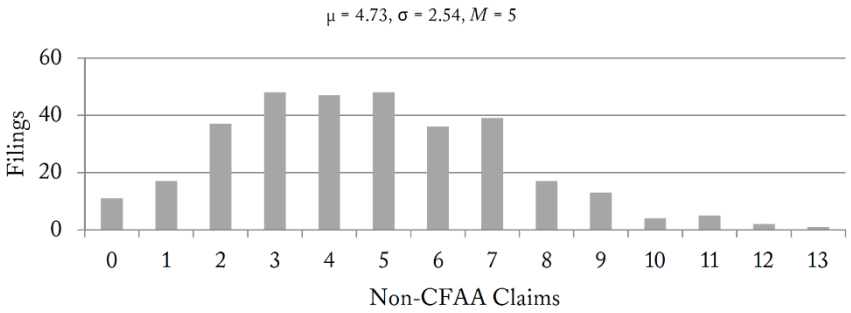
148 *See supra* Table 7.

149 Civil Dataset, *supra* note 86. Measured slightly differently, within the subset of filings that included any (a)(5) claim (137, 68%), a slight majority involved information misappropriation, modification, or deletion (69, 50%).

150 *See id.* ((1030(a)(6)(A) ∧ 1030(a)(4)) / (1030(a)(6)(A))).

151 *See id.* ((1030(a)(6)(A) ∧ 1030(a)(4) ∧ Mobile Phone Unlocking) / (1030(a)(6)(A) ∧ 1030(a)(4))).

**Figure 11: Number of Non-CFAA Claims in Civil Filings**




This high rate of coclaiming buttresses the theory that, in civil litigation, CFAA and conventional bases of liability are usually redundant. Plaintiffs evidently believe they have a broad range of colorable theories for recovery.

As demonstrated in Table 8, the most frequent cybercrime coclaims are broad, state common law causes of action.

**Table 8: Frequency of Non-CFAA Claims in Civil Filings**

| Non-CFAA Claim | Source of Law | Filings with a Claim |
|---|---|---|
| Contract | State | 161 (50%) |
| Unfair Business Practices | State | 138 (42%) |
| Trade Secret | State | 131 (40%) |
| Conversion | State | 126 (39%) |
| Tortious Interference | State | 125 (38%) |
| Fiduciary Duty | State | 115 (35%) |
| Unjust Enrichment | State | 89 (27%) |
| Civil Conspiracy | State | 86 (26%) |
| Stored Communications Act | Federal | 67 (21%) |
| Computer Trespass | State | 63 (19%) |
| Fraud | State | 62 (19%) |
| Trademark | Federal | 56 (17%) |
| Wiretap Act | Federal | 54 (16%) |
| Trespass to Chattels | State | 44 (14%) |
| Copyright | Federal | 36 (11%) |
| Privacy Tort | State | 27 (8%) |
| Defamation | State | 21 (6%) |
| Negligence | State | 17 (5%) |
| Wiretap Statute | State | 15 (5%) |

This result is consistent with the theory that courts have adapted conventional tort and property claims to technology, making dedicated, computer-specific causes of action less necessary.

The leading civil coclaims also reinforce the conclusion that civil cybercrime mediates commercial grievances, not sophisticated computer intrusions. Claims grounded in contract, unfair business practices, and fiduciary duty appear in the overwhelming majority of civil cybercrime cases[152]—and necessarily arise from business and employment relationships.[153]

Comparing claiming coincidence across CFAA and non-CFAA causes of action reveals that this external redundancy is not unique to specific cybercrime offenses, as demonstrated by Table 9.

**Table 9: Coincidence Between the Most Common CFAA and Non-CFAA Claims in Civil Filings**

| | Contract | Unfair Business Practices | Trade Secret | Conversion | Tortious Interference |
|---|---|---|---|---|---|
| Taking Information | 62 (46%) | 58 (43%) | 69 (51%) | 42 (31%) | 46 (34%) |
| Fraud | 61 (55%) | 58 (52%) | 52 (47%) | 43 (39%) | 54 (49%) |
| Unintentional Damage and Loss | 45 (47%) | 50 (52%) | 33 (34%) | 36 (38%) | 42 (44%) |
| Reckless Damage | 25 (45%) | 24 (44%) | 23 (42%) | 17 (31%) | 22 (40%) |
| Intentional Damage | 24 (50%) | 20 (42%) | 15 (31%) | 16 (33%) | 22 (46%) |

Litigants invoke the same state common law causes of action, regardless of whether their cybercrime claim arises from a taking information, fraud, or damage theory.[154]

A final observation is how many cases are in federal court solely based on a CFAA claim. A slight majority of filings do not include any federal claim other than CFAA (166, 51%).[155] While plaintiffs in some of these cases could assuredly invoke diversity jurisdiction, the high proportion strongly implies that many CFAA plaintiffs rely upon the statute as a hook for federal subject matter jurisdiction, and many of these disputes would end up in state court but for CFAA.[156]

152 *See infra* Table 9.

153 Claims for trade secret theft, conversion, and tortious interference suggest an underlying commercial dispute, but are not so conclusive. A hacker breaching a system and obtaining information could be liable under trade secret or conversion theories for misappropriating confidential business information. An intentional disruption of a commercial computer system could be actionable as tortious interference since the aim is interfering with ongoing and prospective business operations.

154 Civil Dataset, *supra* note 86.

155 *Id.* ((¬Other Federal Claims) / (All Civil Claims)).

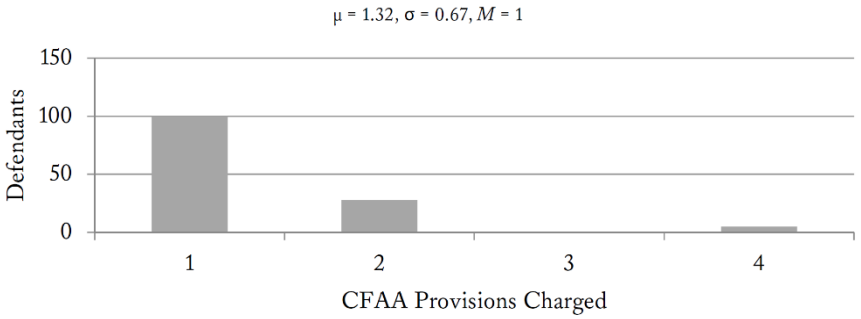
156 Some courts have recognized CFAA usage as a strategic mechanism for federal subject matter jurisdiction and have declined to exercise supplemental jurisdiction over associated state law

### 2. Criminal Prosecutions

a. *Internal Redundancy*

At first glance, CFAA's internal redundancy appears significantly less pronounced in criminal prosecutions than in civil cases.[157] Prosecutors uniformly reference specific provisions of CFAA, and the overwhelming majority of defendants are accused of violating just one of CFAA's statutory offenses (100, 75%), as illustrated by Figure 12.

