IN THE

UNITED STATES COURT OF APPEALS

FOR THE FIFTH CIRCUIT

NO. 16-41264

UNITED STATES OF AMERICA,
Plaintiff-Appellee,
v.

MICHAEL THOMAS,
Defendant-Appellant.

APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF TEXAS (SHERMAN DIVISION), NO. 4:13-CR-227-ALM-CAN

OPENING BRIEF FOR THE APPELLANT MICHAEL THOMAS

Aaron K. Williamson (N.Y. Bar # 4580999)
Tor B. Ekeland (N.Y. Bar # 4493631)
Tor Ekeland P.C.
43 W. 43rd Street, Suite 50
New York, NY 10036-7424
Telephone: 773-727-8363
Facsimile: 718-504-5417
aaron@torekeland.com
tor@torekeland.com
Attorneys for Defendant-Appellant

CERTIFICATE OF INTERESTED PERSONS

The number and style of the case in the court below is *United States of America v. Michael Thomas*, 4:13-cr-00227-ALM-CAN, in the United States District Court for the Eastern District of Texas, Sherman Division.

The undersigned counsel of record certifies that the following listed persons have an interest in the outcome of this case. These representations are made in order that the judges of this Court may evaluate possible disqualification or recusal.

Federal District Judge:	Hon. Amos L. Mazzant III
Magistrate Judge:	Hon. Christine A. Nowak
Appellant:	Michael Johnathan Thomas
Appellant's Attorneys:	Aaron K. Williamson
	Tor B. Ekeland
United States Attorneys:	Brit Featherston
Assistant United States Attorneys:	Camelia E. Lopez
	Marisa J. Miller
	Robert A. Wells

REQUEST FOR ORAL ARGUMENT

The defendant-appellant, Michael Thomas, respectfully requests oral argument. This appeal presents an issue of first impression in any circuit court of appeal, in an area of substantial disagreement between circuits: whether the Rule of Lenity requires that "without authorization" be interpreted narrowly in Computer Fraud and Abuse Act ("CFAA") cases brought under 18 U.S.C. § 1030(a)(5)(A), as many courts have held that it does in cases brought under 18 U.S.C. § 1030(a)(2) and (a)(4). Oral argument of the facts and applicable precedent would benefit the Court.

TABLE OF CONTENTS

TABLE OF CITATIONS

Cases

Statutes

Other Authorities

STATEMENT OF JURISDICTION

Jurisdiction of this Court is invoked under 28 U.S.C. § 1291 as an appeal from a final judgment of conviction and sentence in the United States District Court for the Eastern District of Texas. Notice of appeal was timely filed in accordance with Federal Rule of Appellate Procedure. 4(b) Jurisdiction is also invoked pursuant to 18 U.S.C. § 3742.

Written judgment was entered by the district court on August 31, 2016. [1] A timely notice of appeal was filed on September 8, 2016. [2]

---

1 ROA.1375-80 (Judgment).

2 ROA.1381-82 (Notice of Appeal).

STATEMENT OF THE ISSUES

1. Applying the Rule of Lenity, circuit courts have held that a CFAA defendant cannot be criminally liable for acting "without authorization" unless he does something he had "no rights, limited or otherwise," to do. As ClickMotive's IT administrator, Michael Thomas was broadly authorized to "damage" its systems within the meaning of the CFAA. Did he do so "without authorization" if he violated company policy or his common law duty of loyalty?
2. A statute is void for vagueness if it fails to either (1) "define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited" or (2) "establish minimal guidelines to govern law enforcement." If criminal liability under CFAA § 1030(a)(5)(A) is determined by reference to a broad corporate policy of general applicability or the common law duty of loyalty, is it void for vagueness as applied?

STATEMENT OF THE CASE

1. ClickMotive did not impose explicit or implicit restrictions on Thomas's broad authority as an IT administrator

Michael Thomas has "broad responsibilities for managing ClickMotive's systems and network."[3] Beginning in February 2010, Thomas worked as an information technology ("IT") administrator for ClickMotive LP for about two years.[4] ClickMotive designed and maintained websites for car dealerships. Thomas was one of two people responsible for maintaining ClickMotive's network and computer systems.[5] Because ClickMotive was a small company, these responsibilities extended to every computer in ClickMotive's offices—from the servers that ran the company intranet, to the laptops issued to individual employees, to the appliance that controlled the electronic door-access system.[6]

As an IT administrator, Thomas had unlimited administrative access to all of these systems—his user account was permitted to take any action or delete any file on any ClickMotive system.[7] ClickMotive did not maintain any policy specifically governing the IT staff's activity.[8]

---

3 ROA.1944 (Testimony of Ray Myers).
4 ROA.2682 (Government Exhibit 3).
5 ROA.1959-60 (Testimony of Ray Myers).
6 ROA.1864 (Testimony of Ray Myers).
7 ROA.1944-45 (Testimony of Ray Myers).
8 ROA.1951 (Testimony of Ray Myers).

Thomas was the administrator of all of the computer systems at issue in this case. He managed ClickMotive's backup systems, deciding when and how the company's servers should be backed up, and when backups should be removed.[9] He also managed the company intranet, which consisted of a "wiki" that ClickMotive employees periodically updated with information relevant to their jobs.[10] Thomas used the wiki to store various information about the computer systems he maintained.[11] Like every employee, Thomas was permitted to add information to the wiki and to delete it.[12] ClickMotive had no policy regarding when it was permissible to delete information from the wiki.[13]

Thomas managed ClickMotive's email server: he added and removed users, changed user permissions, and managed user groups.[14] He managed the company's internal network, including its firewall and the virtual private network ("VPN") that enabled employees to log into the network remotely.[15] By virtue of these responsibilities, Thomas was effectively on call twenty-four hours a day, and he

---

9 *See* ROA.2682 (Government Exhibit 3).

10 ROA.1952-53 (Testimony of Ray Myers). A wiki is a website, similar to Wikipedia, that can be edited by any registered user. *Id*.

11 ROA.2384 (Testimony of Andrew Cain).

12 ROA.1952-53 (Testimony of Ray Myers).

13 ROA.2384 (Testimony of Andrew Cain).

14 ROA.1947-48 (Testimony of Ray Myers).

15 ROA.1946 (Testimony of Ray Myers).

maintained a pager alert system to notify him (and, if he was unavailable, other employees) of issues that arose while he was away from the office.[16]

2. When ClickMotive fired the only other IT Administrator, Thomas's responsibilities increased

Thomas was first recommended for the ClickMotive job by his friend Andrew Cain, who at the time was ClickMotive's only IT employee.[17] Thomas worked side by side with Cain for two years until, on December 1, 2011, Cain was terminated without notice.[18] Cain was very upset by his termination.[19] He was ClickMotive's first employee.[20] The company's owners, Ray Myers and Stuart Lloyd, were "serial entrepreneurs" who had started and sold several companies in the past and shared the proceeds with their employees.[21] Now, as the owners were actively seeking outside investors,[22] Cain had been cut off from any such share.

While the owners gave Cain the bad news, Thomas was pulled aside by his supervisor and offered a bonus to stay on for three months and take over Cain's responsibilities.[23] Thomas hesitated to accept the offer. He and Cain were close—

---

16 ROA.1947-48 (Testimony of Ray Myers).
17 ROA.2369-70 (Testimony of Andrew Cain).
18 *Id*.
19 ROA.2369 (Testimony of Andrew Cain).
20 *Id*.
21 ROA.1935 (Testimony of Ray Myers).
22 ROA.1837 (Testimony of Stuart Lloyd).
23 ROA.1959 (Testimony of Ray Myers).

at trial, Cain described Thomas as having been his "only friend."[24] Thomas was the first person Cain told about his termination, calling him on the drive home that day to express his hurt and anger.[25] Now Thomas not only had to do the jobs of two people, he had taken one of those jobs from his close friend.

Cain believed he had been wrongfully terminated and immediately began preparing a lawsuit against ClickMotive, as another ex-employee had recently done.[26] Cain's wife asked Thomas to obtain emails from ClickMotive to "help with those lawsuits."[27] Thomas searched the email of ClickMotive's executives and provided some emails to Mrs. Cain.[28] He was not charged with any offense related to searching for, obtaining, or providing these emails.[29] He did not delete or alter any emails.

