No. 19-783

In The

Supreme Court of the United States

NATHAN VAN BUREN,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Writ Of Certiorari To The United States Court Of Appeals For The Eleventh Circuit

BRIEF OF PROFESSOR ORIN S. KERR AS AMICUS CURIAE IN SUPPORT OF PETITIONER

ORIN S. KERR
Counsel of Record
334 North Addition
Berkeley, CA 94720
(510) 664-5257
orin@orinkerr.com

COCKLE LEGAL BRIEFS (800) 225-6964
WWW.COCKLELEGALBRIEFS.COM

TABLE OF CONTENTS

TABLE OF CONTENTS—Continued

TABLE OF AUTHORITIES

Page

CASES

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

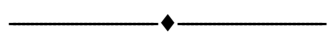
Page

OTHER AUTHORITIES

TABLE OF AUTHORITIES—Continued

INTEREST OF THE AMICUS CURIAE

Orin S. Kerr is a Professor of Law at the University of California, Berkeley School of Law. He has written extensively about 18 U.S.C. § 1030, known as the Computer Fraud and Abuse Act (CFAA). His experience includes working as a lawyer in CFAA cases from the prosecution side, criminal defense side, and civil defense side; testifying about the law before congressional committees; and helping to draft amendments to it. The interest of amicus is the sound development of the law.[1]



SUMMARY OF ARGUMENT

This brief makes five points in support of reversal, focusing on the broader context of the dispute. It starts with some background about the CFAA and then turns to the choices the Court faces. It next explains how the two parts of the CFAA should fit together. It then offers a case study of the government's approach, the prosecution of Lori Drew. The brief concludes by explaining

[1] Both parties have consented to the filing of this amicus curiae brief. No counsel or party made any monetary contribution supporting the preparation or submission of this brief. No counsel for any party authored this brief in whole or in part. The University of California at Berkeley provides financial support for faculty members' research and scholarship that helped defray the costs of preparing this brief. The University is not a signatory to this brief, however, and the views expressed here are solely those of the amicus curiae. No other person or entity, other than the amicus curiae, has made a monetary contribution intended to fund the preparation or submission of this brief.

why the government is trying to stretch the CFAA to fit this case, and how Congress (and only Congress) can craft a consensus law that meets the government's needs.

ARGUMENT

Petitioner did not violate the CFAA. To appreciate why, it helps to understand the broader context of this case and the role and structure of the CFAA. This brief tries to explain that broader context in five steps.

First, the fundamental question is whether violating verbal limits on computer use triggers CFAA liability—not, as Petitioner frames it, whether having an unauthorized purpose violates the law.

Second, the statutory structure of the CFAA would put the Court in a bind if it allows verbal limits to have the force of criminal law. It would have to either allow that for every limit or else devise new rules for which limits count.

Third, the difficulty of distinguishing between access without authorization and exceeding authorized access counsels in favor of interpreting the latter narrowly.

Fourth, the risk of abuse in the government's broad position is not merely hypothetical. The Court can best appreciate that risk by studying the 2008 prosecution of Lori Drew.

Fifth, appreciating the "insider problem" of computer crime law shows why the government is trying to stretch the CFAA to cover Petitioner's conduct. It also shows why rejecting the government's position could lead Congress to pass a consensus solution to the government's problem.

I. THIS CASE IS ABOUT WHETHER CFAA LIABILITY EXTENDS TO VIOLATING VERBAL LIMITS ON COMPUTER USE (SOMETIMES CALLED "CONTRACT-BASED" RESTRICTIONS).

Petitioner's brief presents this case as a dispute about unauthorized purpose. *See* Petr. Br. 14-18. It is more precise to say the case concerns whether words control authorization. It is helpful to untangle the difference between these perspectives to understand the case's significance.

First, some history. At the dawn of the computer era, in the 1970s and 1980s, courts and legislators struggled to identify when computer misuse was criminal. *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1602-13 (2003) (hereinafter *Cybercrime's Scope*). Legislators responded in the 1980s by enacting computer trespass laws that apply physical-world trespass concepts to computers. *See id*. at 1613-17.

The CFAA is the federal computer trespass statute. The law is violated when access to a computer is

unauthorized, much like how physical trespass laws are violated when physical presence is unlicensed. *See* Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143, 1148-55 (2016) (hereinafter *Norms*).