**Figure 12: Number of Specific CFAA Provisions in Criminal Prosecutions**




Prosecutors thus appear to be exercising restraint in cybercrime cases. Even in fact patterns where judicial constructions of CFAA would allow for charging under multiple statutory provisions, prosecutors rarely invoke more than one type of offense. The result also suggests that prosecutors make a meaningful effort to distinguish between various cybercrime offenses.

There is, though, a cynical alternative reading of this result. Prosecutors can already easily obtain a maximum five-year sentence under CFAA's broad taking-information provision.[158] An additional conviction for fraud or damage would likely carry the same maximum sentence and would be subject to the

claims. *See, e.g.*, Landmark Credit Union v. Doberstein, 746 F. Supp. 2d 990, 993-94 (E.D. Wis. 2010) (stating that plaintiff's claim "borders on the frivolous" and is "an attempt to artificially create federal jurisdiction"); Contemporary Serv. Corp. v. Hartman, No. 08-02967, 2008 WL 3049891, at *3-4 (C.D. Cal. Aug. 4, 2008) (discussing the differences in what plaintiffs must prove for CFAA claims in comparison to state law claims).

157 This criminal charging analysis provides equivalent treatment to principal, attempt, accomplice, and conspiracy charges under each CFAA provision, since the purpose of the analysis is to compare the scope and invocation of CFAA's various provisions.

158 *See* 18 U.S.C. § 1030(c)(2)(B) (2012) (setting a five-year maximum sentence for CFAA's taking information offenses, so long as prosecutors can establish any of several straightforward enhancements).

same sentencing guidelines. And, since the charges arise from the same conduct, sentences would likely run concurrently.[159] Additionally, if the underlying theories for various offenses overlap too extensively, courts might invalidate the charges on Double Jeopardy Clause grounds.[160] Accordingly, if prosecutors make charging determinations to obtain the greatest possible punishment, they would have little incentive to charge under multiple CFAA provisions. Prosecutors would instead charge under just the offense that is both the easiest to prove and most punitive.[161]

Results on charging coincidence (Table 10) do not, unfortunately, aid in selecting between these competing hypotheses of prosecutorial behavior.

**Table 10: Coincidence of Specific CFAA Provisions in Criminal Prosecutions (18 U.S.C. § 1030(a) (2012))**

| | (2)(C) | (5)(A) | (4) | (2)(B) | (5)(B) | (7) | (6)(A) | (2)(A) | (3) |
|---|---|---|---|---|---|---|---|---|---|
| **(2)(C)** | | 15 (24%) | 5 (8%) | 3 (5%) | 5 (8%) | 4 (6%) | 4 (6%) | 0 (0%) | 0 (0%) |
| **(5)(A)** | 15 (31%) | | 7 (14%) | 0 (0%) | 4 (8%) | 2 (4%) | 4 (8%) | 0 (0%) | 0 (0%) |
| **(4)** | 5 (21%) | 7 (29%) | | 0 (0%) | 0 (0%) | 1 (4%) | 1 (4%) | 0 (0%) | 0 (0%) |
| **(2)(B)** | 3 (20%) | 0 (0%) | 0 (0%) | | 0 (0%) | 0 (0%) | 0 (0%) | 0 (0%) | 0 (0%) |
| **(5)(B)** | 5 (56%) | 4 (44%) | 0 (0%) | 0 (0%) | | 0 (0%) | 3 (33%) | 0 (0%) | 0 (0%) |
| **(7)** | 4 (57%) | 2 (29%) | 1 (14%) | 0 (0%) | 0 (0%) | | 0 (0%) | 0 (0%) | 0 (0%) |
| **(6)(A)** | 4 (80%) | 4 (80%) | 1 (20%) | 0 (0%) | 3 (60%) | 0 (0%) | | 0 (0%) | 0 (0%) |
| **(2)(A)** | 0 (0%) | 0 (0%) | 0 (0%) | 0 (0%) | 0 (0%) | 0 (0%) | 0 (0%) | | 0 (0%) |
| **(3)** | 0 (0%) | 0 (0%) | 0 (0%) | 0 (0%) | 0 (0%) | 0 (0%) | 0 (0%) | 0 (0%) | |

As seen in Table 10, there are generally low levels of charging coincidence across the statutory provisions. That could be because of prosecutorial restraint and careful statutory interpretation, or it could be due to crass calculations about sentencing.

Examining the frequency of specific CFAA offenses, in Table 11, sheds more light on prosecutorial strategy.[162] The most common CFAA criminal

159 *See* U.S. SENTENCING GUIDELINES MANUAL § 5G1.2 (U.S. SENTENCING COMM'N 2015) (recommending concurrent sentencing).

160 *Cf.* United States v. Cioni, 649 F.3d 276, 281-83 (4th Cir. 2011) (invalidating a CFAA felony enhancement for a Stored Communications Act violation, pursuant to the Double Jeopardy Clause of the Fifth Amendment).

161 There are substantial policy consequences if this alternative theory is accurate. If Congress or the courts narrowed the taking information offense, prosecutors could respond by charging the fraud and intentional damage offenses with greater frequency.

162 Two absences from criminal charging practice warrant brief mention. First, prosecutors made almost no use of CFAA's password trafficking provision. *See infra* Table 11. Since a substantial proportion of the Internet's underground economy involves stolen login credentials, the omission reaffirms that law enforcement has had difficulty reaching sophisticated offenders.

CFAA's unintentional damage and loss offense is also missing from criminal practice. *See infra* Table 11. Apparently, the Department of Justice did not file a single charge under that provision in 2012. *See infra* Table 11. A likely explanation is that the statutory elements include intentional

charge parallels the most common civil claim: taking information.[163] That result comes as little surprise, since the taking information offense is the broadest in the statute.

**Table 11: Frequency of Specific CFAA Provisions in Criminal Prosecutions**

| Charge (Principal, Attempt, Accomplice, or Conspiracy Liability) | Statutory Provision | Defendants |
|---|---|---|
| Taking Information | 1030(a)(2)(C) | 63 (47%) |
| Intentional Damage | 1030(a)(5)(A) | 49 (37%) |
| Fraud | 1030(a)(4) | 24 (18%) |
| Taking Federal Information | 1030(a)(2)(B) | 15 (11%) |
| Reckless Damage | 1030(a)(5)(B) | 9 (7%) |
| Extortion | 1030(a)(7) | 7 (5%) |
| Trafficking in Passwords | 1030(a)(6)(A) | 5 (4%) |
| Taking Financial Information | 1030(a)(2)(A) | 3 (2%) |
| Accessing a Federal System | 1030(a)(3) | 1 (1%) |
| Unintentional Damage and Loss | 1030(a)(5)(C) | 0 (0%) |

In a departure from the practices of private plaintiffs, however, prosecutors less frequently allege CFAA's broad fraud offense.[164] Criminal defendants face a fraud charge at roughly a third the frequency that plaintiffs include a fraud claim.[165]

This result suggests that prosecutors are making a greater effort than private litigants to distinguish among fraud theories of cybercrime liability. Prosecutors appear to generally treat CFAA fraud as a species of financial fraud—most cases directly involve either financial misconduct (11, 46%)[166] or a financial institution or agency (12, 50%).[167]

Another departure from civil practice is how prosecutors have invoked CFAA's intentional damage offense. Criminal defendants face a charge under that provision roughly half more often than civil cases invoke it. What's more,

unauthorized access. If prosecutors can already clear that mental state hurdle, they can likely demonstrate that the subsequent damage or loss was reckless or intentional.