3. After Cain's firing, ClickMotive's network experienced problems

The difficulty of managing ClickMotive's entire IT infrastructure became immediately apparent. On Friday, the day after Cain was fired, a power outage brought down ClickMotive's entire network.[30] Thomas worked all morning to get the network back online. Eventually, the network was restored, but because several

---

24 ROA.2369-70 (Testimony of Andrew Cain).
25 ROA.2371 (Testimony of Andrew Cain).
26 ROA.2372-73 (Testimony of Andrew Cain).
27 ROA.2373 (Testimony of Andrew Cain).
28 ROA.2373 (Testimony of Andrew Cain).
29 ROA.489-494 (Government's Trial Brief).
30 ROA.2375 (Testimony of Andrew Cain).

systems were not connected to backup power, problems persisted.[31] Thomas logged in from home on Saturday and continued to work on the remaining issues.[32]

On Sunday, catastrophe again struck the ClickMotive network: outside hackers launched a denial-of-service attack that overwhelmed the company's firewall.[33] The firewall responded by refusing all outside traffic, making it impossible to log in to the network remotely.[34] Knowing that ClickMotive would be unable to function the next day with the network offline, Thomas drove to the office on Sunday evening and spent two hours diagnosing and fixing the problem.[35] By the time he finished, he had determined to resign. He left his keys, laptop, and electronic-entry badge behind, along with a letter of resignation and an offer to stay on as a consultant until the company found a replacement.[36]

4. "Damage" amidst the chaos

It is over this hectic weekend that Thomas is accused of damaging the ClickMotive network. After Friday's power outage, while he was repairing the

---

31 ROA.2386 (Testimony of Andrew Cain).
32 ROA.2306 (Testimony of Kevin Ates); ROA.2461 (Testimony of Chuck Easttom).
33 ROA.2311-2314 (Testimony of Kevin Ates).
34 *Id*.
35 *Id.* at 2314.
36 ROA.2033 (Testimony of Ray Myers).

damage to ClickMotive's systems, Thomas disabled the pager notification system that would otherwise continually report these errors.[37]

Late Friday night, a virtual machine responsible for making backups of the email server began reporting errors. On Saturday morning, Thomas powered down and deleted that virtual machine.[38] That same day, he consulted websites containing troubleshooting information about the virtual machine server software.[39]

On Sunday, Thomas deleted remotely stored backups of several servers.[40] He turned off jobs that automatically caused new remote backups to be made.[41]

While he was in the office troubleshooting network problems on Sunday night, Thomas changed a setting on a server involved in authentication to the VPN. The "network policy service" program was previously set to automatically restart itself if it stopped running; after the setting change, it needed to be manually restarted.[42] When another ClickMotive employee restarted the server on Monday,

---

37 ROA.1923 (Testimony of Ray Myers).
38 ROA.2505-06 (Testimony of Chuck Easttom).
39 ROA.2462-63 (Testimony of Chuck Easttom).
40 ROA.2089 (Testimony of Jeff Gonzalez).
41 *Id.*
42 ROA.2471-72 (Testimony of Chuck Easttom).

he had to restart this program to permit employees to log in to the network remotely using the VPN.[43]

Between Friday night and Sunday, Thomas deleted a handful of pages from the ClickMotive wiki related to various IT matters.[44] Finally, he changed a few settings on the email server, removing users from an email distribution group and removing the contact record for a third-party support representative.[45] There were no written company policies prohibiting any of this activity.[46]

5. ClickMotive quickly restores its systems

ClickMotive discovered all of these issues on Monday and addressed most of them immediately. On Monday, ClickMotive restored access to the VPN[47] and restored the deleted wiki pages from a backup made the preceding Thursday or Friday.[48] On Tuesday, ClickMotive reactivated the pager notification system.[49]

After Thomas deleted remote backups of various ClickMotive servers, they could not be retrieved.[50] However, redundant backups of the affected servers

---

43 ROA.2038-43 (Testimony of Jeff Gonzalez).
44 ROA.2005 (Testimony of Ray Myers).
45 ROA.2022-2024 (Testimony of Ray Myers).
46 ROA.2384 (Testimony of Andrew Cain) (no policy governing wiki deletions); ROA.1952 (Testimony of Ray Myers) (no policy governing changing settings on email server).
47 ROA.2005 (Testimony of Ray Myers).
48 ROA.2131 (Testimony of Marko Rangel).
49 ROA.2007 (Testimony of Ray Myers).
50 ROA.2058 (Testimony of Jeff Gonzalez).

existed locally on the servers themselves.[51] Those local backups were not disturbed.[52] ClickMotive did not subsequently suffer any data loss that necessitated the missing backups.[53] The virtual machine that Thomas deleted was only one of a "redundant pair."[54]

6. Thomas discusses ClickMotive's civil suit, and later the prosecution, with Cain

The following week, Thomas told Cain that he had "tinkered" with ClickMotive's system before resigning.[55] When Cain asked why, Thomas said that he didn't know.[56] He gave no indication that he believed he had done anything illegal.[57] When ClickMotive's lawyers served Thomas a civil petition for pre-suit discovery two weeks later, he was "confused and upset."[58] Neither Thomas nor Cain believed at the time that "anything Thomas had done merited a civil lawsuit . . . [m]uch less criminal charges."[59]

It was after being served this civil notice that Thomas first came to believe "that there might be any kind of penalties . . . for the things he [was] alleged to

---

51 ROA.2382-83 (Testimony of Andrew Cain).
52 ROA.2383 (Testimony of Andrew Cain).
53 ROA.2024 (Testimony of Ray Myers).
54 ROA.1982 (Testimony of Ray Myers).
55 ROA.2375 (Testimony of Andrew Cain).
56 *Id*.
57 ROA.2375, 2386-87 (Testimony of Andrew Cain).
58 ROA.2388 (Testimony of Andrew Cain).
59 ROA.2389 (Testimony of Andrew Cain).

have done."[60] Only upon being served with the civil pre-suit petition and then learning of the CFAA did Thomas express concern to Cain that he "might have broken the law."[61] But even a year after that, when Cain was approached by the FBI, he spoke freely and waived his right to counsel, because he believed Mike's "tinkering" was "harmless" and didn't believe he was "getting [his] good friend Mike Thomas in trouble."[62]

7. The charges and conviction

On September 11, 2013, Thomas was charged by a grand jury with a single felony count of "knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer" under § 1030(a)(5)(A) of the CFAA.[63] On June 8, 2016, he was convicted by a jury.[64] On June 22, 2016, Thomas moved for judgment of acquittal under Federal Rule of Criminal Procedure Rule 29.[65] On August 31, 2016, the district court entered its judgment, sentencing Thomas to time served plus 3 years' supervised release and ordering

---

60 ROA.2387 (Testimony of Andrew Cain).
61 ROA.2378 (Testimony of Andrew Cain).
62 ROA.2379 (Testimony of Andrew Cain).
63 ROA.17 (Indictment).
64 ROA.860 (Jury Verdict).
65 ROA.861-897 (Motion for Acquittal).

restitution in the amount of $131,391.21.[66] Thomas filed a timely notice of appeal on September 8, 2016.[67] On November 8, 2016, the district court denied Thomas's motion for judgment of acquittal.[68]

SUMMARY OF THE ARGUMENT

Michael Thomas had unlimited authorization to access, manage, and use ClickMotive's computer systems, and was given broad discretion in his exercise of that authority. His responsibilities involved deleting data, managing user privileges, and other activities that, without authorization, could constitute "damage" as that term is specifically defined by the CFAA. The central issue in this case is whether Thomas acted "without authorization" if he performed these same actions in a matter that was contrary to the company's interests.

The evidence was insufficient to support the jury's conclusion that Thomas acted without authorization, for three reasons. First, according to the plain language of the statute, a computer user can only cause "damage without authorization" if he has "no rights, limited or otherwise," to "impair" the "integrity or availability" of the data or system at issue. Because Thomas's had broad

---

66 ROA.1375-80 (Judgment).
67 ROA.1381-82 (Notice of Appeal).
68 ROA.1483-92 (Order on Motion for Acquittal).

authorization to manage ClickMotive's systems, including to "damage" them, his conduct cannot have been "without authorization."

Second, because the term "without authorization" is ambiguous, the Rule of Lenity requires the Court to apply the construction that favors Thomas. The interpretation of the term "without authorization" applied by the district court is broader than the alternative construction adopted by a plurality of circuit courts. The Court should resolve this ambiguity in favor of Thomas and reverse his conviction.

Third, because the district court's interpretation of "damage without authorization" fails to clearly define what conduct is prohibited or to adequately guide law enforcement, it renders the statute void for vagueness as applied to Thomas. The only evidence that Thomas's authorization was limited in any way was testimony about ClickMotive's employee policy prohibiting "destruction of valuable property." Such a broad policy cannot delineate minor infractions from felonies sufficiently to satisfy due process. It therefore cannot sustain Thomas's conviction.

