American University Washington College of Law

THE CRIMINAL LAW PRACTITIONER

Volume XVI, Issue II **Summer 2026**

Articles


THE CRIMINAL LAW PRACTITIONER
EST. 2009

AMERICAN UNIVERSITY WASHINGTON COLLEGE OF LAW

THE CRIMINAL LAW PRACTITIONER


THE CRIMINAL LAW PRACTITIONER
EST. 2009

American University Washington College of Law
THE CRIMINAL LAW PRACTITIONER

Contents


THE CRIMINAL LAW PRACTITIONER
EST. 2009

Letter from the Editor

Isabel V. Capecci, The Criminal Law Practitioner

Dear Readers,

Thank you for your interest in The Criminal Law Practitioner. This Summer 2026 Issue marks the second and final in the 16th Volume of our publication. This journey has been one characterized by academic and professional curiosity, cross-discipline collaboration, and collective creativity. As always, I want to give a big shout out to our entire staff, especially my predecessor Davis Hayman. Their hours of tireless dedication has made this experience rewarding and fulfilling for everyone on our Editorial Board, and I believe this commitment is reflected in the intriguing articles.

First, "California's Racial Justice Act" analyzes the application of California's Racial Justice Act to law enforcement throughout a criminal proceedings. This piece argues that while California's Racial Justice Act is based on admirable goals, it falls short of achieving those goals and goes on to suggest certain amendments that could enable the Act to better achieve the legislature's goals.

Second, in "Artificial Crimes, Real Consequences: Rethinking Federal Power in the Age of AI and Internet-Based Crime" Washington College of Law's own Leyla Izquierdo, argues for the application of the Categorical Approach more consistently because both the internet and AI systems are interstate by design. Izquierdo focuses her analysis on the Wire Fraud Act, the Computer Fraud and Abuse Act, and federal money laundering statutes.

These pieces each reflect their others' unique and novel approach to criminal legal scholarship, as each explore niche areas of criminal legal practice. The Summer 2026 of the 16th Volume of our publication represents months of collaborative work between the Criminal Law Practitioner, its staff, and the faculty and staff of American University Washington College of Law. This semester has truly been a collaborative process and one full of love and dedication to criminal law scholarship. I'd like to thank each member of this process for their dedication. I hope this issue and these two incredible pieces serve as catalysts for meaningful, cutting-edge discussion on the novel issues that are facing our practice area. I hope this piece communicates the dedication, passion, and care that went in to getting it in your hands. As always, please contact us at clp@wcl.american.edu if you have any comments or questions.

Very Respectfully,

Isabel Capecci

Isabel V. Capecci
Editor-in-Chief


THE CRIMINAL LAW PRACTITIONER
EST. 2009

CALIFORNIA'S RACIAL JUSTICE ACT

BY JOHN E.B. MYERS[1]

INTRODUCTION

America has a shameful legacy of racism. At the same time, efforts to combat racism span the Nation's history. The post-Civil War amendments to the U.S. Constitution abolished slavery (13th Amendment) and guaranteed equal protection of the law (14th Amendment). In 1871, Congress passed Title 42, Section 1983, of the U.S. Code, the Ku Klux Klan Act, to fight the Klan and protect civil rights. Section 1983 allows citizens to sue state and local government officials for violations of constitutional rights. California's Tom Bane Civil Rights Act became law in 1987, allowing lawsuits against law enforcement. In 2020, the California Legislature added a new tool in the fight against bias, the Racial Justice Act (RJA) (Penal Code § 745). The RJA applies at all stages of the criminal justice process and to judges, attorneys, expert witnesses, jurors, and law enforcement.[2] This article focuses on law enforcement.

---

[1] John Myers, *Visiting Professor of Law*, UC Law San Francisco and reserve Police Officer, University of the Pacific and City of Ione.

[2] I'm aware that some prefer the term "criminal injustice system," *see, e.g.*, Alec Karakatsanis, *Unusual Cruelty: The Complicity of Lawyers in the Criminal Injustice System*, 1-5 (The New Press 2019). Others prefer "criminal legal system," because, apparently, they believe the system does not dispense justice. *See, e.g.*, Alma Magaña, *Public*

I. RJA's Five-Step Process

The RJA has five steps: (1) Defendant files a motion in court claiming an officer "exhibited bias or animus toward the defendant because of the defendant's race, ethnicity, or national origin;"[3] (2) Defendant presents enough evidence to establish a prima facie case of bias;[4] (3) If defendant proves a prima facie case, the judge orders discovery; (4) Following discovery the judge holds a hearing at which the defendant must prove bias by a preponderance of the evidence;[5] and (5) If defendant wins at the hearing, the judge orders a remedy.

A. Prima Facie Case

The Legislature deliberately made it easy for defendants to establish a prima facie case of bias.[6] The defendant presents facts that, *if true*, establish a likelihood of bias. The defendant does *not* have to prove his facts *are* true: only that his facts *might* be true. Statistical evidence that minorities are stopped or arrested at rates higher than their proportion of the population can be sufficient for a prima facie case.[7] Unless the defendant's evidence is obviously false, the judge accepts the defendant's evidence and ignores evidence that there was no bias.[8]

B. Discovery

When the defendant's evidence establishes a prima facie case, the judge orders the government to produce "all evidence relevant to a potential violation" of the RJA.[9]

Defender Discretion, 59 UC DAVIS L. REV. 885 (2025). Call me old fashioned but I'll continue with the older term criminal justice system because I believe the system—warts and all—dispenses justice most of the time.

3 Cal. Penal Code § 745(a)(1), (b) (2026).

4 *See* McDaniel v. Superior Court, 111 Cal. App. 5th 228, 248 (2025) ("the requisite showing at the discovery stage is a low bar"); Finley v. Superior Court, 95 Cal. App. 5th 12 (2023) (the Court of Appeal discusses the meaning of prima facie evidence, writing that prima facie evidence can be slight, just enough to create a reasonable inference of a fact. Prima facie evidence does not have to rule out contrary inferences).

5 Cal. Penal Code § 745(c) (1)-(2) (2026).

6 Act of Oct. 13, 2025, ch. 721, § 1, 2025 Cal. Stat. 1, legislative findings, Section (c) ("The Legislature reasserts the low threshold to establish a prima facie showing under" the RJA).

7 Act of Oct. 13, 2025, ch. 721, § 1, 2025 Cal. Stat. 1, § (c) ("The Legislature again emphasizes its rejection of McKleskey v. Kemp, 481 U.S. 279 (1987), and its intent that statistical evidence be sufficient for finding a prima facie case and may suffice to show an RJA violation."). *See also* Cal. Penal Code § 745(h)(1). For in-depth treatment of statical evidence, *see, e.g.*, Deepak Prekumar et al., *Empirical Analysis of Racial Disparities in Policing*, 65 SANTA CLARA L. REV. 267, 280 (2025).

8 *See* Bonds v. Superior Court, 318 Cal. Rptr. 3d 226 (2024) (Officer Cameron conducted a traffic stop of defendant and found an illegal concealed firearm. At an RJA hearing, the trial judge believed Officer Cameron's testimony that he could not tell the driver's race when he stopped the car. The Court of Appeal ruled the trial judge was wrong to credit Cameron's testimony because, even if the officer was telling the truth, the stop might have been based on unintentional bias.).

9 The Legislature intends broad discovery under the RJA. *See* Act of Oct. 13, 2025, ch. 721, § 1, 2025 Cal. Stat. 1, legislative findings, Section (b), Legislative findings and declarations: "The Legislature also intends that individuals must be afforded access to a broad range of relevant discovery to develop and support their potential RJA claims. Otherwise, they are left in the impossible position of having their claims rejected for want of the very data they seek. This is antithetical to the RJA."

Discovery under the RJA is likely broader than discovery already available to defendants under California's Reciprocal Discovery Act[10] and *Brady v. Maryland*.[11]

C. Hearing on Motion

Following discovery, the court holds a hearing at which the defendant must prove intentional or implicit bias by a preponderance of the evidence.[12] "The defendant does not have to prove intentional discrimination."[13] An officer who was not intentionally biased—who did everything by the book and with no conscious influence of race—can nevertheless be found to have violated the RJA through implicit bias. As the Court of Appeal put it in *Bonds v. Superior Court*,[14] "[A] defendant can seek relief regardless of whether the discrimination was purposeful or unintentional."[15]

D. Remedy

When a defendant prevails at an RJA hearing, the judge imposes a remedy. The judge could dismiss an enhancement (*e.g.*, use of a firearm during carjacking (PC § 12022.53(a)(5)), reduce a felony to a misdemeanor, or grant "any other remedy not prohibited by another law."[16] Under the RJA, defense attorneys are asking judges to suppress evidence (guns, drugs) found during searches that do *not* violate the Fourth Amendment.

II. Pros and Cons of the RJA

The goal of the RJA is laudable. As the Legislature said, "Because racial bias in the criminal legal system is the result of centuries of historical and embedded racial injustice, it requires bold, concerted, and ongoing efforts to undue."[17] Today, police academies, sheriffs, police chiefs, and the California Peace Officer Standards and Training agency (POST) devote considerable resources to training on bias, particularly implicit bias. No doubt much remains to be done. The question remains: Do the benefits of the RJA in its present form outweigh the problems it creates?

A. The RJA Prima Facie Showing is Meaningless

Several areas of California law require a party seeking relief in court to begin with a prima facie case. Thus, a petitioner must establish a prima facie case in employment

10 Cal. Penal Code § 1054.1.
11 Brady v. Maryland, 373 U.S. 83, 87 (1963).
12 Cal. Penal Code § 745(c)(2), (d).
13 *Id.*
14 *Bonds*, 318 Cal. Rptr. 3d at 230-31.
15 *Id.* at 823.
16 Cal. Penal Code § 745(e)(1)(D).
17 Act of Oct. 13, 2025, ch. 721, § 1, 2025 Cal. Stat. 1, § (f).

discrimination cases,[18] certain claims for resentencing,[19] and habeas corpus.[20] A prima facie case is not much, but it should be something: it should have some capacity to separate wheat from chaff. In employment discrimination, the plaintiff must present enough evidence to raise a reasonable inference of discrimination.[21] In resentencing, the court examines the record of conviction for evidence justifying a hearing on resentencing.[22]

The RJA views the world through a racial lens. As explained below, virtually anything police do, no matter how lawful, can be viewed as evidence of implicit bias. In the complete absence of bias, all a defendant must do to get an RJA hearing is provide statistics that members of his group are stopped or arrested more often than members of other groups. The statistics don't have to shed any light on the facts of the defendant's case.

B. RJA Discovery, An Unwise Windfall for the Defense?

California provides extensive statutory and constitutional discovery for defendants in criminal cases. If defense attorneys can get additional discovery—discovery that will impose significant burdens on prosecutors and police—defense attorneys will seek the discovery. That's their job. Given how easy it is under the RJA to establish a prima facie case and obtain discovery, it is difficult to see why defense attorneys would not file RJA motions in all cases involving minority defendants. Indeed, wouldn't it be ineffective assistance of counsel for a defense attorney to fail to file an RJA motion?

There is no evidence that the Legislature gave any thought to whether the cost in time and money of responding to an avalanche of RJA discovery demands will reduce racism. What is certain is that lawyers will act like lawyers and ask for the moon. Consider the discovery request in *People v. Allen*.[23] Officer Ahumada was on patrol when he spotted a fast-moving car make an abrupt stop at a stoplight. Ahumada followed the car, which made a turn and immediately parked. As Ahumada passed the car he observed tinted windows. After the officer passed the car, the driver did a U-turn and drove away from the officer. Ahumada initiated a traffic stop. The driver refused Ahumada's orders to completely roll down the window and turn off the car. The driver became verbally aggressive, rolled the window all the way up, and stopped communicating with the officer. Additional officers arrived. Officer Shafer banged on the windshield. Seconds later, Shafer unholstered his firearm and pointed it at the ground. The driver fled at high speed.

A year earlier, the same driver led police on a chase at speeds up to 120 miles an hour. In the current case, defendant was, charged with felony evading and reckless driving, the driver filed a motion under the RJA, claiming Officer Shafer's decision to draw his weapon was racist. The trial judge concluded there was no connection between

[18] Sendell v. Taylor-Listing, Inc., 115 Cal. Rptr. 3d 453, 471 (2010).
[19] People v. Lewis, 491 P.3d 309, 314 (Cal. 2021).
[20] In re Grinder, 114 Cal. App. 5th 845, 861 (2025).
[21] *Sandell*, 115 Cal. Rptr. 3d at 458.
[22] *Lewis*, 491 P.3d at 314.
[23] The People v. Keshaun T. Allen, No. D084607, 2025 WL 3525769, at * 3-5, (Cal. Ct. App. Dec. 9, 2025).

unholstering the weapon and race. The Court of Appeal ruled the trial judge was wrong, and discovery was ordered.

The driver's lawyer asked for an order that the District Attorney gather data on all times Officer Shafer unholstered his duty weapon, investigated or made an arrest for resisting arrest, or used or threatened force. Defense counsel also asked that Officer Shafer be ordered to disclose any instances where he unholstered his weapon and did not document it in a written report. The driver supported his discovery request with statistics that in San Diego County police stop Black drivers out of proportion to their numbers in the population.

The traffic stop in *People v. Allen* was lawful under the Fourth Amendment. There was no doubt the driver violated the law by fleeing. The trial judge saw no connection between drawing a firearm in a dangerous situation and race. Yet, under the RJA, the state must pour through an officer's career to document every occasion when he drew his weapon or used or threatened force. Decide for yourself whether such broad discovery helps reduce bias or amounts to a waste of time and money.

C. The RJA Punishes Lawful Behavior

The small number of RJA appellate cases to date (April 2026) reveals an uncomfortable reality for cops. Even when cops do everything by the book—full compliance with the Constitution, statutory law, and Department policy—they will be accused of racism in RJA proceedings. For example, under the Fourth Amendment, pretextual traffic stops are legal.[24] Suppose a deputy conducts a pretextual stop and discovers the gun used to murder a child. With the RJA, the defendant can claim that the stop—legal under the Fourth Amendment—was racist. The defendant does not have to prove the deputy was consciously or unconsciously biased. All the defendant has to do is offer statistical evidence of disproportionate stops. That done, the RJA requires the court to impose a remedy, and defense counsel will ask the court to suppress the gun.

Under *Terry v. Ohio*,[25] a police officer with reasonable suspicion that a detained person is armed and dangerous can perform a limited pat search for weapons. A long line of decisions state that in evaluating reasonable suspicion to search, cops can consider the fact that a suspect is wearing baggy clothes that could hide a weapon.[26]

In *Hernandez v. Superior Court*,[27] the defendant was wearing baggy clothing. The defendant filed an RJA claim against the searching officer, citing as evidence of bias a news report from National Public Radio that wearing baggy clothing is a proxy for race. The Court of Appeal agreed with defendant, writing, "Despite [the officer's] asserted reasons for conducting a pat search, i.e., lighting and baggy clothing, there remains the possibility that the officer's actions were a product of an implicit bias that associated things the officer did know, including the clothing Hernandez was wearing, with his race."[28]

---

24 *See generally* Whren v. United States, 116 S. Ct. 1769 (1996).
25 Terry v. State of Ohio, 88 S. Ct. 1868, 1873 (1968).
26 *See, e.g.*, People v. Collier, 83 Cal. Rptr. 3d 458, note 1.
27 Hernandez v. Super. Ct. of Santa Clara, 338 Cal. Rptr. 3d 741, 751 (2025).
28 *Id.*

Consider the facts in *Finley v. Superior Court*.[29] Officer Gunn observed a Buick parked in a high crime area of San Francisco. Gunn ran the license plate which came back to an Acura. Gunn turned on his emergency lights. The driver, Finley, told Gunn he had purchased the Buick a couple of weeks earlier. Finley provided documents establishing the Buick was not stolen. Gunn ran Finley's name and discovered he was on federal probation with a search clause. Gunn searched the car and discovered a loaded handgun without a serial number. Officer Gunn did exactly what the Fourth Amendment allows: Everything by the book. Nevertheless, Finley filed an RJA motion claiming the stop was based on Finley's race.