163 *See infra* Table 11.

164 *See supra* Table 11.

165 *Compare supra* Table 11, with *supra* Table 6.

166 *See* Criminal Dataset, *supra* note 86 (((1030(a)(4) ∨ 1030(a)(4) Conspiracy) ∧ Financial Misfeasance) / (1030(a)(4) ∨ 1030(a)(4) Conspiracy)).

167 *See id.* ((Financial Institution Computer System) / (1030(a)(4) ∨ 1030(a)(4) Conspiracy)).

most of the cases under that provision involve either a circumvention of a technical protection (35, 71%)[168] or a software disruption (11, 22%).[169]

At a high level, this result indicates that part of CFAA is functioning as intended. Cases under CFAA's intentional damage provision map closely onto archetypal computer abuse of the sort that Congress and state legislatures emphasized when they enacted cybercrime statutes.

Looking more closely at fact patterns, though, prosecutors are not treating the intentional damage offense as a distinct theory of cybercrime liability. Most criminal cases involving CFAA's intentional damage offense appear much better characterized by the statute's taking information offense. While prosecutors have made a meaningful effort at distinguishing CFAA's fraud offense, they have treated the intentional damage offense as a catchall.

A likely explanation for why prosecutors are lumping fact patterns into the intentional damage offense is that it has uniquely enhanced sentencing consequences. As a statutory matter, the intentional damage offense is automatically associated with a maximum sentence of ten years.[170] And, under the federal sentencing guidelines, intentional damage automatically increases a defendant's recommended period of incarceration.[171]

In sum, prosecutors appear to exhibit complex strategic behavior in distinguishing cybercrime offenses. Where there is little or no sentencing difference, prosecutors *are* exercising much greater restraint than civil plaintiffs. They usually charge just one type of violation, and they usually select an appropriate theory.

Where there is a sentencing difference, though, prosecutors are blurring the distinctions between cybercrime offenses. They tend to charge just one type of violation—but they often charge the violation associated with substantially enhanced punishment, not the violation that best fits the defendant's conduct.

b. *External Redundancy*

Only a slight majority of CFAA prosecutions involve at least one non-CFAA charge (69, 52%).[172]

168 *See id.* (((1030(a)(5)(A) ∨ 1030(A)(5)(A) Conspiracy) ∧ Circumvention of a Technical Protection) / (1030(a)(5) ∨ 1030(A)(5)(A) Conspiracy)).

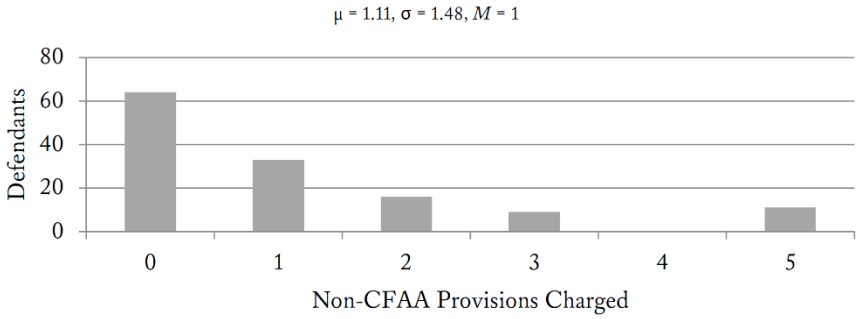
169 *See id.* (((1030(a)(5)(A) ∨ 1030(A)(5)(A) Conspiracy) ∧ Software Disruption of a Computer System) / (1030(a)(5)(A) ∨ 1030(A)(5)(A) Conspiracy)).

170 18 U.S.C. § 1030(c)(4)(B)(i).

171 *See* U.S. SENTENCING GUIDELINES MANUAL § 2B1.1(b)(18)(A)(ii) (U.S. SENTENCING COMM'N 2015) (directing an offense enhancement of four levels where the charge is intentional damage).

172 *See infra* Figure 13 ((Count of defendants with › 1 non-CFAA charge) / (All Criminal Defendants).

**Figure 13: Number of Non-CFAA Charges in Criminal Prosecutions**




What's more, among prosecutions that involve archetypal computer abuse—circumvention of a technical protection or disabling a computer system—most defendants face only CFAA charges (45, 58%).[173] This result stands in stark contrast to civil litigation practice. In criminal law, cybercrime offenses *are* fairly unique.[174] Examining the frequency of specific criminal charges, seen in Table 12, sheds more light on prosecutorial strategy.

173 *See* Criminal Dataset, *supra* note 86 (((Circumvention of a Technical Protection ∨ Software Disruption of a Computer System) ∧ Only CFAA Charges) / (Circumvention of a Technical Protection ∨ Software Disruption of a Computer System)).

174 An alternative interpretation, that prosecutors are strategically charging solely cybercrime offenses because they are the most punitive and easiest to prove, would also be consistent with this data. But examining the federal criminal statutes controverts that hypothesis—there are not lesser federal offenses that would generally reach archetypal computer abuse.

**Table 12: Frequency of Non-CFAA Charges in Criminal Prosecutions**

| Non-CFAA Charge (Principal, Attempt, Accomplice, or Conspiracy Liability) | Statutory Provision | Defendants |
|---|---|---|
| Identity Theft | 18 U.S.C. §§ 1028, 1028A (2012) | 30 (23%) |
| Wire Fraud | 18 U.S.C. § 1343 | 23 (17%) |
| Bank Fraud | 18 U.S.C. § 1344 | 22 (17%) |
| Access Device (Production, Trafficking, Possession, or Use) | 18 U.S.C. § 1029 | 16 (12%) |
| Racketeer Influenced and Corrupt Organizations Act (RICO) Conspiracy | 18 U.S.C. § 1962 | 9 (7%) |
| False Statements to a Federal Official | 18 U.S.C. § 1001 | 7 (5%) |
| Health Insurance Portability and Accountability Act (HIPAA) Disclosure | 42 U.S.C. § 1320d-6 | 4 (3%) |

The commonality between these cocharged offenses is that they are all (but one) accompanied by higher maximum or recommended sentences than the most frequent cybercrime offenses.[175] Where prosecutors do file a noncybercrime charge, then, they appear motivated by sentencing considerations.