ARGUMENT

I. Standard of Review

This is an appeal from the district court's denial of Thomas's motion for judgment of acquittal. On appeal from a motion for judgment of acquittal, this

Court reviews sufficiency-of-the-evidence claims *de novo*.[69] The evidence is viewed "in the light most favorable to the verdict to determine whether a rational trier of fact could have found that the evidence established their guilt beyond a reasonable doubt."[70] In doing so, neither the weight of the evidence nor the credibility of witnesses is reappraised.[71]

II. As an IT Administrator, Thomas Had Unlimited Access and Authorization to "Damage" ClickMotive's Systems

Thomas was ClickMotive's IT administrator. Unlike a "normal user" who "has limited authority and can only access certain files or take certain actions," Thomas had "authority to take any action," "change any setting," "access any data," and "delete any file" on ClickMotive's systems.[72] Many of his daily responsibilities involved "impairment" of ClickMotive's systems and therefore "damage" as that term is defined by the CFAA.[73] This broad authority extended to every system Thomas was charged with "damaging." Because the evidence is clear

---

69 *United States v. Harris*, 666 F.3d 905, 907 (5th Cir. 2012); *see United States v. Delagarza-Villarreal*, 141 F.3d 133, 139 (5th Cir. 1997); *United States v. Trevino*, 720 F.2d 395, 398 (5th Cir. 1983).

70 *Harris*, 666 F.3d at 907.

71 *United States v. Steen*, 634 F.3d 822, 825 (5th Cir. 2011).

72 ROA.1944-45 (Testimony of Ray Myers).

73 *See* 18 U.S.C. § 1030(e)(8) (defining "damage"); ROA.1487 (Order on Motion for Acquittal) (Thomas's "job responsibilities . . . included routinely deleting data and removing programs").

that ClickMotive did not explicitly limit this authorization, it is insufficient to support the jury's finding that Thomas acted "without authorization."

A. The CFAA defines "damage" broadly and neutrally

It is an offense under § 1030(a)(5)(A) of the CFAA to cause "damage without authorization" to a protected computer.[74] Despite its everyday connotations, the word "damage" has a neutral meaning under the CFAA. It simply means "any impairment to the integrity or availability of data, a program, a system, or information."[75]

This broad definition applies to innocent and culpable conduct alike. It is intuitive that "damage" is caused by installing malicious software to wipe out large portions of a company's database.[76] But when an employee deletes an email from her inbox or a file from her laptop, she too causes damage: the availability of that data is impaired.[77]

---

74 18 U.S.C. § 1030(a)(5)(A). The law also requires the "knowing" transmission of a "command," an element that is not at issue in this case. *See id*.

75 § 1030(e)(8).

76 *United States v. Shea*, 493 F.3d 1110, 1113 (9th Cir. 2007).

77 *Advanced Aerofoil Techs., AG v. Todaro*, No. 11 CIV. 9505 ALC DCF, 2013 WL 410873, at *5–9 (S.D.N.Y. Jan. 30, 2013). However, some jurisdictions have found that data is not "damaged" if another copy is readily available. *See, e.g., Instant Tech., LLC v. DeFazio*, 40 F. Supp. 3d 989, 1019 (N.D. Ill. 2014) *aff'd*, 793 F.3d 748 (7th Cir. 2015); *Grant Mfg. & Alloying, Inc. v. McIlvain*, No. 10-CV-1029, 2011 WL 4467767, at *8 (E.D. Pa. Sept. 23, 2011); *Cheney v. IPD Analytics, L.L.C.*, No. 08-CV-23188, 2009 WL 1298405, at *6 (S.D. Fla. Apr. 16, 2009); *Dana Ltd. v. Am. Axle & Mfg. Holdings, Inc.*, No. 1:10-CV-450, 2012 WL 2524008, at *6 (W.D. Mich. June 29, 2012).

In particular, IT professionals such as Thomas "are undoubtedly authorized to 'damage' . . . computer systems as part of their daily tasks."[78] Their responsibilities include a wide array of conduct that courts have found to constitute "damage," including creating and deleting user accounts,[79] deleting stored information,[80] and restricting access to their company network.[81]

B. There were no restrictions on Thomas's authority to "damage" ClickMotive's systems

Like all IT administrators, Thomas's daily responsibilities involved authorized "damage" to his employer's systems. As the district court found, Thomas "had unlimited access to all of ClickMotive's IT systems and was responsible for routinely deleting data, removing programs, and taking systems offline for diagnosis and maintenance."[82] There was no ClickMotive policy, written or oral, specifically defining the limits of the IT staff's discretion or authority.[83]

---

78 *United States v. Stratman*, No. 4:13-CR-3075, 2013 WL 5676874, at *4 (D. Neb. Oct. 18, 2013) (unpublished).

79 *United States v. Middleton*, 231 F.3d 1207, 1208 (9th Cir. 2000).

80 *Beta Tech., Inc. v. Meyers*, No. CIV.A. H-13-1282, 2013 WL 5602930, at *4 (S.D. Tex. Oct. 10, 2013).

81 *United States v. Fowler*, 445 F. App'x 298, 300 (11th Cir. 2011).

82 ROA.1483

83 ROA.1951 (Testimony of Ray Myers).

Thomas's unrestricted authority extended to every system at issue in this case. Thomas managed the server that ran ClickMotive's virtual machines.[84] It is undisputed that he had the authority to delete (or "destroy") virtual machines in the scope of his work.[85] In fact, it was Thomas who devised the informal procedure by which virtual machines at ClickMotive should be deleted.[86] It was also "customary" for Thomas to delete virtual machines;[87] he deleted several in the months prior to his termination.[88] Only the last deletion was alleged to have been unauthorized.

Thomas was the administrator of ClickMotive's wiki.[89] Every employee at ClickMotive, Thomas included, was "permitted to remove information from the wiki."[90] Employees "removed information from the company wiki from time to time."[91] The company "maintained no policy for when it was permissible to delete content from the wiki."[92] It was "up to the user's discretion."[93]

---

84 A virtual machine is software that emulates a physical computer. Several virtual machines can be hosted on a single physical server.

85 ROA.1983

86 ROA.2017-18, 2061, 2090

87 ROA.1980, 2301-02

88 ROA.1983

89 ROA.1947, 2005-07.

90 ROA.1953

91 *Id.*

92 ROA.2384

93 *Id.*

Thomas was responsible for managing ClickMotive's Microsoft Exchange email server.[94] This job required "adding and removing users from the system" and "chang[ing] users' access to various groups."[95] This server also operated the pager notification system; Thomas managed the alerts that went to pagers.[96] ClickMotive's policies did not cover "when the IT operations manager could change the Microsoft Exchange settings."[97]

Thomas was the administrator of ClickMotive's network and firewall,[98] as well as the VPN that employees used to connect to the network remotely.[99] Thomas had authority to disable network services, including the network policy service.[100]

Thomas was responsible for managing the company's backups.[101] This job necessarily involved deleting backup files periodically.[102] Similarly, he was

---

94 ROA.1948
95 ROA.2681
96 ROA.2681
97 ROA.1952
98 ROA.1946
99 ROA.2313-17
100 ROA.2095 (testimony of ClickMotive employee Jeff Gonzalez that disabling network policy service was reasonable for some purposes, including "troubleshooting purposes").
101 ROA.1074
102 *Id*. *See also* ROA.909 (Government agrees Thomas was authorized to delete "obsolete materials.").

responsible for wiping data off of employees' laptops following their termination.[103]

All of these responsibilities involved "impairment to the integrity or availability" of ClickMotive "data," "program[s]," "information," or "systems." Thomas was therefore, as a matter of law, authorized to "damage" ClickMotive's systems.

C. The district court erred in concluding that Thomas was never authorized to cause "damage"

The evidence is insufficient to support the district court's conclusion that Thomas "was not authorized to damage ClickMotive's system."[104] The undisputed evidence above establishes that he was, as does the district court's own assessment of it: Thomas "was responsible for routinely deleting data, removing programs, and taking systems offline for diagnosis and maintenance."[105] All of these activities cause CFAA "damage."

The court nonetheless concludes that Thomas was never authorized to cause "damage." Despite accurately summarizing the evidence, the court misapplies the law in two ways. First, it conflates the statute's "damage" and "authorization"

---

103 ROA.2141
104 ROA.1487
105 ROA.1483

elements. Second, it defines "damage" by reference to "economic value," improperly expanding the statutory definition.

1. Damage may be authorized or unauthorized

The district court erroneously redefines "damage" to exclude "permitted, routine data deletions."[106] This reading is contrary to the plain language of the statute, which defines damages as "*any* impairment to the integrity or availability of data, a program, a system, or information."[107] Whether the damage is authorized is a separate question and the determinative issue in this case.

By incorporating "permission" into the "damage" inquiry, the court renders the modifier "without authorization" redundant. If impairment of data is only "damage" when it is unauthorized, Congress need not have specified that the statute prohibits "damage *without authorization*."[108] "A statute should be construed so that effect is given to all its provisions, so that no part will be inoperative or superfluous, void or insignificant."[109] Because the district court's interpretation of "damage" renders "without authorization" inoperative, it should be rejected.