At the prima facie stage Finley cited: (1) Gunn ran Finley's plate for "no apparent logical non-racial reason,"[30] (2) Gunn's justification that Finley was parked "in a high-crime area is a notorious reference to neighborhoods with a high concentration of Black people;"[31] (3) Gunn ran Finley's name,[32] (4) a Sergeant on scene told other officers he did not want to discuss the situation on camera, (5) Gunn made a small error in his police report, and (6) Black people in San Francisco are more likely to be stopped than other groups. Under the RJA, the judge considers only evidence presented by the defendant, and ignores contrary evidence. In this case the judge made the mistake of believing Officer Gunn, so the Court of Appeal ruled in Finley's favor and ordered an RJA hearing.

The take away for cops is clear: Do everything lawfully; act for non-racist reasons: It doesn't matter. You will be accused of racism.

D. Curb Thy Tongue

If a cop uses intentionally racist language, there should be consequences. Language around race is a minefield, and it is easy to set off an explosion without intending to. In RJA proceedings, defense attorneys look for words that may evidence bias. The Legislature equated "dehumanizing and othering language"[33] with racism, referencing the words predator, monster, sociopath, terrorist, brute, thug, and gangster.[34] The Legislature criticized "gratuitous references to gangs, tattoos, nicknames, or neighborhoods."[35] In *R.D. v. Superior Court*,[36] a minor was charged in juvenile court with carrying a loaded firearm in public, resisting arrest, and lying to police.[37] The juvenile court judge violated the RJA by stating, "This is a serious gang banger we are dealing with."[38] The Legislature condemned "racially incendiary or coded words such as 'ghetto,' 'hood,' 'baby mama,'

---

29 Finley v. Super. Ct of Cty. & Cnty. Of San Francisco, 312 Cal. Rptr. 3d 907, 911 (2023).

30 *See id.* (noting that cops run plates for entirely legitimate reasons, including detecting stolen cars).

31 *See id.* (does this mean cops are racist when they work to keep citizens safe in areas where crime is rampant?).

32 *See id.* (it is normal, non-racist, practice to run names).

33 Act of Oct. 13, 2025, ch. 721, § 1, 2025 Cal. Stat. 1; Cal. Penal Code § 745 (West 2026).

34 *See* People v. Quintero, 328 Cal. Rptr. 3d 771, 775 (2024) (horrible kidnapping and rape in concert case against two defendants. In closing argument the prosecutor referred to the defendants as monsters and predators. The Court of Appeal concluded "the prosecution's use of the race-neutral terms 'monsters' and 'predators in closing argument did not violate the California Racial Justice Act . . . .").

35 *Id.*

36 R.D. v. Super. Ct. of Sacramento Cnty., 330 Cal. Rptr. 3d 155 (2025).

37 Cal. Penal Code § 745(f) (West 2026), The RJA applies in delinquency proceedings in juvenile court.

38 *R.D.*, 330 Cal. Rptr. 3d at 160.

or 'pimp.'"[39] In *Hernandez v. Superior Court*,[40] cops were criticized for uttering the terms "homie" and "primo."

There is a literature on "racism expressed through language."[41] Carey and Hewitt write, "[R]acism in language, which is referred to as discursive racism . . . is a form of racism that uses words that are rooted in stereotypical meaning, and typically includes racially tinged forms of everyday communication that sustain racism."[42] Carey and Hewitt provide examples: "No can do" and "Long time no see" were once used to mock Asian immigrants whose English was less than perfect. The term "inner city" is sometimes used to describe communities of color.[43] Using the term "Sup" to greet a Black person, rather than "What's happening," can be construed as racist.[44] The word "minority" is viewed by some as racist.[45]

Police officers avoid racist terms. Even in high stress situations involving fights and weapons, officers generally do an admirable job avoiding disrespectful language.[46] There is often a lot of gratuitous swearing—especially the F word—which drives command staff nuts, but seldom do patrol officers use racially tinged language in stressful situations. Nevertheless, with body cameras rolling, defense attorneys will scour the record for a single word or phrase that *might* be evidence of *possible* bias.[47] Because it is so easy for a defendant to establish a prima facie case under the RJA, and because the judge is not allowed to consider the officer's reasons for using particular words, any slip of the tongue, however unintentional, may lead to an RJA discovery order.

III. Equating Legitimate Law Enforcement Practices with Racism

POST teaches what it calls "Principled Policing in the Community. (PPC).[48] Among its many attributes, PPC favors "Monitoring areas of frequent criminal activity."[49] Is doing so racist? Because the RJA views law enforcement through a racialized lens, anything law enforcement does could be the product of racism. Thus, in *Bonds v. Superior Court*,[50] a defense expert witness opined that terms like "proactive enforcement" and "high crime area" are words of implicit bias.

39 Act of Oct. 13, 2025, ch. 721, § 1, 2025 Cal. Stat. 1.
40 Hernandez v. Super. Ct. of Santa Clara, 338 Cal. Rptr. 3d 741, 745 (2025).
41 Mia L. Carey & Amber A. Hewitt, *Words Matter: A Guide to Inclusive Language around Racial and Ethnic Identity*, at 5 (Washington D.C. Office of Human Rights and Mayor's Office of Racial Equity Apr. 2023).
42 *Id.*
43 *Id.* at 8.
44 *Id.* at 9.
45 *Id.* at 15.
46 Jeremy Story, *Chief's Corner: F-bombs Harm Everyone*, POLICE ONE, Aug. 06, 2025, https://www.police1.com/chiefs-sheriffs/chiefs-corner-f-bombs-harm-everyone.
47 *Id.*
48 Learning Domain 3, Principled Policing in the Community, Version 6.0, Commission on Peace Officer Standards and Training (POST) (2005).
49 *Id.* at 1-11.
50 Bonds III v. Super. Ct. of San Diego Cnty., 318 Cal. Rptr. 3d 226, 232 (2024).

IV. Is the Racial Justice Act Constitutional?

The RJA draws lines based on race, granting substantial benefits to minority group defendants and denying those benefits to non-minority defendants who are similarly situated. By the time *Brown v. Board of Education*[51] was decided in 1954, "[t]he time for making racial distinctions had passed."[52] In *Students for Fair Admissions, Inc. v. President and Fellows of Harvard College*,[53] the Supreme Court wrote, "Eliminating racial discrimination means eliminating all of it." And in *Palmore v. Sidoti*,[54] the Court stated that the core principle of the equal protection clause is "doing away with all governmentally imposed discrimination based on race."

Proponents of the RJA argue that minority and non-minority defendants are not similarly situated, and they have a point. The question is whether the Equal Protection Clause tolerates the blatant race-based line drawing at the heart of the RJA.

Conclusion

The RJA is based on a wonderful idea: Eliminate racism from the criminal justice system. Because the RJA views almost everything as potentially racist, however, it is fair to ask whether the Act in its current form does more good than harm. Is it good public policy to allow defendants who committed heinous crimes to have the charges reduced or to escape responsibility altogether when there is no evidence of bias apart from statistics that have only a tangential, if any, relationship to the case? Or would justice be better served by amending the RJA so that statistical evidence is admissible at the prima facie and the hearing stages of RJA proceedings, but is not alone sufficient to prove bias?

Does society benefit at the prima facie stage from the RJA rule that the judge is only allowed to consider the defendant's evidence suggesting possible bias, and must ignore altogether the government's evidence that race played no role? Would the RJA be improved by allowing a "fair fight" at the prima facie stage, allowing the judge to consider all the relevant evidence, not just half?

Finally, is it wise to brand cops who are trying to follow the law and treat people with respect racist because of statistics? Make no mistake, that is what is happening under the RJA. Assuming the RJA is constitutional, with a few sensible amendments, the Act could become the tool the Legislature intended.

[51] Brown v. Board of Ed. of Topeka, Shawnee County, Kan., 347 U.S. 483 (1954).
[52] Students for Fair Admissions, Inc. v. President and Fellows of Harvard College, 600 U.S. 181, 204 (2023).
[53] *Id.* at 206.
[54] Palmore v. Sidoti, 466 U.S. 429, 432 (1984).


THE CRIMINAL LAW PRACTITIONER
EST. 2009

ARTIFICIAL CRIMES, REAL CONSEQUENCES: RETHINKING FEDERAL POWER IN THE AGE OF AI AND INTERNET-BASED CRIME

BY LEYLA IZQUIERDO[1]

INTRODUCTION

Artificial intelligence (AI) is transforming cybercrime with its increasing ability to seamlessly mimic human behavior and rapidly generate content, enabling even unskilled actors to launch sophisticated attacks, including AI-enhanced spear phishing campaigns and executive impersonation to commit fraud.[2] Losses from fraud driven by generative AI (GenAI) are projected to soar from $12.3 billion in 2023 to $40 billion by 2027—a compound annual growth rate of 32 percent.[3] The Department of Justice (DOJ) has cautioned that "[w]

[1] Leyla Izquierdo, J.D. Candidate, May 2027, American University Washington College of Law.

[2] See U.S. Dep't of Homeland Sec., Pub.-Priv. Analytic Exch. Program, *Impact of Artificial Intelligence on Criminal and Illicit Activities*, 18–19 (2024), https://www.dhs.gov/sites/default/files/2024-10/24_0927_ia_aep-impact-ai-on-criminal-and-illicit-activities.pdf (describing how AI fills skill gaps and enables less-skilled actors to carry out a range of crimes from spear phishing, a targeted phishing attack via malicious emails or texts, and executive impersonation, which uses deepfake audio or video to mimic executives).

[3] Satish Lalchand et al., *Generative AI is expected to magnify the risk of deepfakes and other fraud in banking*, DELOITTE CTR. FOR FIN. SERVS. (May 29, 2024), https://www.deloitte.com/us/en/insights/industry/financial-services/deepfake-banking-fraud-risk-on-the-rise.html.

here AI is deliberately misused to make white-collar crime significantly more serious," prosecutors will pursue harsher sentences for both individual and corporate defendants.[4] Yet prosecutors remain bound to federal criminal statutes written long before the digital age, many of which contain an interstate commerce element, giving rise to conflicting interpretations among the federal circuits over whether internet-based crimes inherently satisfy that element.[5] As crimes move further into the digital space and economic risks rise, clarifying the statutory basis for federal prosecution has become increasingly urgent.[6]

In 2025, AI crimes reported in the United States ranged from a deepfake scam that cloned "General Hospital" star Steve Burton and drained a woman's life savings, to the DOJ's indictment of a $703 million Medicare fraud ring that used AI to fabricate "consent" call recordings to support fraudulent Medicare claims.[7] These incidents illustrate the breadth of AI-enabled fraud schemes already confronting federal and state law enforcement.[8] They also underscore the practical significance of resolving the ongoing circuit split, which would bring uniformity to whether federal prosecutors may bring charges, whether cases may proceed in federal court, and what penalties defendants may ultimately face.[9]

Most recently, the First Circuit adopted one of the most expansive jurisdictional interpretations to date regarding internet use in white-collar crime prosecutions in *United States v. O'Donovan*,[10] holding that internet use alone suffices to satisfy the "interstate or foreign commerce" requirement of the Wire Fraud Act (WFA), 18 U.S.C. § 1343.[11] Even in the absence of evidence that the communications crossed state lines, the court concluded that "proof that the defendant transmitted the iMessages over the Internet was sufficient to satisfy the interstate-commerce element" for wire fraud.[12] In doing so, the First Circuit joined the Third and Fifth Circuits in adopting what is effectively a "categorical approach," under which internet-based conduct is treated as presumptively interstate.[13] This approach

4 Lisa Monaco, Deputy Attorney General, *Remarks at the American Bar Association's 39th National Institute on White Collar Crime* (Mar. 7, 2024), https://www.justice.gov/archives/opa/speech/deputy-attorney-general-lisa-monaco-delivers-keynote-remarks-american-bar-associations.

5 Valeria G. Luster, *Let's Reinvent the Wheel: The Internet as a Means of Interstate Commerce in* United States v. Kieffer, 67 OKLA. L. REV. 589, 589–90 (2015).

6 *Id.* at 591; *see also* U.S. Dep't of Homeland Sec., *supra* note 2, at 36.

7 Kevin Ozebek, *Woman Conned Out of Life Savings by Scammers Using AI to Pose as 'General Hospital' Star*, ABC7 (Aug. 26, 2025), https://abc7nyabc7.com/post/los-angeles-woman-conned-life-savings-scammers-using-ai-pose-general-hospital-star-steve-burton/17655567/; Press Release, U.S. Att'y's Off., N. Dist. of Tex., *Four Individuals Charged in Northern District of Texas with Health Care Fraud Schemes Totaling over $210 Million as Part of National Takedown* (July 1, 2025), https://www.justice.gov/usao-ndtx/pr/four-individuals-charged-northern-district-texas-health-care-fraud-schemes-totaling.

8 *See* Ozebek, *supra* note 7 and accompanying text.

9 *See* Catherine Beal, *The Very Interstate Nature of the Internet? Establishing Uniform Requirements for Internet Transmissions Within Interstate and Foreign Commerce*, 32 AM. U. J. GENDER, SOC. POL'Y & L. 383, 386–387 (2024) (arguing that resolving the circuit split would establish a uniform jurisdictional test and provide clearer prosecutorial guidance).

10 United States v. O'Donovan, 126 F.4th 17, 35–36 (1st Cir. 2025).

11 *Id.*; 18 U.S.C. § 1343.

12 *O'Donovan*, 126 F.4th at 36.

13 *See* Elkan Abramowitz & Jonathan Sack, *The Internet, Interstate Commerce And Wire Fraud*, N.Y. L.J., Mar. 14, 2025, https://static.maglaw.com/docs/Abramowitz%20Sack%20NYLJ%203.14.25.pdf (explaining that the First Circuit aligned with circuits treating internet use as sufficient to establish interstate commerce and noting the Second Circuit's unpublished endorsement of that reasoning).

stands in sharp contrast to the "evidentiary approach" adopted by the Ninth and Tenth Circuits, which requires proof that a charged transmission actually crossed state lines or otherwise affected interstate commerce.[14]

The growing focus of federal agencies on AI-enabled white-collar crime makes the lack of a uniform approach especially consequential.[15] Following then–DOJ Deputy Attorney General Lisa Monaco's March 2024 statement that "[f]raud using AI is still fraud," subsequent criminal prosecutions have reinforced that position, with the DOJ continuing to apply existing fraud statutes aggressively to AI-augmented schemes in 2025.[16] The Securities and Exchange Commission (SEC) has likewise expanded its enforcement efforts to target fraud committed using AI and other emerging technologies.[17] Meanwhile, the Federal Bureau of Investigation (FBI) issued public service announcements in 2024 and 2025 warning the public about GenAI-enabled fraud and urging the adoption of safeguards such as using family code words to verify identity, limiting the availability of personal information online, and reporting suspected fraud to IC3.gov, demonstrating the federal government's sustained focus on AI-enabled fraud.[18] Complementing these efforts, the U.S. Department of the Treasury has addressed AI-enabled fraud through both policy and oversight, maintaining a department-wide framework governing the use and risks of AI in the financial sector and by issuing alerts that provide red flag indicators to help financial institutions identify fraud schemes involving GenAI.[19]

Most contemporary AI systems are cloud-based, with data stored and processed on remote servers housed in geographically dispersed data centers that operate over the globally interconnected internet.[20] Because these systems operate on infrastructure that is interstate by design, treating their use as categorically interstate does not erase constitutional limits

[14] United States v. Wright, 625 F.3d 583, 595, 597 (9th Cir. 2010); United States v. Kieffer, 681 F.3d 1143, 1155 (10th Cir. 2012).

[15] *See* Bruce D. Sokler et al., *DOJ Deputy Chief Announces "Stiffer Sentences" for AI-Related White-Collar Crime — AI*, THE WASH. REP. (Mar. 14, 2024), https://www.mintz.com/insights-center/viewpoints/2024-03-14-doj-deputy-chief-announces-stiffer-sentences-ai-related-white (noting the DOJ's intensified enforcement posture toward AI-augmented misconduct and its intent to seek enhanced penalties under existing federal statutes).

[16] *See* Monaco, *supra* note 4; Eric Rosen, *AI-Powered Fraud and DOJ's Expanding Enforcement Toolkit: What Businesses and Executives Need to Know Now*, DYNAMIS LLP, https://www.dynamisllp.com/knowledge/ai-fraud-enforcement-doj-defense-strategies-2025.