This case asks the Court to settle what makes access unauthorized—in the words of the statute, either an access "without authorization" or an act that "exceeds authorized access." 18 U.S.C. § 1030(a)(2). The question is hard because two different theories of authorization exist. The first theory, based on technology, is universally accepted. The second theory, based on words, is deeply controversial. This case asks whether CFAA liability is limited to the first theory or if it also extends to the second theory.

An overview of the two approaches may be helpful. The first theory, based on technology, is that conduct becomes unauthorized when it circumvents a technological restriction on access. I have called this the "code-based" approach because it requires bypassing a limit created by computer code. *See Cybercrime's Scope* at 1644-46. This covers traditional hacking, such as exploiting a software vulnerability or successfully guessing another person's password. *See United States v. Morris*, 928 F.2d 504, 510-11 (2d Cir. 1991).

The idea behind the code-based theory is that computers are programmed to control who can access them. Someone who intentionally circumvents technological barriers to access violates privacy and the security of the information stored on the computer. He "breaks in" to the computer much like a trespasser who

picks a lock to a home or sneaks in through an open window. *See Norms* at 1171-72.

Importantly, no one disputes that the CFAA criminalizes this kind of access. Scholars and lower courts debate the edge cases, disputing exactly what counts as circumventing technological restrictions. *See*, *e.g.*, *Norms* at 1161-80. But everyone agrees that the CFAA criminalizes the bypassing of code-based restrictions.

This case is instead about the second theory of CFAA liability, the one based on words. In a networked world, computer owners often allow others to use their computers subject to verbal restrictions on how that use can proceed. I have called these restrictions "contract-based" limits, as they often take the form of agreements that may form contracts. *See Cybercrime's Scope* at 1645-46. The contract-based theory does not require an actual contract to be formed. Rather, it refers to any verbal restriction on how a computer can be used.

When a computer owner imposes a contract-based restriction, the technology permits access but written rules condition what kinds of uses are allowed. We all encounter these limits frequently in the form of terms of service or employment restrictions on using employer computers for work-related reasons. If the contract-based theory of the CFAA is correct, these words have the force of criminal law: A person who violates an expressed restriction is unauthorized just like one who actually breaks in by circumventing technological barriers.

All of this matters because Van Buren's brief frames the question presented in a somewhat confusing way. His brief focuses on whether an improper purpose can trigger CFAA liability. *See* Petr. Br. 14-18. But purpose matters in this case only because the verbal restriction here happened to be purpose-based. Van Buren was told that he could access the computer only for official purposes, and he accessed it for personal reasons instead. *See* J.A. 16-17. The important interpretive question is not whether purpose matters, but whether words matter. If a computer owner limits use with a verbal restriction, whether one based on purpose or something else, does violating that verbal restriction violate the CFAA?

Unfortunately, the statutory text is entirely unilluminating. The CFAA does not define "access . . . without authorization." Congress did define "exceeds authorized access" in 18 U.S.C. § 1030(e)(6), but that definition is notably unhelpful:

> the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.

This definition is largely circular. It uses a concept, entitlement, that is simply a synonym for authorization. To be entitled is to be authorized. *See*, *e.g.*, *Merriam-Webster's Dictionary Online* (defining "entitled" as "having a right to certain benefits or privileges," and defining "authorized" as "having or done with legal or official approval"). The statutory definition begs the

question of in what circumstances a person lacks authorization or entitlement to act.

II. THE COURT SHOULD REJECT THE CONTRACT-BASED THEORY OF CFAA LIABILITY.

The Court should solve this puzzle by adopting the code-based approach to CFAA liability and rejecting the contract-based approach. The CFAA prohibits circumventing technological restrictions. But it does not criminalize acts, such as Van Buren's, that only violate express restrictions on computer use.

This is the best interpretation for two reasons. First, existing trespass norms do not include violating verbal restrictions on use. Second, extending the CFAA to contract-based restrictions would either criminalize the way millions of Americans use the Internet or require courts to draft a new statute.

(a) Existing Trespass Norms Do Not Extend to Contract-Based Violations.