---

106 ROA.1488

107 § 1030(e)(8) (emphasis added).

108 § 1030(a)(5)(A) (emphasis added).

109 *Hibbs v. Winn*, 542 U.S. 88, 101 (2004).

2. Economic harm is irrelevant to the damage inquiry

The district court also errs by defining damage by reference to economic harm, distinguishing "routine, permitted deletions" from those that "negatively impact the economic value of the computer system."[110] Neither statute nor caselaw constrains "damage" to the impairment of valuable or current data. Section 1030(a)(5)(A) prohibits "damage without authorization," regardless of harm.[111] Economic harm, which the CFAA terms "loss," is relevant only to punishment:[112] it defines the boundary between misdemeanor and felony conduct[113] and is a factor in the applicable sentencing guidelines.[114]

To support its erroneous conclusion that only valuable data can be "damaged," the district court cites a Southern District of New York case, *United States v. Yücel*.[115] *Yücel* is inapposite. The defendant in *Yücel* surreptitiously installed "remote access tools" on the computers of unsuspecting strangers for the purpose of stealing their credit card information.[116] He argued that merely

---

110 ROA.1488

111 *Compare* § 1030(c)(4)(B)(i) (prescribing a maximum 10-year prison term for a violation of (a)(5)(A) resulting in a "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value") *with* § 1030(c)(4)(G)(i) (prescribing up to 1 year imprisonment for a violation of "any other offense" under (a)(5)(A) regardless of loss).

112 *Id*.

113 *Id*.

114 U.S. SENTENCING GUIDELINES MANUAL § 2B1.1 (U.S. SENTENCING COMM'N 2016).

115 ROA.1488; *see* 97 F. Supp. 3d. 413, 416 (S.D.N.Y. 2015).

116 97 F. Supp. 3d at 421.

installing the software (without then using it) did not cause "damage."[117] *Yücel* held that it did, citing a Senate Report which said that "damage" was intended to encompass situations where "intruders . . . alter existing log-on programs" for the purpose of stealing passwords, then later "restore[] the altered log-on file to its original condition."[118]

To the extent that *Yücel*'s holding relies on the finding that the remote access tool's presence "negatively impact[s] the economic value of the computer system,"[119] it is wrongly decided. Nothing in the statute suggests that "damage" encompasses economic value. Rather, it is clear from the CFAA's structure that it does not—the statute explicitly distinguishes "damage" to a computer[120] from the resulting economic "loss."[121] *Yücel* cites no support for its "economic value" construction of "damage," nor does the district court.[122] In any case, *Yücel*'s dubious construction is not limiting: it merely adds diminution of economic value to the list of things which may constitute "damage."[123]

The statute is clear: "damage" encompasses *any* impairment to the integrity or availability of data, no matter the data's value or the user's identity or purpose.

---

117 97 F. Supp. 3d at 421.
118 *Id*. at 420.
119 *Id*.
120 § 1030(e)(3).
121 § 1030(e)(11).
122 *See* ROA.1487-88 (Rule on Motion for Acquittal).
123 *See Yücel*, 97 F. Supp. 3d at 420.

When "damage" is given the appropriately broad construction, it plainly encompasses Thomas's authorized responsibilities.

III. The District Court Erred in Concluding that Thomas Acted "Without Authorization"

When a court is confronted with an undefined term in a statute, those words "will be given their plain meaning absent ambiguity."[124] In the CFAA, the plain, ordinary meaning of "without authorization" is narrow: to be liable for accessing or damaging a computer "without authorization, "[125] a computer user must act with "no rights, limited or otherwise." This definition has been adopted by a plurality of circuit courts, out of a concern that broader interpretation would circumvent Congress's will, dilute other express statutory language, and encompass the ordinary conduct of many other computer users.

The district court relies on a different construction, holding that Thomas acted "without authorization" because he violated broad proscriptions in ClickMotive's employee handbook. Even if this interpretation is plausible, it is at odds with the narrower construction embraced by several circuit courts. Faced with a "choice . . . between two readings of what Congress has made a crime, it is

---

[124] *United States v. Reed*, 375 F.3d 340, 344 (5th Cir. 2005) (quoting *Tex. Food Indus. Ass'n v. United States Dep't of Ag.*, 81 F.3d 578, 582 (5th Cir. 1996)).

[125] *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009).

appropriate, before [choosing] the harsher alternative, to require that Congress should have spoken in language that is clear and definite."[126]

The Rule of Lenity therefore requires this Court to resolve the conflict by adopting a narrower construction of "without authorization" that favors Thomas. By that construction, Thomas cannot be criminally liable for causing "damage without authorization" because he was authorized to cause "damage" as the CFAA specifically defines that term.

A. A defendant acts "without authorization" if he has "no rights, limited or otherwise"

A computer user acts "without authorization" within the meaning of the CFAA when he does something he "has no rights, limited or otherwise" to do.[127] Applying this construction to § 1030(a)(5)(A), "one who is authorized to access a system, but not authorized to damage it, violates the statute by intentionally damaging it 'without authorization.'"[128] Therefore, a defendant who is authorized to both access and to damage a computer cannot be criminally liable under § 1030(a)(5)(A) if he causes damage that offends a broad corporate policy.

---

126 *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 206 (4th Cir. 2012) (quoting *United States v. Universal C.I.T. Credit Corp.*, 344 U.S. 218, 221-22 (1952)).

127 *Brekka*, 581 F.3d at 1133.

128 *United States v. Stratman*, No. 4:13-CR-3075, 2013 WL 5676874, at *1 (D. Neb. Oct. 18, 2013).

1. "Access without authorization" cases demonstrate the plain meaning of "without authorization"

This construction of "without authorization" has been widely adopted by circuit courts in "access without authorization" cases. The Ninth Circuit in *Brekka*, for example, determined that the "ordinary, contemporary, common meaning" of "authorization" means that "a person who uses a computer 'without authorization' has no rights, limited or otherwise, to access the computer in question."[129] The Second, Fourth, and Sixth Circuits agree with *Brekka* that "without authorization" means to lack permission or sanction entirely.[130]

Of the circuit courts, only the Seventh has applied a broader construction in a "damage without authorization" case. *International Airport Centers, L.L.C. v. Citrin* involved an employee who decided to start a business competing with his employer.[131] Before quitting, he deleted valuable files from his company laptop.[132] The Seventh Circuit held that the defendant's authorization terminated when he

---

[129] *Brekka*, 581 F.3d at 1133 (quoting *Perrin v. United States*, 444 U.S. 37, 42 (1979).

[130] *See United States v. Valle*, 807 F.3d 508, 524 (2d Cir. 2015) (citing *Brekka*, 581 F.3d at 1133); *WEC*, 687 F.3d at 204 (also citing *Brekka*, at 1133); *Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am.*, 648 F.3d 295, 303-04 (6th Cir. 2011) (same).

[131] *Int'l Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418, 419 (7th Cir. 2006).

[132] *Id.*

"resolved to destroy files . . . in violation of [his] duty of loyalty" and therefore that these deletions were unauthorized.[133]

Citrin has been rejected explicitly by the Fourth and Ninth Circuits and implicitly by the Second and Sixth, all of which instead adopted *Brekka*'s narrower construction. As the Ninth Circuit pointed out, the cessation-of-agency interpretation of "authorization" nullifies other parts of the statute prohibiting access *in excess* of authorization.[134] The Court explained that by prohibiting "exceeding authorized access" in addition to "access without authorization," Congress specifically intended to address situations where a user has some authority but oversteps its bounds. To read a duty-based limitation into the "without authorization" offense would subvert this intent.[135]

"Without authorization" should be given the same meaning in the "damage without authorization" context: "having no rights, limited or otherwise." This construction is necessary to avoid constitutional notice and vagueness questions, as shown below in Section II(C). It also promotes consistent application of § 1030(a)(5)(A) in two ways: (1) it accords with the vast majority of existing

---

133 *Id.* at 420.

134 *Brekka*, 581 F.3d at 1133. *See* 18 U.S.C. § 1030(a)(2), (a)(4).

135 *Id.* The Fourth Circuit similarly expressed a concern that *Citrin*'s overly expansive interpretation "has far-reaching effects unintended by Congress." *WEC*, 687 F.3d at 206.

1030(a)(5)(A) opinions; and (2) it gives uniform meaning to "without authorization" throughout § 1030 offenses, making the statute internally coherent.

2. The plain meaning of "without authorization" is compelled in damage cases to make "without authorization" consistent across the statute

The meaning of "without authorization" is definitively established in the "access" cases discussed above, and must be applied consistently across the statute. "A term appearing in several places in a statutory text is generally read the same way each time it appears."[136] Absent a clear indication that "without authorization" was "employed in the different parts of the act with different intent,"[137] the phrase must be accorded the same narrow interpretation applied by the Second, Fourth, Sixth, and Ninth Circuits in "access" cases.