[17] Press Release, Sec. & Exch. Comm'n, SEC Announces Cyber and Emerging Technologies Unit to Protect Retail Investors (Feb. 20, 2025), https://www.sec.gov/newsroom/press-releases/2025-42#:~:text=The%20Securities%20and%20Exchange%20Commission,artificial%20intelligence%20and%20machine%20learning.

[18] *Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud*, FED. BUREAU OF INVESTIGATION, PUB. SERV. ANNOUNCEMENT NO. I-120324-PSA (Dec. 3, 2024), https://www.ic3.gov/PSA/2024/PSA241203; *Senior U.S. Officials Impersonated in Malicious Messaging Campaign*, FED. BUREAU OF INVESTIGATION, PUB. SERV. ANNOUNCEMENT NO. I-051525-PSA (May 15, 2025), https://www.ic3.gov/PSA/2025/PSA250515.

[19] *Treasury and Artificial Intelligence*, U.S. DEP'T OF THE TREASURY, https://home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/treasury-and-artificial-intelligence; *FinCEN Issues Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions*, FIN. CRIMES ENF'T NETWORK (Nov. 13, 2024), https://www.fincen.gov/news/news-releases/fincen-issues-alert-fraud-schemes-involving-deepfake-media-targeting-financial.

[20] *See Cloud AI Adoption Soars: 9.7 Million Developers Deploy AI in the Cloud*, EVANS DATA CORP., https://evansdata.com/blog/cloud-ai-adoption-soars.php [hereinafter *Cloud AI Adoption Soars*] (describing the cloud as the leading deployment environment for AI); *see infra* Section I.A.1.

but instead applies them to modern technology.[21] This approach, however, raises concerns that it affords prosecutors broad discretion, enabling forum shopping and the stacking of charges under statutes such as the WFA, the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, and the federal money laundering statutes, 18 U.S.C. §§ 1956–1957.[22] Nevertheless, existing safeguards mitigate these risks.[23] DOJ charging policies require prosecutors to pursue cases only where a substantial federal interest is served, courts provide oversight to limit improper venue selection, and sentencing guidelines calibrate punishment to the seriousness of the conduct.[24]

This Comment argues that the categorical approach should be consistently applied because the internet and cloud-based AI systems are interstate by design.[25] The "interstate or foreign commerce" element appears in numerous criminal statutes, including 18 U.S.C. § 2251 and § 2252 (child pornography offenses) and 18 U.S.C. § 2314 (transportation of stolen goods).[26] This Comment, however, focuses on the WFA, the CFAA, and the federal money laundering statutes because they are frequently invoked in technology-driven prosecutions and reflect distinct formulations of the interstate-commerce element.[27] Recent prosecutions such as *United States v. Smith*[28] and *United States v. Charolia*[29] illustrate why categorical reasoning is necessary. *Smith*'s AI-generated music fraud relied on billions of automated streams across global platforms, while *Charolia*'s scheme used fabricated AI recordings transmitted abroad to bill Medicare for millions of dollars in false claims.[30] Both crimes depended on interstate systems by design, and conditioning jurisdiction on particular cross-border transmissions would have elevated routing mechanics over the interstate nature of the crime. Unlike the evidentiary approach, which risks arbitrary outcomes based on packet routing or server location, the categorical approach secures federal jurisdiction over AI-driven misconduct while aligning enforcement with the technological realities of

21 United States v. MacEwan, 445 F.3d 237, 245 (3rd Cir. 2006) (holding that the internet is a channel and instrumentality of interstate commerce).

22 *See, e.g.*, Jamie Williams, *New Federal Guidelines for Computer Crime Law Do Nothing to Reign In Prosecutorial Overreach Under Notoriously Vague Statute*, ELEC. FRONTIER FOUND. (Oct. 31, 2016), https://www.eff.org/deeplinks/2016/10/what-were-scared-about-halloween-prosecutorial-discretion-under-notoriously-vague (discussing how vague federal computer crime statutes permit charge stacking and expansive prosecutorial discretion); *see also* 18 U.S.C. § 1030 (Computer Fraud and Abuse Act); 18 U.S.C. §§ 1956–1957 (money laundering).

23 *See* U.S. Dep't of Just., Justice Manual §§ 9-27.220–240 (requiring federal prosecution only where there is probable cause, a substantial federal interest, and no effective prosecution available in another jurisdiction); *see infra* Section II.B.

24 *See* Justice Manual, *supra* note 23; United States v. Auernheimer, 748 F.3d 525, 533–36 (3d Cir. 2014) (vacating CFAA and identity-fraud convictions for improper venue); U.S. Sent'g Comm'n, U.S. Sent'g Guidelines Manual § 2B1.1 cmt. background (Nov. 1, 2025) (explaining that loss and offense characteristics measure the seriousness of fraud offenses).

25 *See* Michele Martinez Campbell, *The Kids Are Online: The Internet, the Commerce Clause, and the Amended Federal Kidnapping Act*, 14 U. PA. J. CONST. L. 215, 243–45 (2011) (describing the internet as an instrumentality of interstate commerce).

26 *See* 18 U.S.C. §§ 2251, 2252, 2314.

27 *See infra* Section I.C.

28 No. 24 Cr. 504 (S.D.N.Y. filed Aug. 26, 2024).

29 No. 1:25-cr-00304 (N.D. Ill. filed June 5, 2025).

30 *Smith*, No. 24 Cr. 504, ¶¶ 1, 25; *Charolia*, No. 1:25-cr-00304 ¶ 7 (Counts One Through Four).

modern fraud.[31]

This Comment proceeds as follows. Part I provides the necessary background by explaining the infrastructure of AI and the internet, surveying recent AI-driven white-collar prosecutions, examining the circuit split over how courts analyze the interstate-commerce element in internet-based cases, and outlining the statutory framework of the WFA, the CFAA, and the federal money laundering statutes.[32] Part II argues that the categorical approach embraced by the First, Second, Third, and Fifth Circuits provides the sounder framework.[33] It explains that modern internet and AI infrastructure fragments, routes, and recombines data across servers in multiple states, making digital conduct inherently interstate.[34] It further shows that this interpretation respects Congress's authority to regulate the channels and instrumentalities of commerce while ensuring that federal law remains enforceable against AI-driven misconduct.[35] This Comment concludes that, absent legislative reform, courts should continue to apply the categorical approach to preserve consistency and fairness in an era when digital conduct rarely respects state borders.[36]

I. Background

A. The Infrastructure of Artificial Intelligence (AI) and the Internet

While there is no single, simple definition of AI, a recent and influential one appears in section 238(g) of the National Defense Authorization Act (NDAA) for Fiscal Year 2019, which has been referenced in Executive Order 13960 and adopted by agencies such as the National Aeronautics and Space Administration.[37] Under the FY2019 NDAA, AI refers to computer systems that operate with limited human oversight, learn from experience and data, perform tasks requiring human-like cognition or perception, employ machine-learning techniques, or act rationally to achieve goals.[38] AI is classified into four categories based on functionality: reactive machines, limited memory machines, theory-of-mind AI, and self-aware AI.[39] Reactive and limited memory machines currently exist, whereas the other two remain theoretical.[40] Reactive Machine AI are systems that have no memory and are task-specific, meaning that a given input always produces the same

[31] *See* United States v. O'Donovan, 126 F.4th 17, 24–25 (1st Cir. 2025) (contrasting categorical and evidentiary approaches to internet transmissions).
[32] *See infra* Section I.A–C.
[33] *See infra* Section II.A–E.
[34] *See infra* Section II.A–E.
[35] *See infra* Section II.A–E.
[36] *See infra* Section III/ Conclusion.
[37] *What Is Artificial Intelligence?*, NASA, https://www.nasa.gov/what-is-artificial-intelligence (last visited Aug. 20, 2025); *see also* Exec. Order No. 13,960, 85 Fed. Reg. 7899 (Dec. 8, 2020) (incorporating the NDAA definition of AI into federal policy).
[38] National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 238(g), 132 Stat. 1636, 1697–98 (2018).
[39] *Understanding the different types of artificial intelligence*, IBM, https://www.ibm.com/think/topics/artificial-intelligence-types (last visited Aug. 20, 2025).
[40] *Id.*

output.[41] Unlike Reactive Machine AI, Limited Memory AI imitates brain neurons and uses both past and present data to select actions likely to achieve a desired outcome.[42] As these systems are trained on more data, their performance improves, but they do not retain that data as long-term experiential memory like a human brain does.[43]

Most modern AI is considered Limited Memory AI.[44] GenAI, a form of Limited Memory AI, relies on deep learning models, a subset of machine learning that "can create complex original content such as long-form text, high-quality images, realistic video or audio and more in response to a user's prompt or request."[45] GenAI systems generally operates in three phases: (1) training a deep learning foundation model on vast amounts of raw, unstructured, unlabeled data;[46] (2) tuning the model for specific applications by feeding it labeled, application-specific prompts and corresponding correct outputs through techniques such as fine-tuning or reinforcement learning with human feedback; and (3) generating outputs that are evaluated and retuned to improve quality and accuracy.[47] Once deployed, these systems generate original outputs autonomously "that are often indistinguishable from human-created content."[48] Examples of GenAI tools include ChatGPT, Google Gemini (formerly Bard), Midjourney, and Copilot, which are capable of generating content such as text, images, and software code in response to user prompts.[49] Yet, while AI developers and engineers understand the technical structure of GenAI, the precise inner workings remain too complex to decipher.[50] That is because what the neural network layers are actually doing to perform the creative task is not fully understood.[51]

While some AI systems are built and trained on local infrastructure, GenAI is increasingly becoming cloud-based, relying on servers housed in data centers around the world and accessed over the internet.[52] Accordingly, a basic understanding of how the

41 *See 4 Types of AI: Getting to Know Artificial Intelligence*, COURSERA, https://www.coursera.org/articles/types-of-ai (last visited Aug. 20, 2025).

42 *Id.*

43 *Id.*

44 *Artificial intelligence (AI): a simple-to-understand guide*, GOOGLE CLOUD, https://cloud.google.com/learn/what-is-artificial-intelligence (last visited Aug. 20, 2025).

45 *Types of AI*, *supra* note 39; *What is artificial intelligence (AI)?*, IBM, https://www.ibm.com/think/topics/artificial-intelligence (last visited Aug. 20, 2025).

46 *What is generative AI?*, IBM, https://www.ibm.com/think/topics/generative-ai? (last visited Aug. 20, 2025); *see also What Is Unstructured Data?*, BOX, https://www.box.com/resources/what-is-unstructured-data (last visited Apr. 8, 2026) (defining unstructured data as information that comes in multiple formats and does not follow a fixed model for analyzing its contents); Abid Ali Awan, *What Is Unlabeled Data?*, DATACAMP (July 4, 2023), https://www.datacamp.com/blog/what-is-unlabeled-data (defining unlabeled data as data lacking identifiers, classifications, tags, or labels).

47 *What is generative AI?*, *supra* note 46.

48 *What Is Generative AI?*, GEEKSFORGEEKS, https://www.geeksforgeeks.org/artificial-intelligence/what-is-generative-ai/ (last updated Dec. 9, 2025).

49 Greg Pavlik, *What Is Generative AI (GenAI)? How Does It Work?*, ORACLE CLOUD INFRASTRUCTURE (Feb. 11, 2025), https://www.oracle.com/artificial-intelligence/generative-ai/what-is-generative-ai/.

50 *Id.*

51 *See id.* (explaining that what a model such as GPT-3.5 is doing internally, "what it's thinking," may or may not ever be fully understood).

52 *Understanding Cloud-based Generative AI*, NUTANIX (Nov. 4, 2024), https://www.nutanix.com/info/artificial-intelligence/generative-ai; *What is the cloud?*, CLOUDFLARE, https://www.cloudflare.com/learning/cloud/what-is-the-cloud/ (last visited Sep. 4, 2025).

internet functions is essential. The internet is a vast collection of networks that "connects millions of computers, people, and other devices from around the world."[53] It operates by breaking data into packets, which are then translated into bits that travel through various networking devices such as routers and switches to get to their destination.[54] Sending packets between devices requires protocols such as the Internet Protocol (IP) for devices on different networks.[55] Every device connected to the internet is part of a network and is assigned a unique IP address, which allows packets to be sent and delivered to the correct destination.[56] When packets arrive at their destination, packets are processed using protocols such as the Transmission Control Protocol (TCP), which ensures that all packets arrive in order, and the Hypertext Transfer Protocol (HTTP), which formats and interprets the data for websites and applications.[57]

1. Data Transmission: AI and the Internet

Much of the evolution of the internet as a network of networks has been driven by economics and national policy rather than by performance considerations.[58] Large corporate networks, such as Internet Service Providers (ISPs), interconnect at network access points, allowing internet traffic to flow seamlessly across independently operated networks.[59] Therefore, although ISPs differ in their geographic coverage, with some spanning multiple continents and others serving narrow regional areas, they are collectively interconnected, meaning every computer on the internet connects to every other.[60] Accordingly, when a user accesses a webpage from home, the request travels through the user's router and modem and then onto the ISP's infrastructure, at which point the data leaves the premises and enters the global network.[61] These backbone interconnections, combined with geographically dispersed data centers that support network infrastructure, render internet traffic almost inherently interstate, consistent with the Federal Communications Commission's recognition that broadband internet access is jurisdictionally interstate.[62]

Cloud computing builds on this same global routing system by shifting computing

---

53 *What Is the Internet?*, LENOVO GLOSSARY, https://www.lenovo.com/us/en/glossary/what-is-internet/ (last visited Sep. 4, 2025); *see also How does the Internet work?*, CLOUDFLARE, https://www.cloudflare.com/learning/network-layer/how-does-the-internet-work/ (last visited Sep. 4, 2025) (defining a network as interconnected computers that exchange information).

54 *How does the Internet work?*, *supra* note 53.

55 *Id.*; *see also What Is the Internet Protocol (IP)?*, CLOUDFLARE, https://www.cloudflare.com/learning/network-layer/internet-protocol/ (last visited Sep. 4, 2025) (defining a protocol as "a standardized way of doing certain actions and formatting data").

56 *What Is the Internet Protocol (IP)?*, *supra* note 55.

57 *Id.*

58 James F. Kurose & Keith W. Ross, *Computer Networking: A Top-Down Approach* 32 (6th ed. 2013).

59 Jeff Tyson, *How Internet Infrastructure Works*, STANFORD UNIV., https://web.stanford.edu/class/msande91si/www-spr04/readings/week1/Howstuffworks.htm (last visited Sep. 4, 2025).

60 *Id.*; Kurose & Ross, *supra* note 58.

61 *How Data Travels Across the Internet*, HENG LU, https://heng.lu/how-data-travels-across-the-internet/ (last visited Sep. 4, 2025); *What Is the Internet Protocol (IP)?*, *supra* note 55.

62 Federal Communications Commission, *Appropriate Regulatory Treatment for Broadband Access to the Internet Over Wireless Networks*, WT Docket No. 07-53, Declaratory Ruling, ¶¶ 18, 28 (Mar. 23, 2007).

and storage away from the user's device and local premises and onto remote servers located in data centers that are accessed over the internet rather than housed in physical locations.[63] These data centers support a wide range of services, such as storage, hosting, and general-purpose computing, whereas AI data centers are optimized for high-performance workloads, enabling parallel processing, real-time analysis of large datasets essential for AI training and inference, and the execution of complex algorithms.[64] Today, many cloud platforms integrate AI capabilities that combine the scalability, cost efficiency, flexibility, and ease of data analysis and sharing associated with cloud computing with access to high-performance computational infrastructure.[65] Because cloud computing abstracts away the physical location of AI hardware, cloud-based AI systems permit remote access to advanced AI computation, rendering such activity far more likely than traditional internet uses to cross state lines or national borders.[66]

2. AI-Driven White-Collar Crimes and Federal Prosecution

As highlighted in this Comment's Introduction, recent federal prosecutions of white-collar crimes show how AI, particularly Limited Memory AI and its generative forms, has already been leveraged in large-scale fraud schemes in the United States.[67] Notably, while GenAI is becoming a daily tool for nearly 40 percent of U.S. adults aged 18–64 and is projected to be adopted by more than 80 percent of businesses by 2026, it has also been widely documented as a tool in ransomware, investment scams, romance scams, and deepfake-driven schemes.[68] These developments have prompted federal enforcement actions and agency warnings.[69]

In 2024, prosecutors in the Southern District of New York brought the first criminal case involving AI-assisted music streaming fraud with *United States v. Michael Smith*.[70] This manipulation triggered more than $10 million in fraudulent royalty payments that should have gone to musicians, songwriters, and other rights holders whose works were legitimately streamed.[71] According to the sealed indictment, Smith purchased hundreds of thousands of songs created with AI and uploaded them to streaming platforms such

63 *Understanding Cloud-based Generative AI*, *supra* note 52.