Criminal trespass laws are traditionally written in general terms. Entrance or presence is criminal when it is not licensed. *See*, *e.g.*, American Law Institute, Model Penal Code § 221.2. The statutory text does not define exactly what it prohibits. Instead, the interpretation of trespass laws traditionally relies on trespass norms—shared senses of what kind of acts constitute an invasion into another person's property. *See Norms* at 1146. Legal meaning comes from norms

instead of statutory text. This works well for traditional physical trespass laws because physical trespass norms are well-settled. *See id.* at 1148-52.

This legal tradition creates a puzzle for courts that must interpret computer trespass laws such as the CFAA. Computer trespass norms are not well-settled, making it difficult to identify exactly what the law prohibits. *See id.* at 1154-55. Circumventing technological restrictions poses an easy case. It is precisely the kind of "breaking in" or "hacking" that the CFAA was designed to target. So far, so good. But the Court should proceed cautiously when considering whether other kinds of conduct fall within the vague prohibition of computer trespass laws.

Specifically, the Court should not interpret the vague language of the CFAA to criminalize breaching contract-based restrictions because existing computer trespass norms do not extend to them. The common expectation is that users with accounts are free to use them. Express restrictions are treated only as an effort to impose a contractual obligation on the user. Violating those terms might be a breach of contract. But it is not an invasion of the computer owner's property that is recognized as a trespass. *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1582 (2010) (hereinafter *Vagueness Challenges*).

That is why most people ignore the written restrictions imposed on their computer use. We disregard terms of service. "Few people bother to read them,

much less follow them. Internet users routinely click through such agreements on the assumption that they are legal mumbo jumbo that don't impact what users are allowed to do." *Id*. Absent an existing trespass norm about ignoring express restrictions, this Court should not interpret ambiguous language in the CFAA as mandating one. The vague language of the CFAA should be construed as limited to the core conduct of breaking in—circumventing technological restrictions on computer use—for which clear trespass norms exist.

(b) Extending CFAA Liability to Contract-Based Violations Would Lead to Astonishing Results Or Require Judicial Creation of A New Statute.

A second reason that violating express restrictions should not trigger CFAA liability is the truly stunning implications of doing so. Either it would create possibly the broadest criminal law that ever existed, or it would require judges to craft a new law in its place.

The statute's structure is the problem. Section 1030 covers everything with a microchip that can be regulated under the Commerce Clause, whether it is connected to the Internet or not. *See Vagueness Challenges* at 1570-71, 1577-78. Section 1030(a)(2) specifically prohibits unauthorized access whenever *any* information of *any* kind is viewed or otherwise obtained. *See id*. at 1577-78. This extraordinary scope means that the only real limit on the CFAA for any

computer is the meaning of unauthorized access—whether access "without authorization" or "exceed[ing] authorized access." 18 U.S.C. § 1030(a)(2).

Because of this structure, holding that Van Buren violated the CFAA would place the Court in a serious bind. The Court would have two unappealing options. Under the first option, *any* intentional violation of *any* express restriction on a protected computer would be a federal crime. Under the second option, courts would have to craft a new jurisprudence about which written restrictions are sufficiently serious or important to justify criminal liability. Neither path is acceptable.

Consider the first option, in which any intentional violation of any written restriction is a federal crime. This would make the CFAA a truly astonishing law. In our networked world, we access hundreds of computers every day that are owned and operated by others. We wake up and check the news, accessing dozens of media computers. We check our e-mail, accessing dozens of e-mail provider computers. And that's all before our first cup of coffee.

Given how often people access computers run by others, a world in which ignoring any written restriction of any computer counts as a federal crime is a world in which most of us are criminals many times over every day.

And that includes me. Like the majority of American adults, I have a Facebook account. Facebook's terms of service require its users to "[p]rovide accurate

information about" themselves. *See* Facebook Terms of Service, https://www.facebook.com/legal/terms/plain_text_terms (last visited July 1, 2020). I recently violated that term by listing my home city as Sealand. Sealand is an offshore platform in the North Sea near England built during World War II to host anti-aircraft guns. It's not actually my home city. I list it only to make a point about the CFAA. But under the government's position, my joke is no laughing matter. It is a federal crime.

Part of the problem is that written restrictions placed on computers can be entirely arbitrary. These days, anyone can run a website. Anyone can buy a computer for another person to use. And the computer owners or operators can impose whatever restrictions they want. Their limits don't need to serve an important interest. They don't even need to make sense.