The most common cocharge, identity theft, would seem to be an odd pairing for cybercrime offenses. The text of the statutory scheme primarily contemplates conventional identity theft involving forged documents.[176] But about half of cybercrime cases involving an identity theft charge arise from accessing another person's account on an online service (15, 50%).[177] The underlying statutory interpretation appears to be that entering another user's login and password constitutes an actionable form of identity theft.

This result bolsters the theory raised earlier that prosecutors strategically blur statutory offenses where enhanced sentences are available. In a plain reading of text and legislative history, the federal identity theft statute was

175 The offense for false statements to a federal official, 18 U.S.C. § 1001, carries the same maximum and recommended sentences as the most common cybercrime offenses. U.S. SENTENCING GUIDELINES MANUAL § 2B1.1(b)(11) (U.S. SENTENCING COMM'N 2015). *Compare* 18 U.S.C. § 1028(b)(2), *with* 18 U.S.C. § 1030(c)(2)(B).

176 *See generally* 18 U.S.C. §§ 1028(a), 1028A(a), (c).

177 *See* Criminal Dataset, *supra* note 86 (((Identity Theft $\vee$ Identity Theft Conspiracy) $\wedge$ Accessing Another Person's Account Without Permission) / (Identity Theft $\vee$ Identity Theft Conspiracy)).

intended to cover a distinct set of fact patterns from its neighboring computer abuse statute.[178] But identity theft offenses are accompanied by substantial and automatic sentence enhancements, so prosecutors have also styled computer abuse to fit within these identity theft offenses.[179]

A notable omission from the top cybercrime cocharges is the federal trade secret statute, part of the Economic Espionage Act (EEA).[180] Given that so many criminal prosecutions involve employees absconding with business information (51, 38%),[181] one would expect many cases to include trade secret counts. But there was only one CFAA case in 2012 that included an EEA count (1, 1%).[182]

A partial explanation is that nearly half of these employee prosecutions arise from government employment (23, 45%),[183] where trade secret protection is not available. As for the remainder, it is possible that prosecutors view the (slight) sentencing increases associated with a trade secret charge as offset by the (significant) additional offense elements.[184]

---

178 *See* 18 U.S.C. § 1028 (framing most offenses in terms of "identification documents" and "authentication features"); *id.* § 1028A (explicitly omitting CFAA as an overlapping offense for purposes of aggravated identity theft). The early legislative history of section 1028 centered on forged identification paperwork. *See False Identification: Hearing Before the Subcomm. on Crime of the H. Comm. on the Judiciary*, 97th Cong. 19 (1982) (statement of Rep. William J. Hughes, Chairman, Subcomm. on Crime of the H. Comm. on the Judiciary) (highlighting fraudulent identification in association with check forgery, travel, and firearm purchasing). Later expansion of the statute, including the provisions that (arguably) reach computer credentials, focused on identity theft and associated financial fraud. *See* S. REP. NO. 105-274, at 4-9 (1998); *Identity Theft and Assumption Deterrence Act: Hearing on S.J. Res. 512 Before the Subcomm. on Tech., Terrorism, and Gov't Info. of the S. Comm. on the Judiciary*, 105th Cong. 1, 2 (1998) (statement of Sen. Jon Kyl, Chairman, Subcomm. on Tech., Terrorism, and Gov't Info. of the S. Comm. on the Judiciary) (emphasizing identity theft arrests and financial losses).

179 *See* 18 U.S.C. § 1028(b)(1)(D) (imposing maximum sentence of fifteen years for identity theft if a defendant obtains $1,000 in value within one year); *id.* § 1028A(b)(2) (imposing mandatory two-year, non-concurrent sentence enhancement for aggravated identity theft); U.S. SENTENCING GUIDELINES MANUAL § 2B1.1(b)(11) (U.S. SENTENCING COMM'N 2015) (suggesting automatic enhancement to recommended sentence for identity theft offenses).

180 18 U.S.C. § 1832.

181 *See* Criminal Dataset, *supra* note 86 ((Employee, Consultant, Contractor, or Distributor ∧ Misappropriating Information) / (All Criminal Defendants)).

182 *See id.* ((Trade Secret Theft) / (All Criminal Defendants)).

183 *See id.* ((Employee, Consultant, Contractor, or Distributor ∧ Misappropriating Information ⋀ Government Computer System) / (Employee, Consultant, Contractor, or Distributor ∧ Misappropriating Information)).

184 The trade secret provisions of the EEA include a ten-year maximum sentence, 18 U.S.C. § 1832(a), but are subject to the same sentencing guidelines as common CFAA offenses, U.S. SENTENCING GUIDELINES MANUAL § 2B1.1(b)(11) (U.S. SENTENCING COMM'N 2015). Moreover, the EEA trade secret offense incorporates a number of additional elements, including reasonable measures to maintain secrecy and independent economic value on account of secrecy. *See* 18 U.S.C. §§ 1832, 1839; *Cyber Security: Protecting America's New Frontier: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary*, 112th Cong. 49 (2011) (statement of Professor Orin S. Kerr) ("Establishing a theft of trade secrets requires proving all the

An examination of specific charge coincidence, as demonstrated by Table 13, lends further support to the earlier observations about cybercrime's uniqueness, as well as how prosecutors are charging identity theft and fraud offenses.

**Table 13: Coincidence Between the Most Common CFAA and Non-CFAA Charges in Criminal Prosecutions**

| | Identity Theft | Wire Fraud | Bank Fraud | Access Device | RICO |
|---|---|---|---|---|---|
| Taking Information | 19 (30%) | 13 (21%) | 11 (17%) | 11 (17%) | 9 (14%) |
| Intentional Damage | 11 (22%) | 16 (33%) | 16 (33%) | 12 (24%) | 9 (18%) |
| Fraud | 4 (17%) | 10 (42%) | 8 (33%) | 1 (4%) | 0 (0%) |
| Taking Federal Information | 1 (7%) | 0 (0%) | 0 (0%) | 1 (7%) | 0 (0%) |
| Reckless Damage | 1 (11%) | 0 (0%) | 0 (0%) | 0 (0%) | 0 (0%) |

The cybercrime offenses that relate to taking information from a federal government computer, and recklessly damaging a computer, have near-zero charge coincidence. In these areas of misconduct, CFAA provides especially unique criminal law coverage.

The high coincidence between information misappropriation charges and identity theft charges reaffirms that prosecutors are strategically invoking identity theft offenses to secure sentencing enhancements. These are fundamentally computer abuse cases, involving account break-ins.

Finally, CFAA fraud charges are frequently paired with wire fraud or bank fraud charges (12, 50%).[185] This result further confirms that, in prosecutorial practice, cybercrime fraud is largely a species of conventional financial fraud.

### F. *Does Cybercrime Law Deter Computer Abuse?*

In a conventional quantitative evaluation of deterrence, a cybercrime offender is motivated by the potential gain associated with misconduct, less the sentence imposed by criminal law, discounted by the probability of successful prosecution.[186]

elements of the crime, and that can be a difficult task. In contrast, proving [under CFAA] that an employee did *something* for reasons other than official company business is vastly easier.").