64 *What is the Difference Between Cloud and AI Data Centers?*, CYFUTURE CLOUD, https://cyfuture.cloud/kb/ai-data-center/what-is-the-difference-between-cloud-and-ai-data-centers (last visited Sep. 4, 2025).

65 *Id.*

66 John Villasenor, *The Tension Between AI Export Control and U.S. AI Innovation*, BROOKINGS (Sep. 24, 2024), https://www.brookings.edu/articles/the-tension-between-ai-export-control-and-u-s-ai-innovation.

67 *See supra* Introduction.

68 *Rapid Adoption of Generative AI*, FED. RSRV. BANK OF ST. LOUIS, (Sep. 4, 2024), https://www.stlouisfed.org/on-the-economy/2024/sep/rapid-adoption-generative-ai; *Gartner Says More Than 80% of Enterprises Will Have Used Generative AI APIs or Deployed Generative AI–Driven Applications by 2026*, GARTNER (Oct. 11, 2023), https://www.gartner.com/en/newsroom/press-releases/2023-10-11-gartner-says-more-than-80-percent-of-enterprises-will-have-used-generative-ai-apis-or-deployed-generative-ai-enabled-applications-by-2026.

69 Monaco, *supra* note 4.

70 Sealed Indictment, United States v. Smith, No. 24 Cr. 504 (S.D.N.Y. filed Aug. 26, 2024); Press Release, U.S. ATT'Y'S OFF. S. DIST. OF N.Y., *North Carolina Musician Charged with Music Streaming Fraud Aided by Artificial Intelligence* (Sep. 4, 2024), https://www.justice.gov/usao-sdny/pr/north-carolina-musician-charged-music-streaming-fraud-aided-artificial-intelligence.

71 *Smith*, No. 24 Cr. 504, at ¶ 1.

as Spotify, Apple Music, and Amazon Music.[72] To disguise their origins, he used AI to generate random song titles and artist names so the recordings appeared to be the work of real musicians.[73] He then created thousands of bot accounts under fake identities, despite agreeing to platform terms that explicitly prohibited streaming manipulation.[74] Using cloud services, macros (small pieces of automated code), and other automation, Smith hard-coded the bot accounts to stream his AI-generated songs billions of times, inflating play counts and creating the illusion of genuine listener demand.[75]

Prosecutors charged Smith with conspiracy to commit wire fraud (18 U.S.C. § 1349), wire fraud (18 U.S.C. § 1343), and conspiracy to commit money laundering (18 U.S.C. § 1956(h)), each carrying a maximum sentence of twenty years.[76] Because the platforms' infrastructure and royalty systems spanned multiple states and countries, the indictment stressed that the scheme necessarily operated on an interstate and international scale.[77] The indictment alleged that Smith "sent and received, and caused others to send and receive, emails and other electronic communications, to and from the Southern District of New York and elsewhere, in furtherance of [the] scheme."[78] It also noted that he used the "proceeds of some form of unlawful activity . . . which transaction affected interstate and foreign commerce and involved the use of a financial institution which was engaged in, and the activities of which affected, interstate and foreign commerce."[79] The indictment further highlighted Smith's use of "cloud computer services so that he could use many virtual computers at the same time."[80]

Less than a year later, in June 2025, the DOJ unveiled its annual nationwide health care fraud takedown, charging over 320 defendants across 36 federal districts with schemes totaling over $14.6 billion.[81] Among the most alarming prosecutions was *United States v. Charolia*,[82] a $703 million operation in which defendants connected to a Pakistan-based call center allegedly obtained Medicare beneficiary identifiers by hacking into websites, scraping public data, and creating deceptive websites.[83] The indictment further alleges that the defendants then used AI to fabricate audio recordings "that purportedly demonstrated beneficiaries consenting to the receipt of over-the-counter COVID-19 test kits."[84] These deepfake-style recordings were submitted as proof to Medicare, enabling the conspirators to bill the government for unnecessary or entirely fictitious at-home COVID-19 test kits and other medical items.[85] Of the approximately

[72] *Id.* ¶¶ 1, 23–24.
[73] *Id.* ¶ 23.
[74] Press Release, U.S. ATT'Y'S OFF. S. DIST. OF N.Y., *supra* note 70.
[75] *Id.* ¶ 26.
[76] Press Release, U.S. ATT'Y'S OFF. S. DIST. OF N.Y., *supra* note 70.
[77] *Smith*, No. 24 Cr. 504, at ¶¶ 34, 37.
[78] *Id.* ¶ 32.
[79] *Id.* ¶ 37.
[80] *Id.* ¶ 12(a).
[81] Press Release, U.S. ATT'Y'S OFF. N.D. ILL., *National Health Care Fraud Takedown Results in Charges Against 324 Individuals, Including 13 in Northern District of Illinois* (July 1, 2025), https://www.justice.gov/usao-ndil/pr/national-health-care-fraud-takedown-results-charges-against-324-individuals-including.
[82] *Id.*; Sealed Indictment, United States v. Charolia, No. 1:25-cr-00304 (N.D. Ill. filed June 5, 2025).
[83] *Charolia*, No. 1:25-cr-00304 at ¶ ¶ 3–4, 20 (Counts One Through Four).
[84] *Id.* ¶ 7 (Counts One Through Four).
[85] *Id.* ¶ ¶ 7, 20 (Counts One Through Four).

$703 million in fraudulent claims, approximately $418 million was paid, and the government seized about $45 million from related accounts.[86]

Prosecutors charged the defendants with health care fraud (18 U.S.C. § 1347), conspiracy to defraud the United States and to sell or distribute beneficiary identifiers (18 U.S.C. § 371; 42 U.S.C. § 1320a-7b(b)(4)), and money laundering conspiracy (18 U.S.C. § 1956(a)(1)(B)(i)).[87] The indictment emphasized that AI was central to the fraud, alleging that Charolia and his co-conspirators "created and distributed to [U.S.-based providers] fabricated records and fake recordings" to support fraudulent Medicare reimbursement claims, underscoring the scheme's interstate and international scope.[88] It further explained that the AI generated recordings purportedly demonstrated beneficiaries' consent to receive over the counter COVID-19 test kits.[89] The indictment also alleged that at least $45,100,161 in payments were funneled through shell companies incorporated in Wyoming and Missouri, including Mavens, Khoka, and VirtuVista, before being diverted abroad to Pakistan and the United Arab Emirates.[90]

These two cases show that AI is no longer a speculative concern but an active tool in complex, high-dollar fraud schemes.[91] They also illustrate the government's willingness to treat AI as a core component of the charged conduct, weaving its use directly into allegations of interstate and foreign commerce.[92] At the policy level, momentum for a federal moratorium on state AI regulation has collapsed.[93] In July 2025, the U.S. Senate removed the proposed moratorium from the draft federal budget bill, leaving federal preemption of state AI regulation unlikely.[94] With the federal government stepping back, attention has shifted to state-level AI regulation, including Texas's Responsible Artificial Intelligence Governance Act.[95] This result makes these cases all the more significant: even as comprehensive legislative frameworks stall, prosecutors continue to confront AI-enabled crimes, some of which, as in *Charolia*, are transnational in scope, and use existing federal statutes to prosecute them.[96]

---

86 *Id.* ¶¶ 20–21 (Counts One Through Four).

87 *Id.* at 17–18, 19, 24.

88 *Id.* ¶ 7 (Counts One Through Four).

89 *Id.*

90 *Id.* ¶ 21 (Counts One Through Four); *Id.* ¶¶ 12–14 (Count Six).

91 *See* Press Release, U.S. ATT'Y'S OFF. S. DIST. OF N.Y., *supra* note 70; Press Release, U.S. ATT'Y'S OFF. N.D. ILL., *supra* note 81.

92 *Id.*

93 Justin Hendrix, *US Senate Drops Proposed Moratorium on State AI Laws Preemption Proposal from Budget Vote*, TECH (July 1, 2025), https://www.techpolicy.press/-senate-drops-proposed-moratorium-on-state-ai-laws-in-budget-vote/.

94 *Id.*

95 *See* Omar Tene, Bethany P. Wither & Reema Moussa, *Federal AI Moratorium Dies on the Vine as Senate Passes the One Big Beautiful Bill Act*, GOODWIN (July 3, 2025), https://www.goodwinlaw.com/en/insights/publications/2025/07/alerts-practices-aiml-federal-ai-moratorium-dies-on-the-vine (noting that the removal of the federal AI moratorium leaves states to advance a "wave of new state AI laws," including Texas's Responsible Artificial Intelligence Governance Act); Texas Responsible Artificial Intelligence Governance Act, H.B. 149, 89th Leg., Reg. Sess. (Tex. 2025) (codified as Tex. Gov't Code §§ 551.001–551.062 (2026)).

96 *See* U.S. Dep't of Just., Crim. Div., Fraud Section, Year in Review 2025 32–33 (Jan. 2026), https://www.justice.gov/criminal-fraud (describing DOJ enforcement priorities and noting that the 2025 Takedown included the *Charolia* case, a transnational health care fraud scheme involving foreign actors who used AI).

B. The Circuit Split Over Internet Use and Interstate Commerce

The phrase "in interstate or foreign commerce" has long served as a threshold requirement in federal criminal statutes, defining the jurisdictional boundary between federal and state authority.[97] Grounded in the Commerce Clause of the United States Constitution, this language reflects Congress's limited power to regulate conduct that extends beyond state lines.[98] In 1995, the Supreme Court in *United States v. Lopez*[99] clarified that Congress may regulate only three categories: (1) the channels of interstate commerce, such as highways or communications networks; (2) the instrumentalities of interstate commerce or persons or things in interstate commerce, such as airplanes, trucks, or internet servers; and (3) activities that substantially affect interstate commerce.[100] *United States v. Morrison*[101] reinforced that category three cannot be invoked lightly, holding that noneconomic, local conduct, such as gender-motivated violence, falls outside federal power even when aggregated nationally.[102] *Lopez* and *Morrison* reflect the Court's reluctance to interpret federal statutes in ways that intrude on state authority without a clear statement from Congress.[103] That principle was reiterated in 2014 in *Bond v. United States*,[104] where the Court reversed a federal conviction arising from a local assault involving household chemicals and warned that statutes should not be construed to reach traditional areas of state criminal jurisdiction unless Congress has made its intent unmistakably clear.[105] Read together, these cases underscore that statutory wording matters when determining the scope of interstate commerce.[106]

Some federal statutes use the phrase "affecting interstate or foreign commerce" rather than "in interstate or foreign commerce" to express this jurisdictional limit.[107] Statutes using "in" have traditionally been construed to require a concrete interstate nexus, while statutes using "affecting" may be satisfied by showing even indirect or minimal effects on interstate commerce.[108] This distinction meant that prosecutors invoking statutes using "in" generally had to prove that the conduct itself or the means used to carry it out crossed state borders or implicated interstate systems.[109] Under the

97 *See* United States v. Bass, 404 U.S. 336, 349–51 (1971) (requiring proof of a commerce nexus and emphasizing federal-state balance); United States v. Lopez, 514 U.S. 549, 561 (1995) (explaining that a jurisdictional element "ensure[s], through case-by-case inquiry, that the [regulated conduct] in question affects interstate commerce").

98 *See* U.S. CONST. art. I, § 8, cl. 3 (granting Congress the power "[t]o regulate Commerce with foreign Nations, and among the several States, and with the Indian Tribes").

99 *See generally* United States v. Lopez, 514 U.S. 549 (1995).

100 *Id.* at 558–59.

101 *See generally* United States v. Morrison, 529 U.S. 598 (2000).

102 *Id.* at 617–19.

103 *See Lopez*, 514 U.S. at 564–68 (emphasizing limits on Commerce Clause power and warning against federal intrusion into areas of traditional state concern); *see also Morrison*, 529 U.S. at 617–618 (reaffirming limits on federal power and emphasizing that regulation of noneconomic violent crime is reserved to the states).

104 *See generally* Bond v. United States, 572 U.S. 844 (2014).

105 *Id.* at 857–60.

106 *Id.* at 858 –59 (underscoring that federal criminal statutes must be interpreted narrowly to avoid intruding into traditional state jurisdiction absent a clear statement from Congress).

107 *See* Abramowitz & Sack, *supra* note 13 (noting that use of "in interstate commerce" signals Congress's intent to regulate a narrower class of activities).

108 *Id.*

109 *Id.*

WFA, for example, prosecutors typically had to show that a wire communication used in a fraudulent scheme traveled between states, regardless of where the communicators were located.[110]

However, the shift to a digitally connected economy has blurred, in practice, how courts apply "in interstate commerce," especially in the context of white-collar crime statutes such as the WFA and CFAA.[111] Today, reliance on the CFAA has expanded to include fraud carried out through "wireless communications" such as emails, cellphone calls, and text messages.[112] Unlike fraud by means of radio, television, or postal mail, internet communications are not easily mapped onto physical geography.[113] Because internet routing is driven by efficiency and network design rather than location, data routinely crosses state and national borders.[114] Consistent with this broader understanding of digital communications, Congress in 2008 amended multiple child-pornography provisions, including adding a new offense in 18 U.S.C. § 2252A(a)(7) that uses the jurisdictional phrase "in or affecting interstate or foreign commerce," signaling an intent to invoke the full breadth of its Commerce Clause authority.[115]

These technical realities have fueled a growing debate over whether jurisdictional analysis should continue to require proof of an actual interstate connection or instead presume that internet based conduct is interstate as a matter of law question continues to divide continued to divide federal circuits.[116] Whereas courts once treated this jurisdictional language as an evidentiary hurdle satisfied only by pointing to actual transmissions across state lines, reliance on multistate systems, or demonstrable economic effects on interstate markets, some circuits now presume that internet use itself establishes the necessary nexus.[117] Thus, in some circuits, the phrase "in interstate commerce" has come to function in practice nearly as broadly as "affecting interstate commerce" when applied to internet-based conduct.[118]

The First, Second, Third, and Fifth Circuits have adopted a categorical, or per se, approach, which represents the majority view.[119] These courts hold that internet use is

[110] *Id.*; *see also* 18 U.S.C. § 1343.

[111] *See, e.g.*, United States v. Gilboe, 684 F.2d 235, 238 (2d Cir. 1982) (holding, in part, that the interstate commerce element of the WFA is satisfied where fraudulent proceeds are routed through interstate wire communications, including international telex transmissions and U.S. bank transfers, even when the scheme is largely foreign); Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1153–55 (2016) [hereinafter Kerr, *Computer Trespass Norms*] (explaining that courts applying the CFAA have struggled to interpret statutory concepts because the norms governing online conduct remain unsettled).

[112] Kerr, *Computer Trespass Norms*, *supra* note 111, at 1145; *see also* Abramowitz & Sack, *supra* note 13.

[113] Kerr, *Computer Trespass Norms*, *supra* note 111, at 1154-55; *see also* Abramowitz & Sack, *supra* note 13.

[114] *See* Kurose & Ross, *supra* note 58.

[115] PROTECT Our Children Act of 2008, Pub. L. No. 110-401, § 304, 122 Stat. 4229, 4242–43 (extending the jurisdictional hook by adding § 2252A(a)(7)).

[116] *See* Abramowitz & Sack, *supra* note 13 (describing the circuit split over whether use of the internet alone suffices to satisfy the "in interstate commerce" requirement).