The fact that Congress did not define a "damage *in excess* of authorization" offense is not an invitation for the courts to invent one.[138] "[W]here Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion."[139] It must therefore be presumed that Congress intentionally defined a scheme that punishes "damage"

---

136 *Ratzlaf v. United States*, 510 U.S. 135, 143 (1993).

137 *Helvering v. Stockholms Enskilda Bank*, 293 U.S. 84, 87 (1934).

138 *See Clark v. Martinez*, 543 U.S. 371, 378 (2005) ("To give these same words a different meaning for each category would be to invent a statute rather than interpret one.").

139 *Gozlon-Peretz v. United States*, 498 U.S. 395, 404 (1991).

only when the individual was without any authority to impair the protected computer.

3. The plain meaning of "without authorization" accords with the majority of existing (a)(5)(A) decisions

Finally, a narrow construction of "damage without authorization" is consistent with the application of § 1030(a)(5)(A) in existing cases. Section 1030(a)(5)(A) cases follow a handful of common fact patterns. Most involve employees (or contractors) who damage their employers' systems after their employment is terminated or suspended.[140] Others involve employees who install malware[141] expressly intended to damage their employers' systems after they are terminated.[142] Still others involve damage by employees who were never authorized, under any circumstances, to cause the sort of damage at issue.[143] In each of these situations, the defendants retained no rights whatsoever to cause damage, and therefore the enforcement of § 1030(a)(5)(A) against them did not extend beyond the plain meaning of "without authorization."

---

[140] *See, e.g., United States v. Kim*, 677 F. Supp. 2d 930, 932 (S.D. Tex. 2009) (damage occurred after defendant's authorization revoked by suspension); *United States v. Middleton*, 231 F.3d 1207, 1208 (9th Cir. 2000) (same).

[141] "Malware" is a portmanteau of "malicious" and "software," and generally refers to software designed to damage, disrupt, or disable a computer system.

[142] *See, e.g., United States v. Shea*, 493 F.3d 1110, 1117 (9th Cir. 2007); *United States v. Sullivan*, 40 F. App'x 740, 741 (4th Cir. 2002); *United States v. Lloyd*, 269 F.3d 228, 233 (3d Cir. 2001).

[143] *See, e.g., Beta Tech., Inc. v. Meyers*, No. CIV.A. H-13-1282, 2013 WL 5602930, at *4 (S.D. Tex. Oct. 10, 2013).

Notably, this interpretation is also consistent with *United States v. Yücel*,[144] the Southern District of New York case relied upon by the district court and the Government for the proposition that § 1030(a)(5)(A) is not impermissibly vague. Just as many of the defendants in the above cases lacked authority to cause any damage, it was beyond question in *Yücel* that the defendant was never authorized to access, much less install intrusive software on, the computers of total strangers.[145]

B. Because "without authorization" is ambiguous, "damage without authorization" must be narrowly construed

While the proposed construction of "without authorization" has been adopted by a plurality of circuit courts, it is not the only plausible interpretation of the term. Section 1030(a)(5)(A) has been interpreted in multiple ways. First, as prohibiting damage by someone with no rights, limited or otherwise, to cause damage.[146] Second, as prohibiting damage by a defendant who "has not been

---

144 97 F. Supp. 3d 413 (S.D.N.Y. 2015).

145 *Id.* at 422.

146 *See Stratman*, 2013 WL 5676874, at *4; *Cornerstone Staffing Sols., Inc. v. James*, No. C 12-01527 RS, 2013 WL 12124430, at *9 (N.D. Cal. Oct. 21, 2013) (holding that, under *Brekka*, "'damage without authorization' under § 1030(a)(5)(A) [does not] prohibit actions by authorized employees); *Advanced Aerofoil Techs., AG v. Todaro*, No. 11 CIV. 9505 ALC DCF, 2013 WL 410873, at *5-9 (S.D.N.Y. Jan. 30, 2013) (employee who deleted valuable information from his laptop prior to quitting to join competing enterprise did not act "without authorization").

permitted by the victim to cause *that* damage."[147] And third, as prohibiting an authorized user from causing damage in violation of his duty of loyalty.[148]

Because § 1030(a)(5)(A) is susceptible to multiple constructions, this Court must use ordinary tools of statutory construction to resolve the conflict. If no single construction is compelled by that analysis, the statute is ambiguous, and the Rule of Lenity requires this Court to adopt the narrower construction offered by Thomas.

1. The Rule of Lenity requires ambiguous criminal statutes to be construed narrowly

The Rule of Lenity is simple: when a criminal statute is ambiguous, that ambiguity must be resolved in favor of the defendant until Congress opts to speak clearly on the matter.[149] The rule recognizes that courts are not "mindreader[s]."[150] If the ordinary tools of statutory construction leave "reasonable doubt" between competing constructions, the Rule of Lenity mandates that the court adopt the one that favors the defendant.[151]

---

147 *Yücel*, 97 F. Supp. 3d at 422 (emphasis added).

148 *Citrin*, 440 F.3d at 420.

149 *United States v. Orellana*, 405 F.3d 360, 370-71 (5th Cir. 2005) (quoting Jones v. United States, 529 U.S. 848, 849-50 (2000)); *see United States v. Valle*, 807 F.3d 508, 523-28 (2d Cir. 2015).

150 *United States v. Santos*, 553 U.S. 507, 515 (2008).

151 *Orellana*, 405 F.3d at 370-71.

A statute is ambiguous when it is open to two plausible, competing interpretations.[152] The mere availability of multiple constructions does not render a statute ambiguous.[153] But when the plain language of the statute does not conclusively support one meaning over the other, courts are obligated to use all the tools at their disposal to resolve the conflict.[154] If doubt still remains after such an inquiry, the court is "required by the rule of lenity to adopt the interpretation that favors the defendant."[155]

2. The Rule of Lenity is a due process requirement

The Rule of Lenity is more than just a rule of statutory construction. It embodies the principle that fair notice is "a right of federal constitutional dimension, grounded in the due process guarantee" and requires that a criminal statute "give fair warning of the conduct that it makes a crime."[156] It is thus a crucial safeguard that protects the liberty interests of criminal defendants when a statute fails to unambiguously pronounce the conduct it targets.

---

[152] *United States v. Hoang*, 636 F.3d 677, 682 (5th Cir. 2011) (quoting *In re Condor Ins. Ltd.*, 601 F.3d 319, 321 (5th Cir. 2010)).

[153] Nor does a split in judicial authority interpreting the same term. *Hoang*, 636 F.3d at 682. But such a divide may nonetheless be "reveal[ing,]" *id.*, particularly to the extent that it provides insight into how courts have grappled with indefinite statutory language.

[154] *Orellana*, 405 F.3d at 371.

[155] *Valle*, 807 F.3d at 526; *see also United States v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2012).

[156] *Lurie v. Wittner*, 228 F.3d 113, 126 (2d Cir. 2000) (quoting *Bouie v. City of Columbia*, 378 U.S. 347, 350 (1964)); *see also Nosal*, 676 F.3d at 863 ("The rule of lenity not only ensures that citizens will have fair notice of the criminal laws, but also that Congress will have fair notice of what conduct its laws criminalize.").

When confronted with an ambiguous statute, courts therefore must adopt the construction favoring the defendant to alleviate constitutional fair notice problems.[157] To the extent that the CFAA's "damage without authorization" provision is ambiguous, its broader constructions do not provide the fair notice required by the constitution. The Rule of Lenity therefore requires this court to construe the term narrowly, such that a defendant acts "without authorization" only when he has "no rights, limited or otherwise."

C. The District Court's Authorization Analysis Raises Constitutional Notice Problems

The district court adopted a broader construction of "without authorization" than this, finding that Thomas acted "without authorization" for three reasons. First, it held that Thomas was "not authorized to damage ClickMotive's system" for any purpose.[158] This conclusion is in error for the reasons discussed above in Section I. Second, the district court held that Mr. Thomas "caused damage 'without authorization' because ClickMotive did not give Thomas permission to delete files without following proper procedures, disable alerts, or change user permissions in a manner that harmed ClickMotive's system."[159]

---

157 *See United States v. Lanier*, 520 U.S. 259, 266 (1997).
158 ROA.1487
159 ROA.1487

This holding asserts two additional reasons why Thomas acted "without authorization." The first, that he failed to follow "proper procedures" when deleting files. The second, that he did not have permission to "delete files," "disable alerts," or "change user permissions" "in a manner that harmed ClickMotive's system." Neither rule would provide defendants with adequate notice of what conduct is criminal. The court's analysis therefore violates the Rule of Lenity and should be rejected.