185 *See* Criminal Dataset, *supra* note 86 (((1030(a)(4) ∨ 1030(a)(4) Conspiracy) ∧ (Wire Fraud ∨ Wire Fraud Conspiracy ∨ Bank Fraud)) / (1030(a)(4) ∨ 1030(a)(4) Conspiracy)) .

186 *See* Gary S. Becker, *Crime and Punishment: An Economic Approach*, 76 J. POL. ECON. 169, 176-79 (1968) (offering a theoretical approach to measuring deterrence based on the number of offenses a criminal would commit, the probability of conviction per offense, and "a portmanteau variable representing all . . . other influences"); Richard A. Posner, *An Economic Theory of the Criminal Law*, 85 COLUM. L. REV. 1193, 1201-05 (1985) (justifying criminal sanctions based on the need to impose optimal deterrence for such offenses, which pecuniary penalties alone cannot achieve).

Available datasets on cybercrime are not sufficiently comprehensive or detailed to credibly estimate these values for individual offenders. It is possible, though, to compute aggregate metrics of how cybercrime law deters cybercrime offenses.

One simple measurement is a comparison of total cybercrime gains to total cybercrime sentences in a given year. The result is a very rough approximation of expected punishment relative to the incentive to commit cybercrime.

$$Expected\ Punishment_{year} = \frac{Total\ Punishment_{year}}{Total\ Gains_{year}}$$

A slightly more sophisticated measurement takes advantage of cybercrime time series data by treating year-to-year changes as natural experiments. By comparing the volume of punishment in sequential years, it is possible to—again, very roughly—estimate the marginal punishment imposed by cybercrime law relative to the incentives for cybercrime. In intuitive terms, this measure reflects how responsive the criminal justice system is to changes in cybercrime volume.

$$Marginal\ Punishment_{year} = \frac{Total\ Punishment_{year} - Total\ Punishment_{year-1}}{Total\ Gains_{year} - Total\ Gains_{year-1}}$$

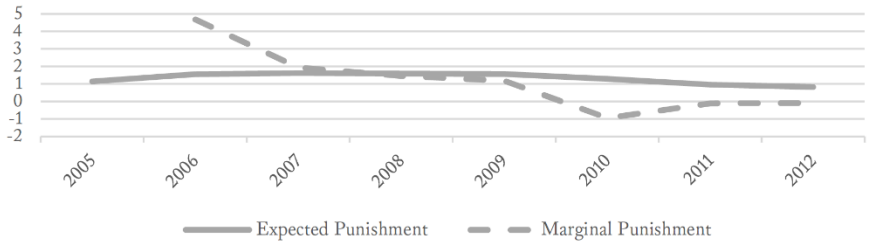
Prosecution data from the Department of Justice are reasonably accurate and are sufficient to calculate the numerators in these equations. The denominators, by contrast, are much more difficult to obtain. Data sources on gains and losses associated with cybercrime are notoriously unreliable,[187] and many high-profile breaches are associated with nonmonetary motives.

In the interest of generating highly defensible figures, I conservatively estimate the gains from cybercrime as those solely due to domestic credit card fraud.[188] I also liberally estimate the punishment associated with cybercrime by including not just CFAA offenses, but also federal identity theft and access device offenses.

187 *See* Ross Anderson et al., *Measuring the Cost of Cybercrime* (critiquing prior attempts at quantifying cybercrime as inconsistent and inaccurate), *in* THE ECONOMICS OF INFORMATION SECURITY AND PRIVACY 265, 267 (Rainer Böhme ed., 2013); Dinei Florêncio & Cormac Herley, *Sex, Lies and Cyber-Crime Surveys* (noting survey errors in attempts to quantify cybercrime), *in* ECONOMICS OF INFORMATION AND SECURITY AND PRIVACY III 35, 37 (Bruce Schneier ed., 2013).

188 The underlying data on credit card fraud are sourced from a regular financial newsletter that maintains a longitudinal fraud dataset. *See Card Fraud Losses Reach $16.31 Billion*, NILSON REP. (HSN Consultants, Inc., Carpinteria, CA), July 2015, at 5, 10 (reporting trends in credit card fraud from the 1990s onwards). For purposes of the marginal punishment metric, movement in credit card fraud functions as a rough proxy for movement in the overall level of cybercrime.

**Figure 14: Deterrence Effects of Federal Cybercrime Law (Months Incarcerated Per $100,000)**




Even with these exceedingly generous assumptions—likely underestimating incentives and overestimating punishments by orders of magnitude—the results are unequivocal. If a would-be offender can expect to earn (very roughly and conservatively) $100,000 and serve just one month in prison, and if punishment levels are far outpaced by incentive growth, then cybercrime law cannot meaningfully deter cybercrime.

### G. *Assessing the Two Perspectives on Cybercrime Law*

In civil cybercrime litigation, the critical perspective has strong empirical support. The volume of litigation has radically increased, and the overwhelming majority of claims do not arise from sophisticated hacking. Rather, cases relate to mundane commercial disputes that happen to involve computers. Considerable evidence indicates that civil cybercrime liability is duplicative of conventional private causes of action, and that private plaintiffs greatly blur theories of cybercrime liability.

The data on criminal litigation are much more mixed. Cybercrime charges increased from the 1990s to the 2000s, but then leveled off. Prison sentences have shot up, but prosecutors continue to exercise substantial discretion over whether to impose any incarceration. Prosecutors generally only charge under one theory of cybercrime liability, but this is likely due to strategic sentencing calculations. A little over half of criminal charges arise from archetypal hacking activities, and prosecutors do succeed in occasionally prosecuting serious offenders. But most defendants engage in unsophisticated and minor misconduct, arising from an existing commercial, employment, or personal relationship. In sum, the state of cybercrime prosecutorial practice is highly nuanced, and neither perspective is descriptively accurate.

## III. RECOMMENDATIONS

Several prescriptions follow naturally from this comprehensive empirical portrait of cybercrime litigation. The data provide support for three readily implementable proposals: congressional elimination of civil CFAA liability, the establishment of clear Department of Justice enforcement priorities, and a narrow interpretation of cybercrime statutes.[189]

### A. *Civil Liability*

Providing private causes of action for cybercrime has proved to be a failed experiment, spurring an explosion of highly redundant litigation.

The underlying cause of this phenomenon appears to be readily discernable: Conventional employment and commercial disputes increasingly involve information technology, are relatively straightforward to investigate, and can generally be addressed through conventional legal processes. Sophisticated hacks, by contrast, can be difficult to uncover and attribute, and perpetrators will often be either outside the reach of United States courts or judgment proof.[190] In more precise policy terminology, private cybercrime liability poses a fundamental target inefficiency.[191] If cybercrime law even cracks the door to mundane private controversies, they will naturally swamp serious computer abuse cases.