[117] *See, e.g.*, United States v. Kieffer, 681 F.3d 1143, 1153–55 (10th Cir. 2012) (holding the interstate-commerce element was satisfied where evidence showed the defendant's website content was transmitted across state lines); United States v. MacEwan, 445 F.3d 237, 244–46 (3d Cir. 2006) (holding that that downloading from the internet can be inherently interstate).

[118] *See, e.g.*, *MacEwan*, 445 F.3d at 244–46.

[119] *See* Abramowitz & Sack, *supra* note 13.

sufficient to satisfy the interstate commerce requirement.[120] This interpretation treats the internet as inherently interstate and presumes that digital transmissions, by their very nature, implicate interstate infrastructure.[121] By contrast, the Ninth and Tenth Circuits embrace a minority view which applies an evidentiary, case-specific, fact-based approach, requiring prosecutors to demonstrate that the conduct at issue either crossed state lines or meaningfully affected interstate commerce.[122]

In the white-collar context, this split is most clearly illustrated by the First and Tenth Circuits.[123] In *O'Donovan*, the First Circuit applied the categorical approach, reasoning that use of the internet to transmit emails or text messages satisfies the interstate-commerce element without requiring proof of the precise routing of the data.[124] The court's ruling promotes predictability and efficiency, and avoids litigating the precise routing of internet communications.[125] By contrast, in *United States v. Kieffer*[126] the Tenth Circuit the interstate commerce element of the WFA cannot be established by internet use alone, but must be supported by record evidence permitting a reasonable inference that communications crossed state lines.[127] The court explained that this was the "typical" case in which the interstate element could be gleaned from the record, such as evidence that a website was accessed by users in multiple states, rather than one in which the government relied solely on the assumption that internet use necessarily involves interstate transmission.[128] Ultimately, the choice between the categorical and evidentiary approaches frames the scope of federal jurisdiction in white-collar prosecutions and illustrates the difficulty of applying traditional commerce concepts to an internet-based, AI-driven economy.[129]

1. The Categorical Approach: First, Second, Third, and Fifth Circuits

The categorical approach treats the internet as inherently interstate.[130] This interpretation was already the majority view prior to the First Circuit's 2025 decision in *O'Donovan*. In fact, the First Circuit had embraced the categorical approach as early

[120] *See generally* United States v. O'Donovan, 126 F.4th 17, 34–36 (1st Cir. 2025) (dispensing with the requirement of proof of actual cross-border movement).
[121] *Id.*
[122] *See* United States v. Wright, 625 F.3d 583, 594 (9th Cir. 2010) (explaining that the government must establish that the charged transmission crossed state lines or otherwise affected interstate systems); *see also* United States v. Kieffer, 681 F.3d 1143, 1153 (10th Cir. 2012).
[123] *See, e.g.*, *O'Donovan*, 126 F.4th at 34–36 (holding that use of the internet is sufficient to establish the "interstate commerce" element of wire fraud without proof of actual data routing).
[124] *Id.* at 28, 34-36.
[125] *Id.*
[126] *See generally* United States v. Kieffer, 681 F.3d 1143 (10th Cir. 2012).
[127] *See id.* at 1153–55 (holding that internet use "standing alone" does not establish an interstate transmission and relying on evidence that the defendant's website was accessed from computers in multiple states and hosted through infrastructure located outside the forum state to support a reasonable inference that content crossed state lines).
[128] *Id.* at 1154–55.
[129] *See generally* Abramowitz & Sack, *supra* note 13 (reviewing the circuit split and analyzing the recent First Circuit decision).
[130] United States v. O'Donovan, 126 F.4th 17, 34–36 (1st Cir. 2025).

as 1997 in *United States v. Carroll*[131] and again in 2009 in *United States v. Lewis*,[132] both child pornography cases.[133] *Carroll* involved a defendant who photographed his underage niece and told her he planned to scan the images for internet distribution and to take the film across state lines for development.[134] *Lewis* concerned a defendant who downloaded child pornography videos from the internet.[135] In both cases, although the government offered no direct evidence that the images were actually distributed or that the downloaded files had physically crossed state lines, the court held that such proof was unnecessary because internet transmissions are functionally equivalent to interstate communications and upheld both convictions.[136]

Building on *Lewis* and *Carroll*, *O'Donovan* reaffirmed the First Circuit's position and extended it to the WFA.[137] The defendant was convicted of honest-services wire fraud and federal programs bribery after attempting to secure a lucrative "host community agreement" for a marijuana dispensary by offering payments to the police chief's brother in hopes of influencing the chief's scoring of applications and lobbying of the mayor.[138] The wire-fraud charges rested on two iMessages the defendant sent to his client during the scheme—messages that, on their face, contained only innocuous reassurances such as "[w]orking this thing hard just so you know my friend."[139] However, because the defendant and his client were both located in Massachusetts when the messages were sent, the jurisdictional question was whether those iMessages nonetheless satisfied the WFA's requirement that the communication be transmitted "in interstate or foreign commerce."[140]

Relying on its prior precedent, the First Circuit found "no material difference" between the WFA's jurisdictional language and the child-pornography statutes at issue in those cases.[141] It therefore held that proof the iMessages were transmitted "over the internet" was sufficient, without any showing that the particular transmissions actually crossed state lines.[142] At the same time, the court still had to decide on the evidence presented by the government.[143] The only evidence offered was testimony from an FBI examiner that the iMessages traveled "over the internet," but he was neither qualified as an expert nor had a proper lay foundation.[144] Because the government's only proof of the jurisdictional element was inadmissible, the error mattered, and the court sent the wire-fraud charges back for a new trial.[145] Notably, the court acknowledged the

131 *See generally* United States v. Carroll, 105 F.3d 740 (1st Cir. 1997).
132 *See generally* United States v. Lewis, 554 F.3d 208 (1st Cir. 2009).
133 *Carroll*, 105 F.3d at 741; *Lewis*, 554 F.3d at 209.
134 *Carroll*, 105 F.3d at 741–43.
135 *Lewis*, 554 F.3d at 209–10.
136 *Carroll*, 105 F.3d at 742–43; *Lewis*, 554 F.3d at 213–16.
137 *See* United States v. O'Donovan, 126 F.4th 17, 29, 34–36 (1st Cir. 2025) (holding that the categorical approach to internet transmissions applies equally to the WFA).
138 *Id.* at 23–29.
139 *Id.* at 26.
140 *Id.* at 34.
141 *See id.* at 34–35 (reaffirming that prior circuit precedent treats use of the internet as categorically interstate in nature).
142 *Id.* at 35.
143 *Id.*
144 *See id.* at 36–37 (noting the examiner's knowledge came only from FBI training sessions).
145 *Id.* at 37–38.

contrary evidentiary approach but declined to follow it, explaining that the law-of-the-circuit doctrine bound it to follow *Lewis* and *Carroll*, and that reconsideration of those precedents could come only through the en banc process.[146]

O'Donovan also built on earlier holdings from the Third and Fifth Circuits.[147] In *United States v. MacEwan*,[148] the Third Circuit upheld a conviction under the Child Pornography Prevention Act, 18 U.S.C. § 2252A(a)(2)(B), after the defendant downloaded approximately 256 images of child pornography from the internet.[149] The issue on appeal was whether those downloads satisfied the statute's requirement that the material be "transported in interstate or foreign commerce," even though the government could not prove that the specific files had crossed state lines.[150] Evidence presented by the government included the defendant's stipulation that the images were downloaded via the internet.[151] The government also offered testimony from a Comcast manager, who explained that internet traffic is dynamically routed under a "shortest path first" method that often crosses state boundaries and passes through the Internet backbone, a system composed of leased commercial and private lines.[152] The Third Circuit emphasized that the internet is inherently interstate in nature and functions as both a channel and an instrumentality of commerce.[153] Relying on this evidence and its conclusion about the internet's interstate character, the court held that downloading from the internet was categorically sufficient to establish the jurisdictional element.[154]

Like *MacEwan*, the Fifth Circuit in *United States v. Runyan*[155] also addressed the interstate commerce jurisdictional question within the context of child pornography statutes.[156] In *Runyan*, the defendant photographed a teenage girl in sexually explicit poses and downloaded images of child pornography from the internet.[157] He was convicted of sexual exploitation of a child under 18 U.S.C. § 2251 and of receipt, possession, and distribution of child pornography under 18 U.S.C. § 2252A.[158] The government introduced evidence that some of the seized images contained embedded website addresses and advertising slogans typical of online distribution, and a forensic expert testified that particular files originated from the internet.[159] The defendant also admitted that he accessed newsgroups to download child pornography.[160] Emphasizing

146 *Id.* at 35–36.

147 *See, e.g.*, United States v. MacEwan, 445 F.3d 237, 244–46 (3d Cir. 2006) (holding that use of the internet to download child pornography was sufficient to satisfy the jurisdictional element because the internet is "a system that is inexorably interstate in nature"); United States v. Runyan, 290 F.3d 223, 239 (5th Cir. 2002) (same).

148 *MacEwan*, 445 F.3d at 237.

149 *Id.* at 240, 244–45.

150 *Id.* at 244.

151 *Id.* at 241.

152 *Id.* at 241-42.

153 *Id.* at 245-46.

154 *Id.* at 246.

155 United States v. Runyan, 290 F.3d 223 (5th Cir. 2002).

156 *Id.* at 239.

157 *Id.* at 231–32.

158 *Id.* at 233.

159 *Id.* at 242.

160 *Id.* at 233, 242 (noting that Runyan admitted receiving images of child pornography from the Internet by accessing "newsgroups" and viewing images).

that the internet is inherently interstate in structure, the court held that internet transmission of images is "tantamount to moving photographs across state lines," categorically satisfying the interstate-commerce element of the statutes in question.[161] The court rejected the argument that the government must present direct, file-by-file proof of interstate transmission, holding that circumstantial evidence linking the charged images to the internet can suffice to establish the interstate commerce element.[162]

In another child pornography case, the Second Circuit reached the same conclusion as the Third and Fifth Circuits.[163] In *United States v. Harris*,[164] the defendant was convicted of three counts of receipt and one count of possession of child pornography under 18 U.S.C. § 2252.[165] On appeal, the defendant argued that the government failed to prove the interstate-commerce jurisdictional element because it did not establish that the particular image files found on his computer had crossed state lines.[166] The record showed, however, that the defendant had obtained thousands of still images and a video clip of child pornography from subscription-based internet websites.[167] The Second Circuit rejected his argument and, relying on its prior decisions and the categorical reasoning of other circuits, held that use of the internet itself was sufficient to satisfy the statute's requirement that the material be "transported in interstate commerce."[168]

Many of the leading circuit cases adopting the categorical approach arose in the child pornography context, where courts concluded that internet transmissions are inherently interstate.[169] Yet, as *O'Donovan* illustrates, the reasoning in those cases has not been confined to that subject matter.[170] Courts in this camp stress several considerations.[171] First, requiring prosecutors to trace the precise geographic path of every digital transmission would impose impractical evidentiary burdens and make enforcement of federal law nearly impossible.[172] Second, treating internet use as categorically sufficient avoids gaps in coverage that would allow defendants to evade liability simply because the government could not reconstruct complex routing data.[173] Third, these courts emphasize the technological reality that internet communications are routinely

[161] *Id.* at 239–40 (quoting United States v. Carroll, 105 F.3d 740, 742 (1st Cir. 1997)).
[162] *Id.* at 242–43.
[163] *See* United States v. Harris, 548 F. App'x 679, 682 (2d Cir. 2013) (summary order) (agreeing that internet transmissions satisfy "in interstate commerce").
[164] *See generally* United States v. Harris, 548 F. App'x 679 (2d Cir. 2013).
[165] *Id.* at 680–82.
[166] *Id.* at 682.
[167] *Id.* at 681-84.
[168] *Id.* at 682-83.
[169] *See, e.g.*, United States v. MacEwan, 445 F.3d 237, 244–46 (3d Cir. 2006) (rejecting the argument that only intrastate transmissions fell outside federal power); United States v. Runyan, 290 F.3d 223, 239–40 (5th Cir. 2002) (holding that downloading and distributing images via newsgroups triggered federal jurisdiction); United States v. Harris, 548 F. App'x 679, 682 (2d Cir. 2013) (relying on defendant's use of subscription websites to establish interstate commerce element).
[170] United States v. O'Donovan, 126 F.4th 17, 24–27, 35–37 (1st Cir. 2025) (relying on internet-commerce precedent developed in child pornography cases).
[171] *See, e.g.*, *MacEwan*, 445 F.3d at 244–45 (noting the internet's architecture ensures interstate routing).
[172] *Id.* at 244 (rejecting evidentiary requirements that would make prosecutions "almost impossible" given the complexity of routing); *Runyan*, 290 F.3d at 239–40 (treating online distribution networks as inherently interstate).
[173] *Runyan*, 290 F.3d at 239–40 (explaining that categorical treatment prevents loopholes for defendants whose transmissions might appear intrastate).

routed across state and national lines, often through backbone servers and data centers geographically far removed from the sender and recipient.[174] And finally, by recognizing the internet as both a channel and an instrumentality of commerce, the categorical approach aligns jurisdiction with the structure of modern communications.[175]

Together, these rationales reflect the court's view that Congress may regulate internet-based transmissions as use of the channels and instrumentalities of interstate commerce, and that the government need not prove the precise interstate routing of any particular transmission.[176] This reasoning has migrated from child pornography cases into white-collar prosecutions, where courts have applied the same principle to emails, text messages, and iMessages sent wholly within one state but transmitted "over the internet."[177] The rationale is even more consequential in today's environment of cloud-based services and AI-driven platforms, where digital information is routinely stored, fragmented, and routed across multiple states.[178] Under the categorical approach, such transmissions would be considered inherently interstate, ensuring that federal statutes regulating conduct "in interstate commerce" can be enforced consistently across contexts ranging from child exploitation to complex financial fraud.[179]

2. The Evidentiary Approach: Ninth and Tenth Circuits

In contrast to the categorical approach, the evidentiary approach requires prosecutors to present concrete proof that the conduct at issue either crossed state lines or otherwise implicated interstate commerce.[180] This narrower interpretation is associated with the minority view adopted by the Ninth and Tenth Circuits.[181]

Until the First Circuit's 2025 decision in *O'Donovan*, the Tenth Circuit's 2012 decision in *Kieffer* was the only appellate case to address whether internet use alone could satisfy the interstate-commerce element of the WFA.[182] In *Kieffer*, the defendant posed as a licensed criminal defense attorney, operating a website and offering legal representation in exchange for substantial fees.[183] He was charged with wire fraud and

[174] *MacEwan*, 445 F.3d at 245 (framing the internet as falling within both "channels" and "instrumentalities" categories of the Commerce Clause).

[175] *See* United States v. Runyan, 290 F.3d 223, 239–40 (5th Cir. 2002) (categorically equating internet transmissions with interstate movement of images).

[176] United States v. MacEwan, 445 F.3d 237, 244–45 (3d Cir. 2006).

[177] *See, e.g.*, United States v. O'Donovan, 126 F.4th 17, 34–36 (1st Cir. 2025).

[178] *See generally* Sealed Indictment, United States v. Smith, No. 24 Cr. 504 (S.D.N.Y. filed Aug. 26, 2024) (AI-generated music streaming fraud conducted through global platforms).

[179] *See generally* Abramowitz & Sack, supra note 13 (reviewing the circuit split and analyzing the recent First Circuit decision).

[180] *Compare* United States v. Schaefer, 501 F.3d 1197, 1200–01 (10th Cir. 2007) (holding that use of the Internet, standing alone, does not establish that a transmission traveled in interstate commerce), *with O'Donovan*, 126 F.4th at 34–36 (holding that proof that communications were transmitted over the Internet was sufficient to satisfy the interstate-commerce element).

[181] United States v. Kieffer, 681 F.3d 1143, 1153–54 (10th Cir. 2012) (requiring case-specific evidence of an interstate nexus rather than presuming internet transmissions are inherently interstate).

[182] *See* Abramowitz & Sack, *supra* note 13 (noting that, prior to *O'Donovan*, the Tenth Circuit was the only federal court of appeals to address whether internet use alone satisfies the WFA's interstate-commerce element).