1. *The court's "proper procedure" improperly criminalizes an employee's deviation from his own prior practice*

By basing its authorization determination on Thomas's failure to follow "proper procedure," the district court dramatically expands the potential scope of criminal liability under § 1030(a)(5)(A). The procedure in question was an unwritten, informal practice devised by Thomas. If criminal liability can turn on nothing more than a change in an employee's habits, defendants can never be certain which changes will criminalize their conduct.

The evidence that Thomas deleted files without following "proper procedure" relates exclusively to his deletion of a virtual machine. Government witnesses testified that "normal procedure" for deleting a virtual machine was to first "create a[nother] functioning version of it," test that new version, then "pull

the other machine off-line."[160] The IT staff's "patterns of previous activity" suggested that they (Thomas and Cain) would typically shut down virtual machines for "approximately" a week before deleting them.[161] This practice "was not always observed," though during the two preceding months (the only period for which records existed)[162] it was observed "almost strictly" by Thomas.[163] It is undisputed that it was nonetheless permissible for machines to be "deleted immediately" once replaced.[164]

This "normal procedure" for deleting virtual machines was not written down anywhere.[165] It was not dictated by ClickMotive,[166] which had no policy regarding the deletion of virtual machines.[167] Rather, it was an informal practice devised by Thomas himself.[168] Thus, the district court essentially held that felony CFAA liability may be predicated on a change to the defendant's own habits.

a. Authorization defined by past practice defies the statute

Defining an employee's authorization according to his own past practice introduces a host of problems. First, nothing in the text or interpretive history of

---

160 ROA.2017
161 ROA.2342
162 ROA.2714 (first entry in virtual machine log file dated October 4, 2011).
163 ROA.2342
164 ROA.2018
165 ROA.2024-25
166 ROA.2090
167 ROA.2024-25
168 *Id.*

the CFAA suggests that a defendant can define the scope of his own authorization.[169] Rather, "[i]t is the *employer's* decision to allow or to terminate an employee's authorization to access a computer that determines whether the employee is with or 'without authorization.'"[170]

The evidence is clear that Thomas "was given broad responsibilities for managing ClickMotive's systems,"[171] including to determine when and how virtual machines should be deleted. When an employee is left to determine how to carry out responsibilities, exercising that discretion in a particular way does not render other approaches unauthorized. To hold otherwise would violate due process.

b. Authorization defined by past practice provides inadequate notice to criminal defendants

The court's "proper procedure" analysis also provides inadequate notice to criminal defendants. If an employee's authorization is circumscribed by his own past practice, he cannot be certain when deviating from that practice is criminal.

An example illustrates the problem: A salesperson receives emails from leads weekly. In the five years since she started her job, her unwavering practice has been to keep these emails for three months each, because sometimes it takes that long to land the sale.

---

169 *Cf. Brekka*, 581 F.3d at 1135 (applying the same reasoning to violations of common law duty of loyalty).

170 *Brekka*, 581 F.3d at 1133 (emphasis added).

171 ROA.1944

The salesperson surely would never suspect that, if she begins deleting these emails after only two weeks, she'll have committed a crime. But the court's analysis does not distinguish that case from this one. In each, the employee is given authority to delete data, with no express limitations on when or how. Deleting the data might be considered "harmful" to the employer in either case. And neither employee has reason to believe that deviating from past practice will invoke criminal liability.

c. Thomas did not have notice that his conduct was otherwise criminal

According to the district court, Thomas had sufficient notice that his conduct was criminal because he "knew or reasonably should have known that . . . causing that damage was in furtherance of or to perpetrate a crime, i.e., destroying ClickMotive's property."[172] In support of this conclusion, the court cites this Court's ruling in *U.S. v. John*.[173] The defendant in *John*, an account manager at Citigroup, obtained confidential customer account information and, in violation of company policy, provided it to her co-conspirators to permit them "to incur fraudulent charges."[174] She was convicted of "exceeding authorized access" to

---

172 ROA.1487

173 *United States v. John*, 597 F.3d 263 (5th Cir. 2010).

174 *Id. at* 269.

Citigroup's customer accounts under § 1030(a)(2), as well as credit card fraud (and related conspiracy charges) under 18 U.S.C. § 371 and 18 U.S.C. § 1029(a).

The defendant in *John* argued that the CFAA's prohibition on "exceed[ing] authorized access" was ambiguous and should not be interpreted to apply where a defendant merely misuses information she is authorized to access.[175] This Court declined to apply the defendant's interpretation, holding that § 1030(a)(2) raises no fair notice concerns where the access in question is "in furtherance of a criminally fraudulent scheme."[176]

Citing *John*, the district court found that Thomas "knew or reasonably should have known" that "destroying ClickMotive's property" was "a crime" and therefore that his CFAA prosecution raised no notice problems.[177] But the holding in *John* was premised on the fact that the defendant's conduct was "*both* in violation of an employer's policies *and* . . . part of an illegal scheme" criminalized by a separate statute.[178] John did not argue that she had no notice that credit card fraud, or acts in furtherance of a fraudulent conspiracy, were criminal. Credit card fraud is obviously a crime.

---

175 *Id. at* 271.
176 *Id. at* 273.
177 ROA.1487
178 *John*, 597 F.3d at 273.

The district court does not identify what separate criminal statute Thomas should have known he was violating. Nor was Thomas charged with one. If the court's point is simply that Thomas should have known that his conduct violated § 1030(a)(5)(A), it begs the question: the conduct violated the statute if Thomas was on notice that it was unauthorized; Thomas was on notice that the conduct was unauthorized because it violated the statute. This circular construction should be rejected, particularly where it determinative of felony liability.

2. ClickMotive's General Policy Provided Inadequate Notice of Criminal Liability

The court's finding that Thomas was not permitted to act "in a manner that harmed ClickMotive's system" raises still graver notice issues. It is based either on a broad ClickMotive policy prohibiting employees from "causing harm" to the company or a general duty of loyalty. Because Thomas did not have notice that a violation of either would result in criminal liability, his conviction cannot be sustained.

a. Only a general company policy prohibited "destruction of valuable things"

The court's conclusion that Thomas was not permitted to "delete files," "disable alerts," or "change user permissions" "in a manner that harmed

ClickMotive's system"[179] has only one basis in the record: the testimony of ClickMotive's Chief Technology Officer, Ray Myers. According to Myers, ClickMotive's employee handbook, which was never introduced into evidence, contained a "blanket policy of you can't do things that interfere with the normal course of business."[180] He also characterized the proscription as a "policy [that] says in some way that you cannot destroy company property"[181] and as one of "plenty of policies against destruction of valuable things."[182]

Even if this amorphous policy can be interpreted to apply to deletion of ClickMotive's data, there is no evidence that Thomas's broad authorization to "delete any file"[183] and "change any setting"[184] on ClickMotive's systems was limited by the company. There were no policies governing when Thomas could change settings on the email server,[185] delete information from the wiki,[186] delete backups,[187] delete a virtual machine,[188] or disable pager alerts.[189] There were, in fact, no policies at all specific to the IT department.[190]

---

179 ROA.1487
180 ROA.1952
181 ROA.1952:15-16
182 ROA.1951
183 ROA.1945
184 *Id.*
185 ROA.1952
186 ROA.2384
187 ROA.1951
188 ROA.1951-52

b. ClickMotive's "blanket policy" is insufficient to provide notice of criminal liability

To satisfy the Rule of Lenity, a statute must "give fair warning of the conduct that it makes a crime."[191] An employee policy broadly prohibiting "destruction of company property" is insufficient to notify employees when their otherwise-authorized computer use becomes criminal.

Thomas was "was responsible for routinely deleting data" and "removing programs."[192] When, according to ClickMotive's "blanket policy," did the deletion of data amount to "destruction of company property" and therefore criminal conduct? The record below demonstrates the difficulty of answering the question: while Myers testified unequivocally that "destruction of computer programs is wrong,"[193] the district court found that doing so was one of Thomas' "job responsibilities."[194]

Not only did ClickMotive's policy fail to identify what data is too "valuable" to delete, it explicitly limited the punishment for violations to "disciplinary action, up to and including termination."[195] If the bounds of criminal

---

189 ROA.1952
190 ROA.1951
191 *Bouie v. City of Columbia*, 378 U.S. 347, 350 (1964).
192 ROA.1483
193 ROA.1952
194 ROA.1483
195 ROA.1950

liability are to be determined by a private policy, surely it must be a policy whose language does not exclude criminal liability.