The easy statutory fix is to eliminate private cybercrime causes of action.[192] Textual revisions are trivial to make, since cybercrime statutes were drafted primarily as a set of criminal offenses.[193] Private causes of action

189 This part focuses primarily on federal reforms in the interest of brevity and because the data examined in this Article were exclusively federal. Nevertheless, these same recommendations extend to state legislatures, prosecutors, and courts.

190 Notably, in a review of recent high-profile data breaches, almost *none* resulted in civil litigation or criminal charges. *See Chronology of Data Breaches*, PRIVACY RTS. CLEARINGHOUSE (Apr. 20, 2005), http://www.privacyrights.org/data-breach [https://perma.cc/8EAG-U8N6] (providing a dataset of data breach incidents).

191 *See* Robert S. Goldfarb, *Compensating Victims of Policy Change*, REG., Sept.–Oct. 1980, at 22, 24 (explaining the theory of target inefficiency).

192 *Cf.* Brenton, *supra* note 10, at 457-59 (recommending the partial repeal of CFAA's private cause of action); Cindy Cohn & Marcia Hofmann, *Part 2: EFF's Additional Improvements to Aaron's Law*, ELECTRONIC FRONTIER FOUND. (Jan. 23, 2013), https://www.eff.org/deeplinks/2013/01/part-2-effs-additional-improvements-aarons-law [https://perma.cc/YP2Q-H5NC] (recommending the total repeal of CFAA's private cause of action, among other revisions); Eric Goldman, *The Computer Fraud and Abuse Act is a Failed Experiment*, FORBES (Mar. 28, 2013), http://www.forbes.com/sites/ericgoldman/2013/03/28/the-computer-fraud-and-abuse-act-is-a-failed-experiment/ [https://perma.cc/HZK4-ZMXS] (same); Orin Kerr, *Proposed Amendments to 18 U.S.C. 1030*, VOLOKH CONSPIRACY (Jan. 20, 2013), http://volokh.com/2013/01/20/proposed-amendments-to-18-u-s-c-1030/ [https://perma.cc/8U7D-DQVT] (same).

193 *See* Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 965-66 (D. Ariz. 2008) ("Simply stated, the CFAA is a criminal statute focused on criminal conduct. The civil component is an afterthought.").

generally consist of secondary add-on provisions, which Congress and state legislatures could simply repeal.[194]

### B. *Enforcement Priorities*

Most federal cybercrime prosecutions arise from minor and technically unsophisticated misconduct, especially employees misappropriating information. There is, though, a meaningful subset of prosecutions that involves serious computer abuse.

The Department of Justice should establish a clear cybercrime enforcement policy to shift this balance.[195] Where a fact pattern involves special factors—for instance, technical sophistication, significant monetary loss, or a federal computer system—federal prosecutors should consider filing cybercrime charges. But where the circumstances are more mundane, such as a commercial or employment dispute that happens to involve information technology, the local United States Attorney's Office should (at most) refer the matter to state and municipal law enforcement agencies.[196]

An enforcement policy could also address concerns about cybercrime overbreadth. Prosecutors rarely charge ordinary consumers, journalists, or security researchers under cybercrime law—yet there is a widely perceived legal risk for those communities.[197] Department of Justice officials already assert a lack of prosecutorial interest in those fact patterns; formalizing a declination policy would go a long way toward allaying concerns.[198]

Finally, an enforcement policy could facilitate doctrinal clarity for cybercrime law, enhancing conformity with the statutory scheme and promoting predictability in criminal justice outcomes. Federal prosecutors do currently appear to be making good-faith attempts at distinguishing individual cybercrime offenses—but only where there is no sentencing

194 At the federal level, for instance, eliminating civil liability would simply require repealing 18 U.S.C. § 1030(g) (2012).

195 *Cf.* Tim Wu, *Fixing the Worst Law in Technology*, NEW YORKER NEWS DESK (Mar. 18, 2013), http://www.newyorker.com/news/news-desk/fixing-the-worst-law-in-technology [https://perma.cc/WTP3-QMB6] (recommending that the Department of Justice adopt a narrow CFAA enforcement policy).

196 *Cf.* Memorandum from James M. Cole, Deputy Att'y Gen., Guidance Regarding Marijuana Enforcement 3-4 (Aug. 29, 2013), http://www.justice.gov/iso/opa/resources/305829 1327 56857467.pdf [https://perma.cc/GT7K-EU6D] (establishing Department of Justice enforcement policy for marijuana offenses, such that state and local law enforcement have primary responsibility).

197 *See supra* Section I.B.

198 *See, e.g.*, David Bitkower, *Testimony Before the Senate Judiciary Subcommittee on Crime and Terrorism*, JUST. NEWS (July 8, 2015), https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-david-bitkower-delivers-testimony-senate-judiciary [https://perma.cc/7FKE-4WP6] ("The department has no interest in prosecuting such harmless acts."); Leslie R. Caldwell, *Prosecuting Privacy Abuses by Corporate and Government Insiders*, U.S. DEP'T OF JUST. (Mar. 16, 2015), http://www.justice.gov/opa/blog/prosecuting-privacy-abuses-corporate-and-government-insiders [https://perma.cc/WVY6-KVFH] ("The Department of Justice has no interest in prosecuting harmless violations of use restrictions like these.").

advantage. The Department of Justice could easily provide guidance on which statutory offenses are most appropriate for recurring fact patterns.[199]

### C. *Narrow Construction of CFAA*

The courts are presently engaged in a debate about the appropriate scope of federal cybercrime law. Since CFAA's scoping provisions are so ambiguous, courts have resorted to reading proverbial legislative history tea leaves. Some conclude that Congress did not intend for CFAA to have broad reach, going far beyond archetypal hacking;[200] others conclude that Congress did contemplate liability for mundane computer misuse, especially by employees.[201]

The empirical data on federal cybercrime litigation enable a powerful new argument to be made from CFAA's legislative history. Congress may have intended to open the federal courthouse door—just a crack—to claims involving routine and unsophisticated computer misconduct.[202] But Congress

---

199 *Cf.* U.S. DEP'T JUSTICE, PROSECUTING COMPUTER CRIMES 1-58 (2010) (reviewing components of CFAA for United States Attorneys).

200 *See, e.g.*, United States v. Nosal, 676 F.3d 854, 858 (9th Cir. 2012) (concluding that a narrower interpretation of CFAA "maintains the CFAA's focus on hacking rather than turning it into a sweeping Internet-policing mandate"); Black & Decker (US), Inc. v. Smith, 568 F. Supp. 2d 929, 935-38 (W.D. Tenn. 2008) (discussing the legislative history of CFAA at length to bolster its conclusion that CFAA should not be read broadly); Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 963-67 (D. Ariz. 2008) ("[T]he legislative history supports a narrow view of the CFAA."); Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479, 495-99 (D. Md. 2005) (relying on the legislative history of CFAA to interpret the statute).