[183] *Compare* United States v. O'Donovan, 126 F.4th 17, 24–25 (1st Cir. 2025) (holding that proof messages were transmitted "over the internet" was categorically sufficient to satisfy the WFA's jurisdictional element), *with* United States

argued that the government had failed to prove the interstate-commerce element because it relied solely on the fact that his fraudulent communications were made over the internet.[184] The government urged that internet use, standing alone, sufficed.[185] The Tenth Circuit rejected that categorical claim, emphasizing instead that the record must provide case-specific evidence of an interstate transmission.[186] Drawing on its earlier decision in *United States v. Schaefer*,[187] the court reiterated that "one individual's use of the internet, standing alone, is insufficient" to establish that a communication actually traveled in interstate commerce.[188] The government had to do more than speculate about routing patterns or assume that Internet transmissions inherently cross state lines.[189]

Turning to the evidence, the court highlighted several critical facts.[190] The defendant had registered his website, boplaw.com, through a domain name registrar whose servers were located in Virginia.[191] Witnesses testified that they accessed the website from computers in Tennessee and Colorado.[192] The court reasoned that for those end users to view the site, its content must have been transmitted from the Virginia servers across state lines to the users' locations.[193] This transmission, the court concluded, was not incidental or after-the-fact but was "an indispensable part of the communication strand necessary" to give clients access to the deceptive website.[194] On that basis, the Tenth Circuit held that a jury could reasonably infer an interstate nexus from the record evidence.[195] Because this link was "incident to the accomplishment of an essential part of the scheme"—namely, inducing victims to pay thousands of dollars for legal services the defendant was unqualified to provide—the jurisdictional element of the WFA was satisfied.[196] Although *Schaefer* was later overruled en banc in *United States v. Sturm*[197] in the child pornography context, the Tenth Circuit did not adopt a per se rule equating internet use with interstate transmission.[198] Instead, *Sturm* held that the government may satisfy the jurisdictional element by proving, through record evidence, that the substantive content of the charged image had at some point traveled in interstate

v. Kieffer, 681 F.3d 1143, 1153–55 (10th Cir. 2012) (requiring case-specific evidence that transmissions actually crossed state lines).

184 *Kieffer*, 681 F.3d at 1152 (describing defendant's fraudulent operation of a law practice and use of a website to solicit clients).

185 *Id.* at 1153 (defendant argued the government failed to show his Internet communications "traveled in interstate commerce").

186 *Id.*

187 United States v. Schaefer, 501 F.3d 1197, 1197 (10th Cir. 2007).

188 *Kieffer*, 681 F.3d at 1153 (citing United States v. Schaefer, 501 F.3d 1197, 1200–01 (10th Cir. 2007), superseded in part by statute as recognized in United States v. Sturm, 672 F.3d 891 (10th Cir. 2012) (en banc)).

189 *Id.* at 1153–54.

190 *Id.* at 1165–66.

191 *Id.*

192 *Id.*

193 *Id.* at 1167 (contrasting the indispensable transmission here with cases where the scheme was already complete before the wire communication occurred).

194 *Id.* (noting that the jury could infer an interstate nexus without tracing "every technical detail" of the transmission chain).

195 *Id.*

196 *Id.* at 1156.

197 *See generally* United States v. Sturm, 672 F.3d 891 (10th Cir. 2012) (en banc)).

198 *Id.* at 901–02.

or foreign commerce, even if the government cannot establish that the particular file possessed by the defendant crossed state lines.[199]

The Ninth Circuit reinforced the evidentiary approach in *United States v. Wright*,[200] making clear that proof of actual cross-border transmission is required when a statute uses the phrase "in interstate commerce."[201] The defendant, a Tucson resident, was prosecuted for transporting and possessing child pornography under 18 U.S.C. § 2252A(a)(1) after undercover FBI agents connected to his computer through Internet Relay Chat (IRC) and downloaded several images.[202] The government argued that the jurisdictional element was satisfied simply because the defendant used the internet, pointing out that he had logged into IRC servers located in California and Virginia.[203] In rejecting the government's invitation to follow the categorical reasoning of cases like *MacEwan* and *Lewis*, the Ninth Circuit emphasized that adopting such a rule would "read the word 'in' out of the statute" and improperly collapse the distinction between "in commerce" and "affecting commerce."[204] Instead, the court highlighted that when the record affirmatively demonstrates intrastate routing, prosecutors cannot rely on broad presumptions about internet infrastructure.[205] In doing so, it underscored that Congress's narrower jurisdictional language requires concrete, case-specific proof of cross-border movement, preserving a role for state authorities where transmissions remain local.[206]

Similar to the categorical approach, many of the leading cases applying the evidentiary approach also arose in the child-pornography context, but the reasoning carries broader implications.[207] In *Kieffer* and *Wright*, the Tenth and Ninth Circuits declined to treat internet use as inherently interstate, reasoning that Congress's decision to employ the narrower phrase "in interstate commerce" rather than "affecting interstate commerce" requires evidentiary proof rather than presumptions.[208] Both courts cautioned that deeming all internet use sufficient would erase statutory text and expand federal jurisdiction beyond what Congress intended, blurring the line between federal and state enforcement.[209] In *Kieffer*, the evidentiary burden was met through proof that the defendant's website was hosted on servers in Virginia and accessed from Tennessee and Colorado, making interstate transmission an indispensable part of the fraudulent

199 *Id.* at 897, 900–02.

200 United States v. Wright, 625 F.3d 583, 592–96 (9th Cir. 2010) (holding that, under the pre-2008 version of 18 U.S.C. § 2252A(a)(1), which prohibited transportation "in interstate commerce," the government was required to prove that the material actually crossed state lines and that mere internet use was insufficient) (superseded by statute on other grounds following Congress's 2008 amendment to § 2252A(a)(1), which expanded the statute to cover transportation).

201 *Id.* at 590–92 (describing undercover FBI operation in which agents connected to Wright's computer and downloaded child pornography images).

202 *Id.* at 589–90.

203 *Id.* at 590–91 (explaining the government's contention that server connections alone should suffice, even though forensic analysis showed the images never left Arizona).

204 *Id.* at 590–92

205 United States v. Kieffer, 681 F.3d 1143, 1153–54 (10th Cir. 2012); *Wright*, 625 F.3d at 594 (distinguishing "in" from "affecting" interstate commerce).

206 *Kieffer*, 681 F.3d at 1154 (warning against eliminating the statutory limitation); *Wright*, 625 F.3d at 592-93 (similar).

207 *See, e.g.*, United States v. Wright, 625 F.3d 583, 585 (9th Cir. 2010).

208 *Id.* at 593–94 (holding intrastate transmission fatal to jurisdiction despite use of out-of-state IRC servers).

209 *Id.* at 583, 594-96, 595–97. *Cf. Kieffer*, 681 F.3d at 1166–67.

scheme.[210] In *Wright*, however, forensic analysis showed that the images never left Arizona, leading the court to conclude that merely logging into out-of-state servers was insufficient because those servers facilitated chat sessions but did not transmit the files themselves.[211] These decisions illustrate the evidentiary approach's core rationale: fidelity to statutory language, respect for constitutional boundaries, and insistence on an actual interstate nexus rather than categorical assumptions.[212] These principles are particularly significant in the era of cloud-based services and AI-driven platforms, where communications may appear interstate but still demand careful evidentiary grounding to justify federal jurisdiction.[213]

C. Federal Statutes Governing White-Collar Crimes

Federal prosecutors rely on a set of statutes to pursue white-collar crimes, many of which, as discussed in this Comment's Introduction, were enacted long before the internet and long before the rise of AI.[214] For internet-based misconduct, the Wire Fraud Act (WFA), 18 U.S.C. § 1343, the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, and the federal money laundering statutes, 18 U.S.C. §§ 1956–1957, are among the primary tools of enforcement.[215] Each contains an interstate commerce requirement that serves as the jurisdictional hook for federal intervention.[216] In today's economy, where most fraud and financial misconduct exploit digital networks, the scope of these statutes turns on how courts interpret that hook.[217] The growing use of AI in fraud, unauthorized access, and financial concealment makes the issue pressing: whether jurisdiction rests on categorical recognition of the internet as inherently interstate, or on evidentiary proof that a particular transmission crossed state lines, will shape the effectiveness of federal enforcement.[218]

1. The Wire Fraud Act and Its Interstate Commerce Requirement

The WFA has long served as a central tool for federal prosecutors.[219] Enacted in 1952 to supplement the mail fraud statute, it extended federal authority to cover communications over emerging technologies such as telephones and radios.[220] Congress

[210] *Kieffer*, 681 F.3d at 1150, 1154, 1166–67.
[211] *Wright*, 625 F.3d at 594.
[212] *See, e.g.*, United States v. Kieffer, 681 F.3d 1143, 1153–54 (10th Cir. 2012); *Wright*, 625 F.3d at 595–96 (emphasizing statutory fidelity and limits on federal reach).
[213] *See* discussion *supra* Section I.A (explaining cloud-based AI infrastructure and routing complexity).
[214] *See* discussion *supra* Introduction; *see, e.g.*, 18 U.S.C. § 1343 (Wire Fraud Act) (enacted as part of the Communications Act of 1934, ch. 652, § 605, 48 Stat. 1064, 1103 (1934), and amended in 1952 to add wire fraud language).
[215] 18 U.S.C. § 1343; 18 U.S.C. § 1030; 18 U.S.C. §§ 1956–1957.
[216] 18 U.S.C. § 1343; 18 U.S.C. §§ 1030(a), (e)(2)(B); 18 U.S.C. §§ 1956(c)(4), 1957(f)(1).
[217] *See, e.g.*, United States v. O'Donovan, 126 F.4th 17, 27–28 (1st Cir. 2025) (interpreting "in interstate commerce" under the WFA); United States v. Wright, 625 F.3d 583, 593–94 (9th Cir. 2010) (requiring proof of cross-border transmission).
[218] Sealed Indictment, United States v. Smith, No. 24 Cr. 504 (S.D.N.Y. filed Aug. 26, 2024).
[219] *See* Jed S. Rakoff, *The Federal Mail Fraud Statute (Part I)*, 18 DUQ. L. REV. 771, 771–73 (1980) (describing centrality of mail and wire fraud statutes in federal prosecutions).
[220] Act of July 16, 1952, Pub. L. No. 82-554, § 18, 66 Stat. 722, 722–23 (codified as amended at 18 U.S.C. § 1343).

designed the statute to prevent fraudsters from exploiting communications networks that crossed state lines, ensuring that the federal government could respond to schemes that operated beyond the reach of any single state.[221] Over time, the statute has proven highly adaptable, extending to new forms of communication technology.[222] Courts have applied it to telegraphs, telephone calls, emails, text messages, and most recently, internet-based communications.[223]

The statute provides that anyone who "devise[s] or intend[s] to devise any scheme or artifice to defraud" and "transmits or causes to be transmitted" such communications "by means of wire, radio, or television communication in interstate or foreign commerce," commits wire fraud.[224] The Supreme Court has defined a "scheme or artifice to defraud" as a plan intended to deprive another of money, property, or honest services through false or fraudulent pretenses.[225] This broad statutory language has enabled the WFA to adapt to new technologies, ensuring that communications-based frauds remain within federal reach.[226]

At the same time, as the circuit split discussed in this Comment's Background illustrates, the internet has complicated application of the statute's jurisdictional element.[227] Because digital transmissions are broken into packets and routed across multiple interconnected networks and servers that may span states or countries, tracing their precise paths is often impractical.[228] In response, most courts have adopted a categorical approach, treating internet use itself as inherently interstate, while currently a minority require case-specific proof that transmissions crossed state lines.[229] This evolution underscores both the adaptability and the stakes of the WFA; whether the statute continues to function effectively against modern fraud, including AI-driven schemes, depends on which approach courts adopt. Under the categorical view, prosecutors can apply the WFA more readily to internet-based misconduct, while under the evidentiary view, federal jurisdiction may turn on case-specific proof of transmission.[230] Each approach reflects a different balance between ensuring federal reach and preserving a role for state enforcement.[231]

---

[221] *See* S. Rep. No. 82-44, at 14 (1951) (explaining intended to establish a federal fraud offense for misuse of radio communications parallel to the existing mail fraud statute).

[222] *See* Cong. Rsch. Serv., R48764, *Crime, the Commerce Clause, and the Internet* 10 (Dec. 15, 2025) (Peter G. Berris).

[223] *See, e.g.*, Pereira v. United States, 347 U.S. 1, 8–9 (1954) (telegraphs); United States v. Weiss, 914 F.2d 1514, 1517 (2d Cir. 1990) (telephone calls); United States v. Panarella, 277 F.3d 678, 681 (3d Cir. 2002) (emails).

[224] 18 U.S.C. § 1343.

[225] *See* Carpenter v. United States, 484 U.S. 19, 27 (1987) (defining "scheme or artifice to defraud").

[226] *See* Ellen S. Podgor, *Mail Fraud: Opening Letters*, 43 S.C. L. REV. 223, 230–31 (1992) (explaining breadth of statutory language).

[227] *See supra* Section I.B; *see supra* Section I.A.

[228] *See supra* notes 50–62 and accompanying text (describing packet routing, ISP interconnection, and geographically distributed cloud infrastructure).

[229] *Compare* United States v. O'Donovan, 126 F.4th 17, 34–35 (1st Cir. 2025) (categorical approach), *with* United States v. Wright, 625 F.3d 583, 594–95 (9th Cir. 2010), *and* United States v. Kieffer, 681 F.3d 1143, 1153 (10th Cir. 2012) (requiring case-specific proof).

[230] *See, e.g.*, United States v. Harris, 548 F. Appx. 679, 682 (2d Cir. 2013) (categorical view). *Cf. Kieffer*, 681 F.3d at 1153 (evidentiary view).

[231] *See* Bond v. United States, 572 U.S. 844, 858–60 (2014) (warning against reading federal statutes to intrude into state criminal jurisdiction absent clear statement).

2. The Computer Fraud and Abuse Act and Its Interstate Commerce Requirement

The CFAA, enacted in 1986, was Congress's response to growing concerns about computer fraud, abuse, and unauthorized access, particularly involving government and financial institution systems.[232] Initially, the statute was narrow, targeting intrusions into computers tied to national defense and financial records.[233] Over time, Congress amended the CFAA to expand its reach as computers became central to commerce and daily life.[234] Today, it criminalizes a broad range of activity, from unauthorized access to government databases to the deployment of malicious code, theft of information, and extortion through threats to damage protected systems.[235] Its breadth reflects Congress's intent to "bring [federal] laws up-to-date" and equip prosecutors to address computer-related crime in light of "rapidly changing technology" that would otherwise render existing laws obsolete.[236]

The statute's jurisdictional reach arises through its definition of a "protected computer." Under 18 U.S.C. § 1030(e)(2)(B), this term includes any computer "used in or affecting interstate or foreign commerce or communication."[237] Courts have generally interpreted this provision expansively, holding that any device connected to the internet qualifies because internet communications almost invariably travel across state or national borders.[238] This interpretation provides the jurisdictional basis for most modern CFAA prosecutions, eliminating the need to prove that a defendant's conduct involved a specific cross-border transmission.[239] In practice, this means that hacking into a company's internal database, transmitting malware, or exfiltrating financial information from a single location can still trigger federal jurisdiction where the targeted system operates within interstate networks, without requiring proof that the defendant's conduct itself crossed state lines.[240]

The CFAA's provisions span a wide spectrum of misconduct.[241] Section 1030(a)(2) prohibits unauthorized access to protected computers to obtain information, while other subsections address fraud furthered by computer intrusions, knowing transmission

[232] *See* Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (codified as amended at 18 U.S.C. § 1001); *see also* S. Rep. No. 99-432, at 2–3 (1986), reprinted in 1986 U.S.C.C.A.N. 2479, 2480 (explaining congressional concern about computer crime targeting financial and government systems).

[233] *See* 18 U.S.C. § 1030 (1986) (noting that the original version limited the scope to "[f]ederal interest computers"); Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561 (2010) [hereinafter Kerr, *Vagueness Challenges*].

[234] *See* Kerr, *Vagueness Challenges*, *supra* note 233, at 1566–67; USA PATRIOT Act, Pub. L. No. 107-56, § 814, 115 Stat. 272, 382 (2001) (codified as amended at 18 U.S.C. § 1030(a)(5)) (expanding CFAA coverage).