D. The narrower construction of "damage without authorization" must be applied to avoid notice problems

United States v. Valle demonstrates the courts' robust application of the Rule of Lenity to CFAA cases, even when faced with far more specific restrictions and far greater harms.[196] The defendant in *Valle* was a New York City police officer who fantasized in online forums about his "desire to kidnap, rape, torture, and eat women whom he knows."[197] Valle exploited his access to a police database to obtain the personal information of a high school classmate whom he had discussed kidnapping with an online acquaintance.[198] He was charged with "exceeding authorized access" under § 1030(a)(2) for violating a department rule prohibiting access for non-law enforcement purposes.[199]

The Second Circuit reversed Valle's CFAA conviction. It recognized that NYPD policy specifically prohibited Valle from accessing the police database for non-law enforcement purposes.[200] Nonetheless, it found that Valle did not "exceed authorized access" because he accessed only information that he was authorized to

---

196 *United States v. Valle*, 807 F.3d 508, 511 (2d Cir. 2015).
197 *Id. at* 516.
198 *Id. at* 513.
199 *Id. at* 524.
200 *Id. at* 524.

obtain *for some purpose*, even though his actual purpose violated department policy.[201]

As the Second Circuit cautioned in *Valle*, "we must not forget that in a free and functioning society, not every harm is meant to be addressed with the federal criminal law."[202] If Thomas's actions violated ClickMotive's policy against "interfering with the normal course of business,"[203] he may well have committed a tort—perhaps even civilly violated the CFAA. But when felony charges are the stakes, a broad policy such as ClickMotive's is insufficient to put an IT administrator on notice of when his otherwise-authorized activities are "without authorization."

IV. The Evidence is Insufficient to Sustain Thomas's Conviction Because the District Court's Construction Renders § 1030(a)(5)(A) Void for Vagueness as Applied to Thomas's Conduct

To the extent that "authorization" within the meaning of § 1030(a)(5)(A) can be construed to encompass Thomas's contractual or common law obligations to ClickMotive, the statute is void for vagueness as applied here and cannot support Thomas's conviction. The Vagueness Doctrine is closely related to the Rule of Lenity and likewise derives from the Due Process Clause of the Fifth

---

201 *Id. at* 523-24.
202 *Valle*, 807 F.3d at 511.
203 ROA.1952

Amendment.[204] It "bars enforcement of a statute which either forbids or requires the doing of an act in terms so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application."[205]

The Vagueness Doctrine has two prongs.[206] The first requires that "a penal statute define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited."[207] The second requires that "the statute must establish minimal guidelines to govern law enforcement."[208] "[T]he constitutionality of a vague statutory standard is closely related to whether that standard incorporates a requirement of *mens rea*."[209]

A. ClickMotive's employee policy did not sufficiently define what conduct was criminally prohibited

When an employee has essentially unlimited authority to manage a computer system, a corporate policy of general applicability cannot adequately define the limits of that authority. The appropriate analysis is illustrated by *United States v. Drew*, a Central District of California case in which a defendant was charged with

---

204 *United States v. Lanier*, 520 U.S. 259, 266 (1997); *United States v. Williams*, 553 U.S. 285, 304 (2008).

205 *Lanier*, 520 U.S. at 266.

206 *See United States v. Drew*, 259 F.R.D. 449, 463 (C.D. Cal. 2009) (citing *Kolender v. Lawson*, 461 U.S. 352, 357–58 (1983)).

207 *Id.*

208 *Id*. (quoting *Smith v. Goguen*, 415 U.S. 566, 574 (1974)).

209 *Colautti v. Franklin*, 439 U.S. 379, 395 (1979).

"access without authorization" under § 1030(a)(2)(C) for violating a website's terms of service.[210]

The defendant in *Drew* conspired with others to create a fake profile on a social networking site for the purpose of harassing a 13-year-old girl, her daughter's classmate.[211] In the fake profile, Drew "posted a photograph of a boy without the boy's knowledge or consent," in violation of the site's terms of service.[212] The conspirators used the profile to lure their target into an online romance and then cruelly harass her until she killed herself.[213] The site's terms of service provided that users were "only authorized to use" the site if they agreed to abide by its terms.[214] Drew was convicted on the theory that she accessed the site after her violation of the terms terminated her authorization.[215]

The *Drew* court identified four "definitional" infirmities in basing criminal liability "upon the conscious violation of a website's terms of service."[216] Though the offense and the offended policy were different in *Drew*, the same notice problems arise in this case.

---

210 *See Drew*, 259 F.R.D. at 449.
211 *Id. at* 452.
212 *Id. at* 453.
213 *Id. at* 452.
214 *Id. at* 462.
215 *Id. at* 453.
216 *Drew*, 259 F.R.D. at 464.

1. Section 1030(a)(5)(A) does not provide notice that it criminalizes breach of employment polices

The *Drew* court found that "the language of section 1030(a)(2)(C) does not explicitly state (nor does it implicitly suggest) that the CFAA has criminalized breaches of contract in the context of terms of service."[217] "Thus, while 'ordinary people' might expect to be exposed to civil liabilities for violating a contractual provision, they would not expect criminal penalties."[218]

The same is true in this case. The CFAA does not define "without authorization,"[219] much less "explicitly state" or even "suggest" that § 1030(a)(5)(A) "has criminalized breaches of contract" such as employment agreements.[220]

While IT administrators "might expect to be exposed to civil liabilities" for violating their employment agreements "they would not expect criminal penalties."[221] The evidence shows that Thomas did not expect them. The Government called Andrew Cain to describe Thomas's state of mind at the time of

---

217 *Drew*, 259 F.R.D. at 464.
218 *Id.* at 464.
219 *See Valle*, 807 F.3d at 523.
220 *See Drew*, 259 F.R.D. at 464.
221 *See id.*

the offense.[222] Cain testified that Thomas did not believe that his actions could give rise even to civil liability, "much less criminal charges."[223]

2. Where authorization turns on broad employment policies, § 1030(a)(5)(A) is impermissibly vague

The second notice problem identified by *Drew* is that catch-all policies do not make it clear which violations "render access unauthorized."[224] If "any and all violations" rendered the user unauthorized, then the terms at issue would criminalize activities like advertising and sending chain letters via the site.[225] If only some violations qualified, there was no way to identify which.[226] Leaving the question of authorization to the site's broad terms therefore rendered the statute "unacceptably vague."[227]

A broad policy like ClickMotive's cannot define the bounds of criminal liability clearly enough to satisfy due process.[228] Its injunction against "destruction of valuable things" does not clearly distinguish between deleting a too-recent backup and deleting an email containing a tepid sales lead—or even tossing a half-used Splenda packet. As in *Drew*, the theory of authorization upon which

---

222 *See generally* ROA.2367-89 (Testimony of Andrew Cain).
223 *See* ROA.2389 (Testimony of Andrew Cain).
224 *Drew*, 259 F.R.D. at 464-465.
225 *Id*.
226 *Id*.
227 *Id*. at 464.
228 *See Drew*, 259 F.R.D. at 464-65.

Thomas's conviction rests does not admit any distinction between small and large violations of company policy—they would all be crimes, so long as the other elements of § 1030(a)(5)(A) were met.

After *Drew* was decided, both the Ninth Circuit (in *Nosal I*)[229] and Second Circuit (in *Valle*),[230] reversed convictions raising similar notice issues. Noting that employment relationships are "traditionally governed by tort and contract law," the Ninth Circuit rejected an "interpretation of the CFAA [that] allows private parties to manipulate their computer-use and personnel policies so as to turn these relationships into ones policed by the criminal law."[231] The court found "[s]ignificant notice problems" with criminal prohibitions that "turn on the vagaries of private polices that are lengthy, opaque, subject to change and seldom read."[232]

Nosal specifically called out "the typical corporate policy that computers can be used only for business purposes," noting that, if minor violations are "tolerated," employees cannot "be on notice of what constitutes a violation sufficient to trigger criminal liability."[233] These problems only multiply where, as

---

229 *United States v. Nosal*, 676 F.3d 854, 860 (9th Cir. 2012).
230 *Valle*, 807 F.3d at 527 (quoting *Nosal*, 676 F.3d at 860).
231 *See Nosal*, 676 F.3d at 860.
232 *Id.*
233 *Id.*

in this case, the corporate policy at issue is not even specific to computer use, but relates broadly to the treatment of "company property."[234] Thomas had no reason to know the policy governed the deletion of data, much less that it criminalized it.

3. Delegating the definition of criminal conduct to employers violates due process

The third problem with looking to private contracts for notice of criminal liability is that this approach renders the drafter, rather than Congress, "the party who ultimately defines the criminal conduct."[235] This approach invites vagueness, because the drafter "can establish terms where either the scope or the application of the provision are to be decided by them *ad hoc* and/or pursuant to undelineated standards."[236] The terms may also permit the drafter to "unilaterally amend and/or add to the terms with minimal notice to users."[237]

The *Drew* court might as well have been describing ClickMotive's handbook. ClickMotive "reserve[d] the right to modify the Handbook or amend or terminate any policy, procedure, or employee benefit at any time."[238] But even if written in stone, its broad prohibitions against "destruction of valuable property" and "interfering with the normal course of business" left ClickMotive with

---

234 ROA.1951-52 (Testimony of Ray Myers).
235 *See id*. at 465.
236 *Id.*
237 *Id*.
238 ROA.2682 (Government Exhibit 3).

indefinite discretion to determine what is prohibited and, according to the district court's view, therefore criminal.