For example, in 2008, in response to the government's prosecution of Lori Drew (discussed in Section IV, *infra*), I announced new terms of use for the *Volokh Conspiracy* blog. Any visit to the blog was unauthorized unless it satisfied all of the following five conditions:

> 1. You will not post comments that are abusive, profane, or irrelevant.
>
> 2. You are not an employee of the U.S. government.
>
> 3. Your middle name is not "Ralph."
>
> 4. You're super nice.
>
> 5. You have never visited Alaska.

Orin Kerr, *New Terms of Use for the Volokh Conspiracy*, Volokh Conspiracy (November 28, 2008), http://volokh.com/2008/11/28/new-terms-of-use-for-the-volokh-conspiracy/.

Imposing criminal liability for violating these terms would be absurd. Granted, any computer owner or operator is free to say that no one can visit his website who has been to Alaska. But backing up that wish with federal criminal law delegates the extraordinary power of the criminal sanction to a computer owner's whim. If computer owners want to keep visitors out, they can put up technological walls. Breaking down those walls will violate the CFAA. But words alone cannot be an adequate substitute.

A second option exists to avoid this absurd result. The Court could say that only *some kinds* of verbal restrictions count. After all, Van Buren violated an unusually important restriction. His training to only access the GCIC database for official law enforcement reasons served critical government interests in privacy and government integrity. Perhaps it might work to limit liability to violating only particularly important restrictions, or clear ones, or ones phrased in particular ways?

It would not. Verbal restrictions on computer use come in endless guises. They can be written in different ways, with different purposes, covering different computers and different data and accessed by different users. A rule that tried to parse serious from non-serious restrictions—or important from unimportant ones, or

clear from murky ones—would force courts to engage in endless line-drawing about what is a crime with no legislative principles to guide them.[2]

No one could know what the law prohibits in such a world. The criminal law would come ex post from judicial decisions instead of ex ante from legislative judgments. But it is Congress's job, not the judiciary's, to say what is a crime. *See United States v. Hudson & Goodwin*, 11 U.S. (7 Cranch) 32 (1812).

III. THE DIFFICULTY OF DISTINGUISHING ACCESS WITHOUT AUTHORIZATION FROM EXCEEDING AUTHORIZED ACCESS COUNSELS IN FAVOR OF PETITIONER'S INTERPRETATION.

There is an additional reason to limit the CFAA to circumventing technological restrictions: Modern technology no longer permits a clear distinction between "access . . . without authorization" and "exceed[ing] authorized access" in § 1030. When the CFAA was enacted, in the 1980s, a plausible line existed between these two concepts. Today's technology blurs or eliminates the line between them, which counsels in favor

---

[2] Drawing distinctions based on the clarity of the restriction would be particularly inappropriate because clarity is primarily a means of figuring out mental state, which is a separate element of 18 U.S.C. § 1030(a)(2). The statute requires an intentional unauthorized access, which likely means intent, hope, or knowledge of the facts relevant to authorization and not the legal status of authorization. *See generally Norms* at 1180-82 (discussing the CFAA's mental state requirement).

of interpreting them to harness the same basic principle. Because access "without authorization" has been limited to circumventing technological restrictions, the same limit should be imposed for "exceed[ing] authorized access."

This argument is pretty technical, I admit. But appreciating it can shed light on the CFAA's broader structure in a way the Court should understand.

Here's the context. The CFAA has two basic prohibitions: "access . . . without authorization" and "exceed[ing] authorized access." Most of the offenses in § 1030(a) use them together. In the 1980s, when Congress enacted the CFAA, the distinction between the two prohibitions likely focused on their timing. In those days, using one of the "federal interest" computers covered by the initial statute typically required a telephone, a modem, and an intentional plan to log in to that computer. It was easy to know when the computer was accessed, permitting a statutory distinction between the initial access and subsequent conduct. *See Vagueness Challenges* at 1565.

If you have a few minutes, watch how Matthew Broderick's character logs in to Dr. Falken's computer in the 1983 movie *WarGames*.[3] Broderick dials up the computer and tries to gain access. A password prompt blocks him. He eventually guesses the correct password—"Joshua," the name of Dr. Falken's son—and

[3] The scene is available at https://www.youtube.com/watch?v=uCWKZWieMSY, also found by searching YouTube for "Wargames 1983 – The voice of WOPR".

hits enter. A flurry of data appears on the screen. The password prompt is replaced by a new prompt, "GREETINGS DOCTOR FALKEN." Broderick declares, "We're in!" He is then free to use the computer. *See generally WarGames* (United Artists & Sherwood Productions 1983). The moment of access is obvious, and the temporal line between initial access and post-access use is clear.