[235] *See* § 1030(a)(1)–(7) (listing covered offenses).

[236] *See* H.R. Rep. No. 98-894, at 4 (1984), reprinted in 1984 U.S.C.C.A.N. 3689, 3690 (explaining that rapidly changing computer technology would render existing laws obsolete and necessitate updated legal frameworks).

[237] § 1030(e)(2)(B).

[238] *See* United States v. Trotter, 478 F.3d 918, 921 (8th Cir. 2007) (holding any internet-connected computer qualifies as a "protected computer"); United States v. Drew, 259 F.R.D. 449, 457 (C.D. Cal. 2009) (same).

[239] *See Trotter*, 478 F.3d at 921 (holding internet-connected computers fall within CFAA jurisdictional scope).

[240] United States v. Ivanov, 175 F. Supp. 2d 367, 373–75 (D. Conn. 2001) (upholding jurisdiction over hacker accessing U.S. systems from abroad); United States v. Mitra, 405 F.3d 492, 495–96 (7th Cir. 2005) (applying the CFAA to interference with a city's emergency radio system used in interstate communication, regardless of whether the defendant's conduct crossed state lines).

[241] *See* 18 U.S.C. § 1030(a)(1)–(7) (enumerating covered offenses).

of malicious code, password trafficking, and computer-based extortion.[242] Penalties vary according to the severity of the offense, ranging from one-year misdemeanor sentences for first-time unauthorized access to terms of up to twenty years for aggravated conduct, such as causing significant damage or endangering public safety.[243] Because of these gradations, the CFAA is used not only in high-profile cases involving state-sponsored cyberattacks but also in routine prosecutions for insider misuse of credentials and theft of trade secrets.[244]

As digital systems have become more central to modern life, the CFAA has taken on increasing importance in addressing evolving forms of computer misuse.[245] As these systems have shifted to cloud-based and AI-driven environments, the statute has become increasingly relevant to new forms of cyber-enabled misconduct. GenAI tools rely on large-scale datasets and high-performance distributed computing infrastructure, and their misuse increasingly occurs through computer network operations that may implicate "protected computers" under the CFAA.[246] For example, AI systems can be employed to generate malicious code, automate password-guessing attacks, or create convincing phishing campaigns that deceive users into revealing credentials.[247] Cloud-based infrastructure also means that these activities nearly always involve protected computers operating in or affecting interstate commerce.[248] Thus, although enacted long before the rise of AI, the CFAA's jurisdictional language has proven adaptable to modern technological realities, providing prosecutors with a ready framework for addressing computer intrusions and AI-enabled cybercrime.[249]

---

[242] § 1030(a)(2), (a)(4)–(7).

[243] *See* 18 U.S.C. § 1030(c) (penalty provisions).

[244] *See* United States v. Nosal, 676 F.3d 854, 856–57 (9th Cir. 2012) (en banc) (addressing insider misuse of credentials under CFAA).

[245] *See* Kerr, *Computer Trespass Norms*, *supra* note 111, at 1144-45, 1155-56 (explaining that computer misuse statutes must be interpreted in light of rapidly changing technology and that courts must develop new norms to apply existing laws to evolving forms of online conduct).

[246] *See* Andrei Preda et al., *How CrowdStrike Trains GenAI Models at Scale Using Distributed Computing*, CROWDSTRIKE (Dec. 22, 2025), https://www.crowdstrike.com/en-us/blog/how-crowdstrike-trains-genai-models-at-scale-using-distributed-computing/ (explaining that large language models require "high-performance, distributed computing clusters at scale," rely on large-scale datasets, and are increasingly used by threat actors in "computer network operations campaigns").

[247] *See Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud*, FED. BUREAU OF INVESTIGATION, PUB. SERV. ANNOUNCEMENT NO. I-120324-PSA (Dec. 3, 2024), https://www.ic3.gov/PSA/2024/PSA241203; DOJ, PROSECUTING COMPUTER CRIMES 2–3, 13-15 (2010), https://www.justice.gov/criminal/file/442156/dl?inline= (noting that CFAA amendments were designed to cover distribution of malicious code and to criminalize trafficking in passwords and similar items) (describing malware, password-cracking, and phishing as CFAA-covered activities); *see also* Bruce Schneier, *A Hacker's Mind: How the Powerful Bend Society's Rules*, 82–85 (2023) (illustrating how AI can scale cyberattacks).

[248] *See* United States v. Trotter, 478 F.3d 918, 921 (8th Cir. 2007) (holding that any internet-connected device qualifies as a "protected computer" under the CFAA); *see also* United States v. Mitra, 405 F.3d 492, 495 (7th Cir. 2005) (recognizing interstate nature of communications systems).

[249] *See* Jack M. Balkin, *The Path of Robotics Law*, 6 CAL. L. REV. ONLINE 45, 46–52 (2015) (arguing that law interacts with new technologies through existing doctrinal frameworks rather than through fixed "essential" characteristics); *see also* United States v. Nosal, 676 F.3d 854, 857–59 (9th Cir. 2012) (acknowledging the government's broad reading of the CFAA that would transform an anti-hacking statute into an expansive misappropriation statute).

3. The Federal Money Laundering Statutes and Their Interstate Commerce Requirement

The Money Laundering Control Act of 1986 marked the first time Congress directly criminalized the movement and concealment of illicit funds.[250] Its two core provisions, codified at 18 U.S.C. §§ 1956 and 1957, remain central to federal efforts against financial crime.[251] Section 1956 prohibits conducting financial transactions with the proceeds of specified unlawful activity when done with certain intents, such as promoting further crime, concealing the source or ownership of funds, or evading reporting requirements.[252] Section 1957, by contrast, focuses on downstream transactions, making it a crime to engage in monetary dealings exceeding $10,000 with funds known to be derived from unlawful activity.[253] Together, these statutes provide overlapping tools for prosecutors to attack both the laundering of criminal proceeds and their subsequent integration into legitimate financial systems.[254]

Both provisions contain jurisdictional language that ties federal authority to commerce. Section 1956 defines "financial transaction" broadly to include movements of funds that "in any way or degree affect interstate or foreign commerce," while section 1957 uses a similarly broad definition of "monetary transaction."[255] Courts have consistently held that this language requires only a minimal connection to interstate commerce.[256] For example, depositing illicit proceeds into a federally insured bank account satisfies the interstate commerce element because transactions involving federally insured financial institutions affect interstate commerce.[257] Decisions from the Fourth and Eighth Circuits confirm this approach, reasoning that the use of federally regulated financial institutions automatically implicates interstate commerce, even when funds never physically cross state lines.[258]

In practice, courts have treated routine banking transactions as sufficient to trigger federal jurisdiction under §§ 1956 and 1957, even absent cross-border movement of funds.[259] Transactions through online banking systems, cryptocurrency exchanges, and cloud-based payment processors all fall within the ambit of §§ 1956 and 1957.[260]

---

250 *See* Pub. L. No. 99-570, § 1352, 100 STAT. 3207, 3207-18 (1986) (enacting the Money Laundering Control Act).

251 *See* 18 U.S.C. §§ 1956–1957 (2022) (criminalizing money laundering transactions and monetary dealings).

252 *See* 18 U.S.C. § 1956(a)(1) (2022) (listing prohibited intents, including promotion, concealment, and evasion).

253 *See* 18 U.S.C. § 1957(a) (2022) (prohibiting monetary transactions involving over $10,000 in criminally derived property).

254 *See* United States v. Santos, 553 U.S. 507, 509–10 (2008) (plurality opinion) (describing §§ 1956 and 1957 as separate money laundering provisions that operate in related but distinct ways).

255 *See* 18 U.S.C. §§ 1956(c)(4), 1957(f)(1) (2022) (defining "financial transaction" and "monetary transaction").

256 *See, e.g.*, United States v. Peay, 972 F.2d 71, 74–75 (4th Cir. 1992) (holding minimal nexus suffices).

257 *Id.*

258 *See, e.g.*, *id.*; United States v. Wadena, 152 F.3d 831, 854 (8th Cir. 1998) (affirming that using a Federal Deposit Insurance Commission insured institution supplies the required interstate-commerce nexus for the money-laundering transaction).

259 *See Peay*, 972 F.2d at 74–75; *Wadena*, 152 F.3d at 831.

260 Brett Nigh & C. Alden Pelker, *Virtual Currency: Investigative Challenges and Opportunities*, FBI L. ENF'T BULL. (Sep. 8, 2015), https://leb.fbi.gov/articles/featured-articles/virtual-currency-investigative-challenges-and-opportunities (noting that 18 U.S.C. §§ 1956 and 1957 apply to transactions involving virtual currency and are used by DOJ to prosecute such conduct).

Prosecutors rely on these statutes to address financial transactions derived from a wide range of predicate offenses, including drug trafficking, violent crimes, fraud, bribery, export-control violations, and human trafficking.[261] Although the drafters of the 1986 Act could not have anticipated the rise of AI, the statutes' broad definitions have proven adaptable, making them key tools for addressing the financial dimensions of AI-enabled misconduct.[262]

II. Analysis

A. The Constitution Does Not Demand Data Packet Tracing

Under the Commerce Clause, Congress may authorize federal criminal jurisdiction only where the conduct bears a sufficient connection to interstate or foreign commerce.[263] Consistent with this constitutional limitation, federal criminal statutes typically include a jurisdictional element, using phrases such as "in interstate or foreign commerce" or "affecting interstate or foreign commerce," with some statutes employing both formulations.[264] This jurisdictional element ensures that federal prosecutions rest on a genuine interstate nexus rather than a merely theoretical one.[265] Modern internet and cloud-based systems operate through geographically distributed physical infrastructure, often implicating multiple jurisdictions simultaneously.[266] Internet routing is driven by network conditions, such as traffic volume, rather than geographic distance or state lines, and transmissions may cross state borders depending on server location and routing paths.[267] Most AI today is cloud-based, and these systems are rarely local; they fragment and distribute inputs, computations, and outputs across multiple data centers, often located in different states.[268] What appears to be a local interaction, such as typing a prompt into a GenAI interface or sending a message, in fact relies on infrastructure that spans state and national borders.[269] Recognizing such transmissions as categorically interstate is therefore not an expansion of federal power, but rather an acknowledgment of technological reality.[270]

This categorical approach is not at odds with the limits the Supreme Court has recognized under the Commerce Clause.[271] In *Lopez* and *Morrison*, the Court curtailed

---

261 *See* 18 U.S.C. § 1956(c)(7) (defining "specified unlawful activity" broadly to include fraud, narcotics, and organized crime).

262 *See* Sealed Indictment, United States v. Charolia, No. 1:25-cr-00304 (N.D. Ill. filed June 5, 2025) ¶¶ 7, 20–22 (Counts One Through Four) (indictment alleging AI-generated audio and interstate laundering, violation of § 1956(h)).

263 U.S. CONST. art. I, § 8, cl. 3; United States v. Lopez, 514 U.S. 549, 558–59 (1995).

264 *See, e.g.*, 18 U.S.C. § 1343 (prohibiting wire communications "in interstate or foreign commerce"); 18 U.S.C. § 1030(e)(2)(B) (defining a "protected computer" as one "used in or affecting interstate or foreign commerce or communication").

265 *Lopez*, 514 U.S. at 561–62.

266 Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729, 734–39 (2016).

267 Luster, *supra* note 5, at 594–95.

268 *Cloud AI Adoption Soars*, *supra* note 20 (describing the cloud as the leading deployment environment for AI).

269 *Understanding Cloud-based Generative AI*, *supra* note 52 (explaining cloud-based generative AI infrastructure).

270 *See supra* Section I.A.

271 *See, e.g.*, United States v. Lopez, 514 U.S. 549, 552–53 (1995) (reaffirming that Congress's Commerce Clause authority is subject to judicially enforceable limits).

Congress's reliance on the substantial-effects category for noneconomic conduct, but it did not disturb Congress's broad authority over the channels and instrumentalities of interstate commerce.[272] *Bond* likewise cautioned courts against construing federal statutes to intrude into traditional areas of state criminal law absent a clear statement from Congress.[273] Here, by contrast, the statutes contain a clear jurisdictional hook.[274] Applying the phrase "in interstate or foreign commerce" to a medium like the internet therefore respects both the statutory text and constitutional federalism, while avoiding the impractical requirement of proving every cross-border transmission.[275]

Congress's 2008 decision to amend child-pornography statutes from covering conduct "in" interstate or foreign commerce to covering conduct "in or affecting" commerce may suggest that Congress regarded "in" as narrower in scope when used in statutes like the WFA, but that recognition does not weaken the categorical argument.[276] Congress uses the phrase "affecting interstate commerce" to invoke the broader scope of its Commerce Clause authority, permitting federal regulation even when the conduct itself does not cross state lines but substantially affects interstate commerce.[277] Internet and cloud-based AI conduct, by contrast, does more than affect commerce—it operates through infrastructure that is inherently interstate in nature.[278] These systems are designed to fragment, route, and recombine data across servers and networks located in multiple states and countries.[279] Because of that architecture, even the narrower "in interstate commerce" formulation is satisfied whenever the internet or cloud-based AI systems are used.[280] In this way, the 2008 amendment underscores Congress's ability to broaden statutory reach where necessary, while confirming that statutes using "in interstate commerce" are already sufficient to cover technologies that are interstate by design.[281] Therefore, the categorical approach not only aligns with congressional intent but also provides a doctrinally sound and practically necessary basis for applying federal statutes to modern internet misconduct.[282]

B. The Categorical Approach in Practice: Expansive but Evidence-Dependent

The First Circuit's recent decision in *O'Donovan* illustrates both the strength and the tension of the categorical approach.[283] The court held that proof the defendant transmitted iMessages over the internet was sufficient to satisfy the interstate-commerce element of the WFA, even though both the sender and recipient were located in

[272] *Id.* at 558–59; United States v. Morrison, 529 U.S. 598, 608–09, 617 (2000).
[273] *See* Bond v. United States, 572 U.S. 844, 858–60 (2014) (invoking principles of federalism and requiring a clear indication from Congress before construing a federal statute to intrude upon traditional state criminal jurisdiction).
[274] *See, e.g.*, 18 U.S.C. § 1343 (wire fraud).
[275] United States v. O'Donovan, 126 F.4th 17, 34–36 (1st Cir. 2025).
[276] *See* PROTECT Our Children Act of 2008, *supra* note 115.
[277] *See* Gonzales v. Raich, 545 U.S. 1, 16–17 (2005).
[278] *See supra* Section I.A.
[279] *See supra* Section I.A.
[280] *See* United States v. MacEwan, 445 F.3d 237, 244–46 (3d Cir. 2006).
[281] *See* 18 U.S.C. § 2252A (as amended 2008). *Cf.* United States v. Lewis, 554 F.3d 208, 213–14 (1st Cir. 2009).
[282] *See supra* Section I.A.2.; United States v. O'Donovan, 126 F.4th 17, 34–36 (1st Cir. 2025).
[283] *See O'Donovan*, 126 F.4th at 34–36.

Massachusetts.[284] In doing so, the court extended earlier holdings in *Carroll* and *Lewis* beyond the child-pornography context and into the WFA.[285] This demonstrates the doctrinal reach of the categorical approach: once the internet is treated as inherently interstate under one statute, the same reasoning may be applied to another statute employing the "in interstate commerce" formulation.[286] In effect, the categorical approach opens the door to harmonizing jurisdictional elements across statutes, ensuring that federal law keeps pace with the realities of modern technology, which is rarely confined to a single state.