201 *See, e.g.*, NCMIC Fin. Corp. v. Artino, 638 F. Supp. 2d 1042, 1058 (S.D. Iowa 2009) (reviewing aspects of CFAA's legislative history before adopting a broad view of the statute); Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1127-29 (W.D. Wash. 2000) (relying on Senate Reports to construe CFAA broadly).

202 In my own reading of the legislative history, Congress did—ever so slightly—consider the issue of unsophisticated employee liability. *See* S. REP. NO. 104-357, at 7-8 (1996) (establishing liability for "individuals who intentionally . . . abuse their authority to use . . . a computer and thereby obtain information of minimal value"); *Security in Cyberspace: Hearings Before the S. Subcomm. On Investigations of the S. Comm. on Gov't Affairs*, 104th Cong. 6 (1996) (statement of Sen. John Glenn) ("Over the years, this Committee has examined threats to security and privacy as diverse as . . . IRS employees browsing through taxpayer records . . . ."); *id.* at 326 (statement of Richard G. Power, Editor, Computer Security Institute) ("Also, in recent weeks, it was revealed that several employees of the Social Security Administration allegedly passed information on 11,000 people . . . to a credit card fraud ring."); *Computer Fraud Legislation: Hearing on S.440 and S. 1678 Before the S. Subcomm. on Criminal Law of the S. Comm. on the Judiciary*, 99th Cong. 35 (1985) (statement of Victoria Toensing, Deputy Assistant Att'y Gen.) (noting an incident where a former employee of the Federal Reserve illicitly accessed money supply information on a computer system); *Computer Crime and Computer Security: Hearing on H.R. 1001 and H.R. 930 Before the H. Subcomm. on Crime of the the H. Comm. on the Judiciary*, 99th Cong. 30 (1985) (statement of John C. Keeney, Deputy Assistant Att'y Gen.) (discussing the potential for computer-based financial fraud by bank employees); *id.* at 149-150 (statement of Allan Robert Adler, Legislative Counsel, ACLU) (noting possible CFAA application to government employees who use data for whistleblowing); *id.* at 213-14 (debating propriety of employee liability for mishandling information); 98 CONG. REC. 31,992-93 (1984) (statement of

did not intend to fling the door wide open, for so much run-of-the-mill commercial litigation.[203]

Setting aside the merits of any individual case, the aggregate civil and criminal caseloads under CFAA simply cannot be reconciled with a fair reading of the legislative record.[204] Nearly every cybercrime anecdote that Congress considered, and nearly every statement in the record, presumed legislation would reach archetypal hacking.[205] There was almost no opposition to CFAA expansion based on potential liability for employees, competitors, or consumers.[206] If the statute were intended to sweep as broadly as it does

---

Sen. Patrick Leahy)(criticizing CFAA for putting government employees at risk when whistleblowing); *id.* at 32,083-84 (statement of Sen. Charles Mathias) (proposing amendment to CFAA that would restrict applicability to government employees).

203 *Cf. Shamrock Foods*, 535 F. Supp. 2d at 967 ("The Court declines the invitation to open the doorway to federal court so expansively when this reach is not apparent from the plain language of the CFAA.").

204 In addition to this aggregate legislative history argument, and a more conventional legislative history argument, there are other reasons to narrowly construe CFAA. A broad interpretation raises myriad issues, including the rule of lenity, due process void-for-vagueness protections, nondelegation considerations, the expectation that Congress should speak clearly when determining significant policy, federalism, and judicial economy. *See* United States v. Valle, 807 F.3d 508, 523-28 (2d Cir. 2015) (following *Nosal* in applying the rule of lenity); WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 203-07 (4th Cir. 2012) (same); *Nosal*, 676 F.3d at 863 (invoking the rule of lenity in declining to extend CFAA to violations of a website's terms of use); United States v. Drew, 259 F.R.D. 449, 462-67 (C.D. Cal. 2009) (holding that an interpretation of CFAA that reaches conscious violations of a website's terms of use is constitutionally void for vagueness); *Shamrock Foods*, 535 F. Supp. 2d at 967 (D. Ariz. 2008) ("The Court declines the invitation to open the doorway to federal court so expansively when this reach is not apparent from the plain language of the CFAA."); Samantha Jensen, *Abusing the Computer Fraud and Abuse Act: Why Broad Interpretations of the CFAA Fail*, 36 HAMLINE L. REV. 81, 137 (2014) ("A narrow interpretation of the CFAA is the only way to ensure that the statute does not eclipse large portions of state law."); Alden Anderson, Comment, *The Computer Fraud and Abuse Act: Hacking into the Authorization Debate*, 53 JURIMETRICS 447, 457-59 (2013) (contending that a broad interpretation of CFAA is inconsistent with the historical division of cases between state and federal courts); Note, *The Vagaries of Vagueness: Rethinking the CFAA as a Problem of Private Nondelegation*, 127 HARV. L. REV. 751, 768-71 (2013) (arguing CFAA violates nondelegation doctrine).

205 After an exhaustive review of committee hearings and reports on CFAA, I located only a handful of anecdotal references to employees misappropriating information. *See supra* note 206. Discussion of hacking, by contrast, pervades the legislative history.

206 From a review of the legislative history, it appears that vocal opposition to CFAA is a recent phenomenon. Congressional hearings did not involve witnesses critical of CFAA's scope until 2011, and those witnesses were only invited after public interest advocacy. *See Cyber Crime: Updating the Computer Fraud and Abuse Act to Protect Cyber Space and Combat Emerging Threats: Hearing Before the S. Comm. on the Judiciary,* 112th Cong. 27 (2011) (joint letter for the record from public interest organizations); *id.* at 48 (letter for the record from Gregory T. Nojeim) (advocating that the committee "address longstanding concerns with the ambiguity and breadth of the CFAA"); *Cyber Security: Protecting America's New Frontier: Hearing Before the H. Subcomm. On Crime, Terrorism and Homeland Security of the H. Comm. on the Judiciary*, 112th Cong. 39 (2011) (statement of Orin S. Kerr, Professor of Law, George Washington University) ("I think the answer is to narrow the scope of [CFAA] . . . ."). The sole exception to this was some initial concern in the 1980s about enforcement against whistleblowers.

in its most common uses today—with significant implications for individual liability and the scope of federal jurisdiction—surely Congress would have spoken more plainly, and would have deliberated the consequences.[207]

## CONCLUSION: A LIMITED ROLE FOR CYBERCRIME LIABILITY

Cybercrime is a serious and growing problem, resulting in (by some estimates) over $100 billion in losses per year.[208] The primary response by federal and state legislatures, so far, has been to impose and expand cybercrime liability.[209]

That approach is no longer tenable. The drawbacks of excessive scope are real—constituting a majority of civil cases and about half of criminal cases. Those drawbacks are inherent in the very concept of computer abuse liability.