Technological change has since muddled this line in two related ways. First, we now live in a connected world. Our phones, laptops, and other devices are now always connected to computers around the world. The specific moment of computer access has been largely replaced by an experience of ongoing computer use. To be sure, there are still moments like entering Doctor Falken's computer with a password. But in a hyper-connected world, our interactions with computers no longer fit the binary world of pre-access and post-access with a clear line between them.

A second change is that the concept of a "computer" has mutated. When Congress enacted the CFAA, a computer was understood as a single box with hardware inside. Today, however, the idea of a discrete computer is largely outdated. Many online services today are cloud-based. They rely on a global network of data centers to provide access on an as-needed basis. When a person uses a cloud-based service, there is no one "computer" that is accessed. *See*, *e.g.*, *What Is the Cloud?*, Cloudfare, https://www.cloudflare.com/learning/cloud/what-is-the-cloud/.

These technological changes have blurred the line between initial access governed by the access-without-authorization prong and subsequent acts governed by the exceeds-authorized-access prong. You can usually describe the same conduct plausibly either way. Imagine a person visits a website and then clicks on a forbidden link that he is not supposed to click on. You could present the clicking on the link as an access to the computer that may or may not be authorized. Alternatively, you could present it as a post-access use that may or may not exceed authorized access. There is no sharp line between them anymore. *Cf. Cybercrime's Scope* at 1619-21 (discussing ways to interpret "access").

The parties happen to agree in this litigation that Van Buren did not access without authorization. Formally, the legal dispute is over the meaning of "exceeds authorized access." BIO 7; Petr. Br. 14. But the general difficulty of distinguishing between these two concepts counsels in favor of interpreting them in the same basic way. As the lower courts have properly held, access "without authorization" is limited to circumventing technological access restrictions. *See United States v. Morris*, 928 F.2d 504, 510-11 (2d Cir. 1991); *Pulte Homes, Inc. v. Laborers' Int'l. Union of N. Am.*, 648 F.3d 295, 304 (6th Cir. 2011). The court should interpret "exceeds authorized access" as imposing the same bar but at a different stage.

Here's how the two prongs should work together. A person who has not accessed a computer at all but circumvents technological restrictions to gain access

commits an access without authorization. On the other hand, a person who has already accessed a computer and then circumvents technological restrictions to gain additional information has exceeded authorized access. Under this view, the precise moment of access to the computer does not matter. The CFAA covers circumventing technological access restrictions in the same way regardless of exactly when the first access to the computer occurs.[4]

In contrast, embracing the government's broad view of "exceeds authorized access" would cause considerable confusion. CFAA prosecutions relying on violations of contract-based restrictions would hinge on a question made difficult to answer by modern technology. In each case, the government would argue that the computer had previously been accessed and that the conduct exceeded authorized access, triggering the contract-based theory. The defense would respond that the prosecuted conduct was instead an access to that computer, limiting the government to the code-based theory. Criminal liability would hinge on identifying exactly when the initial access to that computer occurred. It would be metaphysics as criminal law.

Given the absence of clear lines between these two frameworks, the Court should not lightly adopt an

---

[4] The main exception to this would be 18 U.S.C. § 1030(a)(5)(B)-(C), parts of the computer damage section, which are triggered only by access without authorization. For an overview of the different sections of the CFAA and how they relate to each other, *see* Orin S. Kerr, Computer Crime Law 30-144 (4th ed. 2018).

interpretation of "exceeds authorized access" that departs so dramatically from access "without authorization."