4. The application of contract law to employment agreements introduces further vagueness

Finally, when private contracts define the scope of criminal liability, "a level of indefiniteness arises from the necessary application of contract law" and "contractual requirements" to a criminal prosecution.[239] In *Drew*, this meant determining whether, under the contract's forced-arbitration provision, only a private arbitrator could decide whether a breach occurred.[240]

Here, a similar limitation exists—the handbook acknowledgment that Thomas signed stated that a violation "could result in disciplinary action, up to and including termination."[241] If the handbook policy notified Thomas's of the limits of his authorization, then it also notified him of the limits of his liability.

B. ClickMotive's policy did not define "minimal guidelines to govern law enforcement"

As in *Drew*, the CFAA provision at issue here fails to define "minimal guidelines to govern law enforcement" when premised upon a breach of contract,

---

239 *Drew*, 259 F.R.D. at 465.

240 *Id*.

241 ROA.2682 (Government Exhibit 3).

because its scienter requirement establishes "absolutely no limitation or criteria as to which of the breaches should merit criminal prosecution."[242]

Section 1030(a)(5)(A) contains a dual scienter requirement: the defendant must (1) "*knowingly* cause[] the transmission of a program, information, code, or command" and thereby (2) "*intentionally* cause[] damage, without authorization, to a protected computer."[243] But both are satisfied by routine, benign activity—when a user deletes a file from a network drive or disconnects his computer from the company network, he "knowingly" transmits a command with the "intention" of "impair[ing]" the "integrity or availability" of "data" or a "system."[244]

After this low hurdle is surmounted, the only question separating a defendant in Thomas's position from criminal liability is whether he knew his conduct violated his employment agreement.[245] Therefore, the only "guideline" governing when § 1030(a)(5)(A) should be enforced is what constitutes a breach of that agreement. "[I]f every such breach does qualify, then there is absolutely no limitation or criteria as to which of the breaches should merit criminal prosecution."[246]

---

242 *Drew*, 259 F.R.D. at 467.
243 § 1030(a)(5)(A) (emphasis added).
244 *See* § 1030(e)(8) (defining "damage" as "any impairment to the integrity or availability of data, a program, a system, or information").
245 *See Drew*, 259 F.R.D. at 466.
246 *Id.* at 467.

If an employee's "authorization" is determined by reference to his employment agreement, § 1030(a)(5)(A) "becomes a law that affords too much discretion to the police and too little notice to citizens."[247] Because the only evidence that Thomas was "without authorization" was his violation of vague prohibitions in ClickMotive's employee handbook, his conviction should be overturned.

C. The district court's "plain reading" does not resolve the prosecution's vagueness issues

To answer the vagueness concerns raised by Thomas's motion for judgment of acquittal, the district court adopted the supposedly "straightforward reading" of "damage without authorization" announced by *United States v. Yücel*.[248] According to this reading, "a defendant causes damage without authorization when he has not been permitted by the victim to cause that damage."[249] Both the district court and *Yücel* claim that "[t]his straightforward reading of the phrase easily satisfies both prongs of the vagueness test."[250] Neither says how.

But *Yücel*'s reading of "damage without authorization" is neither straightforward nor unambiguous: a court must still determine *why* "that damage" caused by the defendant was "without authorization." It is at this stage of the

---

247 *Id.* (quoting *City of Chicago v. Morales*, 527 U.S. 41, 64 (1999)).
248 ROA.1486 (Order on Motion for Acquittal).
249 *Id*. (quoting *Yücel*, 97 F. Supp. 3d at 422.).
250 *Id*.

inquiry—locating the source and bounds of the defendant's authorization—that resort to broad policies introduces vagueness.

Nearly every office worker is permitted to delete emails from her inbox. *Yücel*'s "straightforward reading" does not say when a worker may delete a specific email—to "cause *that* damage," in *Yücel*'s formulation. If the answer in a particular prosecution is that company policy required employees to pursue the best interests of the company, then the statute is void for vagueness as applied.

Similarly, Thomas was permitted to do everything he was charged with doing. The district court concluded that he was "without authorization" in this particular instance because his actions "harmed ClickMotive's system."[251] Since § 1030(a)(5)(A) does not define "damage" with regard to "harm," the salient prohibition could only have been ClickMotive's policy that, in the prosecution's words, "no employee should do anything to harm the company."[252] That policy is too indefinite either to put employees on notice of criminal liability or to establish minimal guidelines for law enforcement.

The district court's effort to demonstrate that *Yücel*'s "straightforward reading" does not raise vagueness issues is ultimately circular. Thomas was "without authorization" because "ClickMotive did not give [him] permission" to

---

251 ROA.1487 (Order on Motion for Acquittal).
252 ROA.2530 (Government's Closing Statement).

"delete files," "disable pager alerts," or "change user permissions"—at least not "without following proper procedures" or "in a manner that damaged ClickMotive's system."[253] But once again, the only evidence that ClickMotive "did not give Thomas permission" to do these things is Ray Myers's testimony pointing to the handbook policy (and his general sense of right and wrong):

> Q: Now, there are no specific policies about when the IT operations manager could delete a virtual machine, is that right?
>
> A. Not around the timing of it. There were policies against destruction of things that are valuable.
>
> Q. Would you say that the word virtual machine appears in the policies in the handbook?
>
> A. Probably not, but a virtual machine is just a computer program, and destruction of computer programs is wrong.
>
> Q. It didn't say anything in the handbook about when the IT operations manager could disable pager alerts?
>
> A. Again, I would go to the blanket policy of you can't do things that interfere with the normal course of business.

---

[253] ROA.1487 (Order on Motion for Acquittal).

> Q. And what did that policy say specifically?
>
> A. I do not have it in front of me, but common sense would say that it's wrong to destroy things of value.
>
> Q. Common sense, but not necessarily the handbook policy?
>
> A. I am absolutely certain that the policy says in some way that you cannot destroy company property.[254]

In the end, then, the district court's determination that Thomas acted "without authorization" was based on the broad policy (or policies) in ClickMotive's employee handbook. For the reasons above, those policies neither provided notice to Thomas that his conduct was criminal, nor adequately guide enforcement of § 1030(a)(5)(A). The district court's application of the statute is therefore void for vagueness and Thomas's conviction must be overturned.

---

[254] ROA.1951-52 (Testimony of Ray Myers).

CONCLUSION AND PRAYER FOR RELIEF

For the foregoing reasons, the Court should find that the evidence is not sufficient to support the district court's determination that Thomas acted "without authorization," and should reverse his conviction. Thomas had unlimited authority over ClickMotive's systems, which was not expressly limited by the company. To the extent that "authorization" under § 1030(a)(5)(A) is ambiguous, the Court should adopt the narrower reasonable construction and find that Thomas cannot have acted "without authorization" by violating a broad employment policy. Finally, the Court should determine that § 1030(a)(5)(A) is void for vagueness where "authorization" is determined by reference to a broad corporate policy.

TOR EKELAND, P.C.
/s/ Aaron Williamson
Aaron Williamson (N.Y. Bar # 4580999)
Tor B. Ekeland (N.Y. Bar # 4493631)
Tor Ekeland, PC
43 W. 43rd Street, Suite 50
New York, NY 10036-7424
Telephone: 773-727-8363
Facsimile: 718-504-5417
aaron@torekeland.com
tor@torekeland.com

Attorneys for Defendant-Appellant

CERTIFICATE OF SERVICE

This is to certify that a true and correct copy of the above and foregoing pleading was electronically served on all counsel of record by way of the Court's CM/ECF system on February 22, 2017.

/s/ Aaron Williamson
Aaron Williamson (N.Y. Bar # 4580999)
Tor B. Ekeland (N.Y. Bar # 4493631)
Tor Ekeland, PC
43 W. 43rd Street, Suite 50
New York, NY 10036-7424
Telephone: 773-727-8363
Facsimile: 718-504-5417
aaron@torekeland.com
tor@torekeland.com

Attorneys for Defendant-Appellant

CERTIFICATE OF COMPLIANCE WITH RULE 32(a)

This brief complies with the type-volume limitation of Fed. R. App. P. 32 a(7)(B) because this brief contains approximately 10,928 words, excluding the parts of the brief exempted by Fed. R. App. P. 32 (a)(7)(B)(iii). This brief was prepared using Microsoft Office Word 2013.