Constructing digital analogies to physical trespass and property damage had an understandable logic in the 1970s and 1980s; computer systems were relatively rare, single-purpose, limited to particular users, dedicated to sensitive applications, and had scarce resources.[210] Legislators and courts could afford to play somewhat fast and loose with "authorization," "damage," and other key scoping provisions, since egregious misconduct was more readily ascertainable: breaking into the nuclear weapons laboratory at Los Alamos, for example, or tampering with medical records at the Sloan Kettering Cancer Center. Both of these examples are drawn directly from early hearings on federal cybercrime law.[211]

---

207 *See Nosal*, 676 F.3d at 857 ("If Congress meant to expand the scope of criminal liability to everyone who uses a computer in violation of computer use restrictions—which may well include everyone who uses a computer—we would expect it to use language better suited to that purpose.").

208 *See, e.g.*, CTR. FOR STRATEGIC AND INT'L STUDIES, NET LOSSES: ESTIMATING THE GLOBAL COST OF CYBERCRIME (2014), http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf [https://perma.cc/BBP8-ANZT] (extrapolating from global data on the cost of cybercrime to produce admittedly rough estimates of losses totaling between $375 and $575 billion).

209 *See* Stewart Baker, *Poisoning the Hamburger Helper*, VOLOKH CONSPIRACY (Sept. 11, 2011), http://volokh.com/2011/09/11/poisoning-the-hamburger-helper/ [https://perma.cc/PE6J-8V6V] ("Every time Congress gets exercised about cybersecurity, the Justice Department claims that the CFAA needs to be updated."); Orin S. Kerr, Powerpoint: Domestic Cybersecurity Law (or at Least Parts of It) (2014), http://www.hoover.org/sites/default/files/kerr_stanfordslides.pdf [https://perma.cc/853B-9XT7] ("Expanding CFAA becomes Congress's favorite way to 'do something' about cybersecurity.").

210 *Cf.* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1601 (2003) ("Unauthorized access statutes are creatures of the 1970s, when the Internet remained the domain of a few scientists and engineers . . . . While technology has advanced considerably in the last three decades, the law has not; the same one-size-fits-all prohibitions on unauthorized access still govern."); Greg Pollaro, *Disloyal Computer Use and the Computer Fraud and Abuse Act: Narrowing the Scope*, 2010 DUKE L. & TECH. REV. ¶¶ 1, 10 (using one computer crime statute for myriad activities "has inevitably forced square pegs into round holes").

211 *See Computer Viruses: Hearing on the Impact of Computer Viruses and Other Forms of Computer Sabotage or Exploitation on Computer Information Systems and Networks Before the S. Subcomm. On Tech. and the Law, S. Comm. on the Judiciary*, 101st Cong. 6 (1989) (statement of Sen. Gordon J. Humphrey) (discussing a hack into the computers at Los Alamos); *The Computer Fraud and Abuse Act of 1986:*

Today, of course, computer systems are pervasive, have myriad functions, can be shared by millions of users, and are used for everyday activities. Assessing the scope of authorization and calibrating compensable harm are radically different and far more challenging tasks; defendants tend to have *some* permission with respect to a computer system, and conduct at issue tends to be less patently wrongful. Plaintiffs and prosecutors can craft a colorable cybercrime claim from myriad modern fact patterns, dragging the courts into doctrinal quagmires and chilling socially beneficial activities.

As against this downside, there is not much upside. The plausible deterrence benefits of cybercrime law are, empirically, negligible.

Cybercrime law does have value, to be sure. Prosecutors are able to charge serious offenders on occasion, and meaningful criminal sanctions should be available. But, on the whole, cybercrime law is an exceedingly limited mechanism for addressing online misconduct.

The federal and state governments have a number of other viable responses to cybercrime. They could mitigate the harms associated with security breaches, by enacting notification and credit monitoring mandates.[212] They could improve defenses, by leveraging acquisitions, promoting best practices, and facilitating information sharing.[213] In areas of critical infrastructure, or where sensitive data are involved, they could impose ex ante security standards and ex post regulatory liability.[214]

---

*Hearing on S. 2281 Before the S. Comm. on the Judiciary*, 99th Cong. 39 (1986) (statement of Joseph Tomkins, Chairman, American Bar Association Criminal Justice Section Task Force on Computer Crime) (describing the "infiltration of hospital records" at the Sloan Kettering Cancer Institute).

212 At the time of writing, forty-seven states have enacted data breach notification laws. *See Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES (Jan. 4, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/7VAZ-RDQU] (collecting state data breach notification statutes). The Obama Administration has also twice proposed a federal data breach notification requirement. THE WHITE HOUSE, ADMINISTRATION DISCUSSION DRAFT: CONSUMER PRIVACY BILL OF RIGHTS ACT (Feb. 27, 2015), https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf [https://perma.cc/5RSQ-F4Y7]; THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD (2012), https://www.whitehouse.gov/sites/default/files/privacy-final.pdf [https://perma.cc/SS9S-VRX8]. At the federal level, there are also sector-specific data breach notification rules. *See* GINA STEVENS, CONG. RESEARCH SERV., RL34120, FEDERAL INFORMATION SECURITY AND DATA BREACH NOTIFICATION LAWS (2010).

213 *See generally* Jonathan Mayer & Edward W. Felten, *California Must Lead on Cybersecurity*, SACRAMENTO BEE (Jan. 24, 2015), http://www.sacbee.com/opinion/the-conversation/article7967445.html [https://perma.cc/WF89-DF5M] (suggesting state-level policies that would promote cybersecurity).

214 *See, e.g.*, FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 243-59 (3d Cir. 2015) (sustaining FTC Act liability for a breached business); COPPA Rule, 16 C.F.R. § 312.8 (2015) (security requirements for certain children's information); GLBA Safeguards Rule, 16 C.F.R. §§ 314.1-5 (2015) (security requirements for certain financial information); HIPAA Security Rule, 45 C.F.R. §§ 164.302–.318 (2015) (security requirements for certain medical information); FED. COMMC'N COMM'N, CHAIRMAN WHEELER'S PROPOSAL TO GIVE BROADBAND CONSUMERS INCREASED CHOICE, TRANSPARENCY, AND SECURITY WITH RESPECT TO

For too long, federal and state policies have overemphasized malicious computer abusers as the exclusive cause of serious cybersecurity incidents. The temptation is understandable—as Ronald Coase famously observed, law conventionally allocates responsibility to actions that give rise to social costs, rather than inaction that magnifies those costs.[215] But technology owners and operators are often in the best position to repel and remediate online misconduct. They just lack sufficient incentives to do so in the status quo—incentives that cybercrime litigation will never provide.

THEIR DATA (2016), https://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0310/DOC-338159A1.pdf [https://perma.cc/7LTA-VK2C] (proposed security requirements for broadband Internet service providers).

215 R.H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1, 13-15 (1960).