IV. THE CAUTIONARY TALE OF *UNITED STATES V. DREW* SHOWS THAT THE RISK OF ABUSE IS NOT JUST HYPOTHETICAL.

Petitioner's case is based partly on a risk of abuse if the Court adopts the government's expansive approach. Petr. Br. 23-36. That concern is not mere conjecture. In 2008, the U.S. Attorney's Office in Los Angeles brought a CFAA prosecution that exemplifies the government's position. The prosecution of Lori Drew serves as a cautionary tale about the extraordinary power the government seeks.[5]

The Drew prosecution started with a terrible tragedy in a suburb of St. Louis, Missouri. In October 2006, a 13-year-old girl named Megan Meier committed suicide. Meier had regularly used the social media networking site MySpace, a then-popular forerunner to today's Facebook. In the weeks before her death, Meier had communicated with a MySpace profile of what appeared to be a handsome 16-year-old boy named Josh Evans. The Evans account had befriended Meier, and Evans expressed his admiration and affection for

[5] I joined Drew's defense team on a pro bono basis to help brief and argue the CFAA issues. This discussion of the case is based only on the public record, primarily consisting of trial testimony and legal documents filed in court. It contains no confidential or privileged information.

Meier. *See United States v. Drew*, 259 F.R.D. 449, 452 (C.D. Cal. 2009).

But the online friendship soured. In messages sent soon before Meier committed suicide, Evans had abruptly ended the relationship. According to one witness, the last message Evans had sent to Meier had said, "You're a shitty person, and the world would be a better place without you in it." Lauren Collins, *The Friend Game*, The New Yorker, Jan. 14, 2008.

An investigation into Meier's suicide revealed that Josh Evans did not exist. The account was fake. It had been created by a group that knew Meier and used it to learn what Meier was saying about her friend Sarah Drew. The senior member of the group was Sarah's mother, Lori Drew. Other participants included Ashley Grills, an 18-year-old employee of Mrs. Drew who actually devised the idea and used the account, and Sarah Drew herself. *See* Kim Zetter, *Government's Star Witness Stumbles: MySpace Hoax Was Her Idea, Not Drew's*, Wired, Nov. 20, 2008.

The Evans hoax became a national news story. Media coverage focused on Lori Drew's role. Many were outraged that Drew had not been charged with causing Meier's death. *See* Christopher Maag, *A Hoax Turned Fatal Draws Anger But No Charges*, N.Y. Times, Nov. 28, 2007. A list of the most despised people on the Internet, published a month before charges were filed, ranked Lori Drew number one. *See* Neel Shah, *The Internet Is For Scorn: Meet the Web's 10 Most Hated People*, Radar Online, Apr. 7, 2008 ("[C]ongratulations,

Lori! You are officially the most despised person in the whole wide web!").[6]

Despite intense public demand to punish Drew, Missouri state prosecutors declined to file charges. A law enforcement spokesperson explained that decision straightforwardly: Drew's conduct "might've been rude, it might've been immature, but it wasn't illegal." Maag, *supra* (quoting Lieutenant Craig McGuire of the St. Charles County Sheriff's Department).

Federal prosecutors in Los Angeles were more creative. They realized that MySpace had expansive terms of service. By using MySpace, the terms stated, "you represent and warrant that . . . all registration information you submit is truthful and accurate" and that "you will maintain the accuracy of such information." *Drew*, 259 F.R.D. at 454.

The terms of service gave prosecutors a hook. Because Josh Evans did not exist, using the account violated MySpace's terms of service. According to prosecutors, this rendered every use of the Evans account an unauthorized access in violation of 18 U.S.C. § 1030(a)(2). And because MySpace's computer servers were in Los Angeles County, federal prosecutors could bring charges in California even though everyone involved was in Missouri.

A federal grand jury in the Central District of California returned a four-count felony indictment against

---

[6] The article is available via the Wayback Machine and can be found at this link: https://tiny.cc/DrewMostHated.

Drew. The indictment charged her with conspiring to violate MySpace's terms of service as well as aiding and abetting terms-of-service violations on three specific dates when the Evans account was used. Each term-of-service violation was a felony, the indictment charged, because it furthered a tortious act under 18 U.S.C. § 1030(c)(2)(B)—specifically, intentional infliction of emotional distress. *See* Indictment at 14, 18, *United States v. Drew*, 2008 WL 2078622 (C.D. Cal.).

The trial of Lori Drew lasted five days in federal court in Los Angeles. In an unusual move, the United States Attorney himself personally led the prosecution. Ashley Grills testified for the government under an immunity agreement. The jury deadlocked on the conspiracy count, and it acquitted on the felony counts based on intentional infliction of emotional distress. However, the jury convicted Drew of three misdemeanor counts of § 1030(a)(2) for aiding and abetting the violation of MySpace's terms of service.

The jury foreperson later explained in a media interview that the jury had acquitted on the felony counts because it lacked evidence of Drew's intent to inflict emotional distress. At the same time, the foreperson viewed the terms-of-service violations alone as serious wrongs, at least in the "gross circumstances of someone killing themselves." Kim Zetter, *Jurors Wanted to Convict Lori Drew of Felonies, But Lacked Evidence*, Wired, Dec. 1, 2008 (quoting the jury foreperson).

The government's sentencing memorandum asked the court to impose the statutory maximum prison sentence: 36 months, consisting of one year for each use of the Evans account that Drew aided and abetted. *See* Sentencing Memorandum of the United States, *United States v. Drew*, 2009 WL 1269549 (C.D. Cal.). Remarkably, the prosecution's detailed memorandum did not even mention MySpace's terms of service. It instead argued that Drew had callously caused Meier's suicide and had shown no remorse. *See id.* The District Court never sentenced Drew because it granted the defendant's motion to dismiss on the ground that construing the CFAA to cover MySpace's terms of service would render the statute void for vagueness. *See Drew*, 259 F.R.D. at 464. The prosecution filed a notice of appeal but later withdrew it.

What is the lesson of the Drew prosecution? In my view, the lesson is this: The power to prosecute people for violating express restrictions on computers is a power to prosecute anyone the government thinks needs prosecuting. The government didn't really care that Drew had aided and abetted terms-of-service violations. That was happenstance. Presumably, the government prosecuted Drew because she was the most hated person on the Internet. The public demanded her punishment, and a United States Attorney found a way to answer the call.

Then-Attorney-General Robert H. Jackson famously remarked that "the greatest danger of abuse of prosecuting power lies" where a prosecutor "picks some person whom he dislikes or desires to embarrass, or

selects some group of unpopular persons and then looks for an offense." Robert H. Jackson, *The Federal Prosecutor*, 24 J. Am. Jud. Soc'y 18, 19 (1940). As *Drew* demonstrates, the government's position in this case would let federal prosecutors find those offenses in the CFAA.

V. UNDERSTANDING THE INSIDER PROBLEM IN COMPUTER CRIME LAW HELPS EXPLAIN WHY THE GOVERNMENT IS STRETCHING THE CFAA IN THIS CASE—AND WHY CONGRESS, NOT THE COURTS, HAS THE SOLUTION.

I'll end with the big picture. Understanding the question presented in this case requires appreciating some broad brushstrokes about the developing law of computer crime. In particular, it's important to understand the "insider problem" and how the government's reliance on the CFAA in this case tries to solve it. That context explains why the government does have an important interest in this case. But it also shows that the government is trying to fit a square prosecutorial peg into a round legislative hole. Rejecting the government's position would send this issue back to Congress to craft a consensus solution.

Here's a summary of the insider problem. In the age of computers and the Internet, it is easier than ever to share sensitive information. That has pros and cons. On the plus side, it's easy for information to be made available to those with a legitimate interest in

seeing it. Anyone with an Internet connection can connect. That's good. On the minus side, it's easy for those who can see sensitive information to convert it to improper uses. Once they have the information, they can press a button to create a new copy, send it to others without permission, or misuse it themselves. That's bad.

The insider problem asks what role criminal law should play in stopping insiders from misusing sensitive information. Insider misuse can cause major harms. When it causes harms, the government understandably wants the criminal laws to deter and punish it. But what criminal laws apply? The government has tried several strategies over time. It lacks a full set of tools under current law, however, which explains why it is trying to stretch the CFAA to fill in the gaps.

One of the government's first strategies was charging insiders under 18 U.S.C. § 2314, the law against interstate transportation of stolen property. When an insider copied the information in the course of converting it to a forbidden use, the thinking ran, the information became "stolen." The stolen property was transported in interstate commerce either by sending it over the Internet or carrying a copy on a portable disk across state lines. Courts rejected this prosecution theory, however, on the ground that § 2314 requires the stolen property to have tangible form. *See*, *e.g.*, *United States v. Brown*, 925 F.2d 1301, 1305-09 (10th Cir. 1991); *United States v. Aleynikov*, 676 F.3d 71, 77-78 (2d Cir. 2012).

A second strategy was to try the federal conversion statute, 18 U.S.C. § 641, at least in cases involving federal government employees. On this thinking, perhaps the employee who used a government computer for impermissible personal reasons was converting the government's property to his own use. Courts largely rejected this approach, as well, although the caselaw was more mixed. *See*, *e.g.*, *United States v. Collins*, 56 F.3d 1416 (D.C. Cir. 1995) (overturning conviction of a DIA employee who used classified computers for personal reasons); *Chappell v. United States*, 270 F.2d 274, 277 (9th Cir. 1959) (holding that government property must be tangible for § 641 to apply). *But see United States v. Girard*, 601 F.2d 69, 71 (2d Cir. 1979) (holding that a DEA employee who sold records about informants to drug dealers had violated § 641).

Congress solved an important part of the insider problem in 1996 with the passage of 18 U.S.C. § 1832, the federal criminal law prohibiting the theft of trade secrets. This law directly addresses the insider problem. It punishes an insider who "without authorization copies" or otherwise obtains a trade secret "that is related to a product or service used in or intended for use in interstate or foreign commerce" with intent to convert it "to the economic benefit of anyone other than the owner." *Id.* at § 1832(a). This statute is regularly used to prosecute insiders in business contexts. *See*, *e.g.*, *United States v. Nosal*, 844 F.3d 1024, 1041 (9th Cir. 2016). But the law has a critical limit: It requires the information to be a trade secret. *See* 18 U.S.C. § 1839(3) (defining trade secret).

The government's quandary is that no obvious solution to the insider problem exists when the information obtained is *not* a trade secret. The gap matters most in cases like *Van Buren*, in which a government insider misuses a sensitive database. What to charge? Section 2314 won't fly because the information is intangible. Section 641 has a chance in some circuits, but courts have construed it narrowly in others. Section 1832 doesn't work because no trade secret is involved.

The government has relied on broad interpretations of the CFAA to try to fill this gap. Employees with access to sensitive databases normally will have been told to access them only for official purposes. The government has used that fact, as in this case, to prosecute insiders on the theory that computer use contrary to expressed limits violates 18 U.S.C. § 1030. *See*, *e.g.*, *United States v. Manning*, 78 M.J. 501, 510-12 (U.S. Army Ct. Crim. App. 2018); *United States v. Valle*, 807 F.3d 508, 528 (2d Cir. 2015); *United States v. Nosal*, 676 F.3d 854, 858 (9th Cir. 2012) (en banc); *United States v. Rodriguez*, 628 F.3d 1258, 1260 (11th Cir. 2010).

But the government's argument proves too much. As written, the CFAA offers no way to let the government bring those cases without also making everyone a criminal who knowingly violates terms of service. You can't get *Rodriguez* without also producing *Drew*. The government may not actually want that broader power, at least in most cases. But using the CFAA to solve the insider problem ends up making most Americans criminals for entirely innocuous conduct.

A better answer is for Congress to enact a new criminal law specifically about insider abuse of sensitive government databases.[7] In effect, the law would be a non-economic version of § 1832 for government employees. Like § 1832, it could apply only to specific kinds of information—in this case, sensitive personal information stored in specific types of government databases. Echoing § 1832, it could prohibit copying or otherwise obtaining that information with intent to convert it to a non-government use.

This proposed law—call it the Privacy Protection Act of 2021—would likely draw widespread support. The government would appreciate it because it helps solve the insider problem. Civil libertarians would support it because it protects personal privacy from rogue government employees. And everyone else would appreciate that it would not make them criminals for the routine ways they surf the web.

[7] Van Buren was also charged with and convicted of honest services fraud through bribery, which represents another government strategy to deal with the insider problem. On this thinking, a government employee who accepts payment for using his insider privileges to misuse sensitive information has deprived the public of its right to the employee's honest services. The Eleventh Circuit held below that there could be enough evidence to support this charge but remanded for a new trial because the jury instructions were flawed. *See United States v. Van Buren*, 940 F.3d 1192, 1205 (11th Cir. 2019). If Congress considers enacting the new law that I suggest, it should also consider whether the honest services fraud statute should apply to these facts and how the two laws might interact.

CONCLUSION

This Court should reverse the Eleventh Circuit, limit the CFAA to circumventing technological restrictions, and let the government pursue the Privacy Protection Act of 2021 in the next Congress.

Respectfully submitted,

ORIN S. KERR
Counsel of Record
334 North Addition
Berkeley, CA 94720
(510) 664-5257
orin@orinkerr.com

July 8, 2020