Yet, the breadth of the rule creates tension because it appears to extend federal jurisdiction to virtually any internet use.[287] Some AI systems and digital tools can be deployed on closed or localized networks that do not implicate interstate commerce in any meaningful way.[288] Treating every use of internet-connected or AI-driven technology as inherently interstate risks overlooking these intrastate applications and collapsing the distinction between conduct that is truly interstate and conduct that is purely local.[289] However, *O'Donovan* also shows that the categorical rule does not eliminate the role of evidence.[290] The government's case failed because its only proof—an FBI examiner's testimony—was inadmissible.[291] The conviction was vacated not because the categorical approach itself was in doubt, but because prosecutors failed to offer admissible evidence that the communications were sent "over the internet."[292]

This evidentiary baseline echoes across other categorical cases. In *MacEwan*, the government relied on a stipulation and expert testimony about routing.[293] In *Runyan*, the government pointed to embedded website addresses, language advertising child pornography, and admissions by the defendant.[294] In *Harris*, the government introduced proof that the defendant used subscription-based websites.[295] These cases show that while courts applying the categorical approach do not require packet-tracing, they still require concrete evidence that the defendant actually used the internet.[296]

The resulting rule is broadly applicable but still grounded in proof.[297] It allows federal statutes to be applied consistently to internet-based misconduct, including white-collar crimes like the public-corruption scheme in *O'Donovan*.[298] The same reasoning

284 *Id.*
285 *Id.* at 35–36; *see also* United States v. Carroll, 105 F.3d 740, 742 (1st Cir. 1997); *Lewis*, 554 F.3d at 213–16.
286 *See O'Donovan*, 126 F.4th at 35–36.
287 *Id.*
288 *See supra* Section I.A.
289 *See* United States v. Wright, 625 F.3d 583, 593–95 (9th Cir. 2010) (declining to treat all internet use as interstate).
290 United States v. O'Donovan, 126 F.4th 17, 36-37 (1st Cir. 2025).
291 *See id.* at 36–38 (holding that the FBI examiner's testimony that the iMessages were transmitted over the Internet "should have been excluded").
292 *See id.* at 29-30 (vacating the wire-fraud convictions because the only evidence establishing the interstate-commerce element was inadmissible).
293 United States v. MacEwan, 445 F.3d 237, 239–40 (3d Cir. 2006).
294 United States v. Runyan, 290 F.3d 223, 239–40 (5th Cir. 2002).
295 Harris v. Alexander, 548 F. App'x 679, 684 (2d Cir. 2013) (summary order) (noting that the defendant "sought out thousands of images on paid-membership sites").
296 *MacEwan*, 445 F.3d at 244; *Harris*, 548 F. App'x at 684.
297 *See MacEwan*, 445 F.3d at 244; *Runyan*, 290 F.3d at 239.
298 *See* United States v. O'Donovan, 126 F.4th 17, 23–24 (1st Cir. 2025).

extends to AI-enabled crimes, where cloud-based systems fragment and route data across servers in multiple states and countries as a matter of course.[299] Although some AI systems can operate locally on closed networks without implicating interstate commerce, the dominant reality is that GenAI, the type most often used in modern fraud schemes, relies on cloud platforms and distributed infrastructure, making its operation inherently interstate.[300] Additionally, the "black box" nature of GenAI complicates matters further: even experts cannot fully explain how models generate outputs, making it more difficult to disentangle local from interstate activity or to pinpoint the technical path through which fraudulent content was created and transmitted.[301] Therefore, just as courts have recognized the interstate nature of downloading images or sending iMessages, the categorical approach can ensure that fraudulent schemes carried out with GenAI, whether through automated music streaming, fabricated patient consent, or other synthetic outputs, fall within federal jurisdiction.

C. The Evidentiary Approach in Practice: Narrower but Impractical

The evidentiary approach used in *Kieffer* and *Wright* shows both the approach's appeal and its limits.[302] In *Kieffer*, the Tenth Circuit required prosecutors to prove that transmissions actually crossed state lines and relied on server location and out-of-state access to establish jurisdiction.[303] This approach honored the statutory text of "in interstate commerce" but made jurisdiction depend on technical details, such as where a website was hosted or accessed, rather than the overall reach of the fraudulent scheme.[304] *Wright* exposed the same fragility. There, the Ninth Circuit rejected jurisdiction because, although Wright initially connected through out-of-state IRC servers, the charged file transfers occurred entirely within Arizona.[305] By tying liability to routing evidence, the evidentiary approach narrows federal reach in ways that do not match culpability.[306] While it preserves room for state prosecutions by requiring proof of actual interstate transmission, it makes federal jurisdiction turn solely on whether prosecutors can demonstrate that an internet communication briefly crossed state lines in an AI-driven economy where digital communications routinely traverse state and national borders by

[299] *See supra* Section I.A (describing cloud-based AI systems operating through geographically distributed data centers and interstate internet routing); United States v. MacEwan, 445 F.3d 237, 245–46 (3d Cir. 2006).

[300] *See supra* Section I.A–B (explaining that modern GenAI systems rely on cloud-based, geographically distributed data centers and global routing infrastructure).

[301] Pavlik, *supra* note 49 and accompanying text (noting that although engineers understand the technical structure of GenAI, the precise inner workings remain too complex to decipher and that neural network processes are not fully understood).

[302] *See e.g.*, United States v. Kieffer, 681 F.3d 1143, 1153-55 (10th Cir. 2012) (holding that the government must prove internet transmissions actually crossed state lines to satisfy "in interstate commerce" under the wire fraud statute); United States v. Wright, 625 F.3d 583, 592–96 (9th Cir. 2010) (finding the government failed to meet their burden of proof that digital files crossed state lines).

[303] *See Kieffer*, 681 F.3d at 1153-54 (finding sufficient interstate nexus where website content was hosted on servers in Virginia and accessed by users in Tennessee and Colorado).

[304] *Id.* at 1152–54 (emphasizing that mere internet use, "standing alone," does not establish an interstate nexus).

[305] *Wright*, 625 F.3d at 594–95 (reversing conviction where digital files never crossed state lines, despite interactions with out-of-state servers).

[306] *Id.* at 595–96 (concluding the government failed to show actual interstate transmission under the statute).

design.[307]

These cases underscore both the strengths and weaknesses of the evidentiary approach. It remains faithful to statutory text and respects federalism by reserving space for state prosecution where conduct is genuinely intrastate.[308] Yet it risks arbitrary outcomes tied to network architecture rather than culpability.[309] In *Wright*, liability turned not on the defendant's use of the internet to distribute contraband, but on the happenstance that the files never crossed state lines.[310] Identical misconduct could yield different outcomes depending on how packets happened to route, elevating technical happenstance over substantive wrongdoing.[311] The problem intensifies with internet and cloud-based AI systems, which fragment and recombine data across servers in multiple states and countries, making it nearly impossible to prove each interstate transmission.[312] Applied here, the evidentiary approach could allow even large-scale AI fraud schemes to escape federal jurisdiction.

Supporters of the evidentiary model argue that requiring proof preserves the jurisdictional element as a real limit rather than a mere formality.[313] Yet the categorical approach does not dispense with proof altogether.[314] Courts still require evidence that the internet was actually used, whether through stipulations, expert testimony, or forensic evidence.[315] What categorical reasoning avoids is not proof itself, but the impractical demand that prosecutors reconstruct every path internet data packets take.[316] In this way, it preserves the jurisdictional safeguard while ensuring that the element does not devolve into arbitrary technicalities.[317] By recognizing that the internet operates through infrastructure that is interstate by design, the categorical approach also promotes consistent enforcement against misconduct ranging from traditional wire fraud to complex AI-driven crimes.[318]

D. The Categorical Standard Preserves Structure and Practical Fairness

The categorical approach does more than provide doctrinal clarity. It also preserves practical fairness in the administration of federal criminal law. The rule that emerges is

[307] Cong. Rsch. Serv., R48764, *Crime, the Commerce Clause, and the Internet* 15–17 (Peter G. Berris, Dec. 15, 2025).
[308] United States v. Sturm, 672 F.3d 891, 896 (10th Cir. 2012).
[309] *Id.* at 893–94.
[310] United States v. Wright, 625 F.3d 583, 594–97 (9th Cir. 2010).
[311] *See id.* at 593–95 (holding jurisdiction failed where files did not cross state lines despite internet use); *see also* United States v. Kieffer, 681 F.3d 1143, 1152–55 (10th Cir. 2012) (requiring proof that transmissions actually crossed state lines); Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L.J. 357, 360–65 (2003) [hereinafter Kerr, *Internet Law*]; *supra* Section I.A.
[312] *See* United States v. MacEwan, 445 F.3d 237, 244–45 (3d Cir. 2006) (describing internet traffic as dynamically routed across interstate backbone systems); *supra* Section I.A.
[313] *See* United States v. O'Donovan, 126 F.4th 17, 34–36 (1st Cir. 2025).
[314] See *MacEwan*, 445 F.3d at 245–46; United States v. Runyan, 290 F.3d 223, 239–40 (5th Cir. 2002).
[315] See *MacEwan*, 445 F.3d at 245–46; *Runyan*, 290 F.3d at 239–40; Harris v. Alexander, 548 F. App'x 679, 684 (2d Cir. 2013).
[316] Kerr, *Internet Law*, *supra* note 311, at 360-66.
[317] *See e.g.*, United States v. Wright, 625 F.3d 583, 593–95 (9th Cir. 2010); United States v. Kieffer, 681 F.3d 1143, 1153-56 (10th Cir. 2012).
[318] *See supra* Section I.A; *MacEwan*, 445 F.3d at 245; *Runyan*, 290 F.3d at 239.

both clear and expansive.[319] It relieves prosecutors of the near impossible task of tracing the geographic path of digital transmissions in AI driven schemes, while ensuring that internet based misconduct remains within the scope of federal jurisdiction.[320] But this efficiency also expands federal charging discretion in ways that risk overreach.[321] By making internet use sufficient as a matter of law, the categorical approach may expose even minor or localized conduct to federal statutes carrying severe penalties.[322]

The defendants in the child-pornography cases, *Carroll*, *Lewis*, *MacEwan*, *Runyan*, and *Harris* were engaged in serious crimes that naturally implicated federal interests.[323] In *O'Donovan*, the underlying scheme was likewise grave, involving attempts to bribe public officials in connection with a competitive licensing process.[324] Yet the jurisdictional hook rested on two in-state iMessages that appeared innocuous on their face.[325] By treating those messages as categorically interstate, the approach illustrates how, in a less serious case than *O'Donovan*, a defendant could be exposed to the WFA's twenty-year maximum for conduct that is not egregious.[326] The concern then is not that defendants like *O'Donovan* avoid accountability, but that the same categorical reasoning can apply to far less serious conduct, creating exposure to disproportionate penalties when the internet is used in comparatively minor schemes.[327]

Critics argue that expanding federal criminal jurisdiction into areas traditionally handled by the states risks broadening overlapping federal-state authority and increasing the burden on federal courts.[328] But here too, existing legal and institutional safeguards mitigate these concerns.[329] First, DOJ charging policies direct prosecutors to pursue cases that serve identifiable federal interests and to decline marginal, purely local matters.[330] Second, constitutional and rule-based venue requirements constrain prosecutorial forum selection by requiring trial in the state and district where the offense was committed, subject to judicial enforcement of proper venue.[331] Third, federal sentencing is structured by the Sentencing Guidelines and 18 U.S.C. § 3553(a), which tie punishment to loss amount, victim impact, and the defendant's role in the offense, helping ensure that minor participants are not sentenced as major offenders.[332]

Concerns about harsh federal penalties and collateral consequences fare similarly. Congress criminalized schemes to defraud executed by means of interstate wire

---

[319] *See* United States v. MacEwan, 445 F.3d 237, 245 (3d Cir. 2006); *Runyan*, 290 F.3d at 239; *O'Donovan*, 126 F.4th at 34–36.

[320] *See infra* note 320.

[321] *See, e.g.*, United States v. Lopez, 514 U.S. 549, 564–68 (1995) (warning that broad Commerce Clause interpretations would convert federal authority into a general police power).

[322] *See, e.g.*, *MacEwan*, 445 F.3d at 245–47; 18 U.S.C. § 1343 (providing for up to 20 years' imprisonment).

[323] *See supra* Section I.B.1.

[324] United States v. O'Donovan, 126 F.4th 17, 21–24 (1st Cir. 2025).

[325] *Id.* at 30–33.

[326] *Id.* at 31–33; 18 U.S.C. § 1343 (providing for a maximum penalty of twenty years' imprisonment for wire fraud).

[327] *O'Donovan*, 126 F.4th at 30–33.

[328] Beal, *supra* note 8, at 383, 386–87, 400–04 (arguing that treating all internet transmissions as inherently interstate risks expanding federal jurisdiction at the expense of traditional state authority).

[329] *See supra* note 23–24 (discussing DOJ charging policies, venue, and federal sentencing).

[330] U.S. Dep't of Just., Just. Manual §§ 9-27.220–240.

[331] U.S. CONST. art. III, § 2, cl. 3; U.S. CONST. amend. VI; FED. R. CRIM. P. 18.

[332] U.S. SENT'G GUIDELINES MANUAL §§ 2B1.1, 3B1.1–3B1.2; 18 U.S. SENT'G COMM'N 2021).C. § 3553(a).

communications and attached substantial penalties to that conduct.[333] That judgment fits the technical realities detailed in the Background section and is further complicated by routing protocols such as border gateway protocols, which select packet paths for efficiency rather than geography; by content delivery networks that cache content across geographically distributed data centers; and by modern AI, especially GenAI, which runs on cloud infrastructure that fragments inputs, computation, and outputs across states and often countries.[334] Where conduct hijacks that infrastructure, federal involvement and forfeiture tools reflect a deliberate legislative choice to protect interstate systems.[335] And in practice, statutory maximums operate as ceilings, with courts selecting sentences based on offense severity and criminal history.[336]

By treating internet use as inherently interstate while still demanding a minimal evidentiary showing, the categorical approach secures both doctrinal clarity and practical enforceability in an era when digital misconduct rarely respects state lines. It also aligns the law with the technological architecture described in the Background: interstate routing and cloud distribution are features of modern networks, not anomalies.[337]

E. Federal Statutes Governing White-Collar Crimes: Implications for the *Smith* and *Charolia* Cases and AI-Driven Crimes

The categorical approach ensures that statutes like the Wire Fraud Act (WFA) can apply broadly to AI-enabled schemes while maintaining fairness through evidentiary standards, prosecutorial guidance, and judicial oversight.[338] *Smith* and *Charolia* demonstrate how existing laws address AI-driven fraud and why categorical reasoning about interstate commerce is critical.[339] In *Smith*, prosecutors charged wire fraud after the defendant used AI to generate songs, fake artists, and bot accounts that streamed billions of plays, producing more than $10 million in fraudulent royalties.[340] Because the platforms operated across states and countries, the scheme was interstate by design.[341] Although wire fraud was not charged in *Charolia*, the AI-generated "consent" recordings created abroad and transmitted into the United States to justify hundreds of millions in Medicare claims show how the WFA could have applied.[342] The CFAA was not charged in either case, but the conduct parallels its focus: bots manipulating cloud platforms in

333 18 U.S.C. § 1343.

334 *See supra* Section I.A and note 68; *What Is BGP?*, CLOUDFLARE, https://www.cloudflare.com/learning/security/glossary/what-is-bgp/ (last visited Sep. 4, 2025) (explaining that Border Gateway Protocol routes internet traffic by selecting among available network paths based on network conditions, efficiency, and routing attributes rather than geographic distance).

335 18 U.S.C. §§ 981(a)(1)(C), 982(a)(2).

336 Deanell Reece Tacha, *Serving This Time: Examining the Federal Sentencing Guidelines After a Decade of Experience*, 62 MO. L. REV. 471, 474, 476 (1997).

337 *See supra* Section I.A.

338 *See supra* Section I.A; 18 U.S.C. § 1343.

339 Sealed Indictment, United States v. Smith, No. 24 Cr. 504 (S.D.N.Y. 2024) ¶¶ 1, 25, 31–34; Sealed Indictment, United States v. Charolia, No. 1:25-cr-00304 (N.D. Ill. June 5, 2025) ¶¶ 2–4, 7 (Counts One Through Four).

340 *Smith*, No. 24 Cr. 504, ¶¶ 1, 10–14, 18–25, 31–34.

341 *Id.* ¶¶ 2–4, 31–34.

342 *Charolia*, No. 1:25-cr-00304, ¶¶ 7 (Counts One Through Four).

Smith and hackers scraping Medicare data in *Charolia*.[343] Courts treat internet-connected systems as "protected computers" under the CFAA because internet connectivity places them within interstate commerce.[344] Money-laundering statutes were also central, as defendants funneled tens of millions through U.S. banks and shell companies.[345] With statutory language requiring only minimal interstate effects, these provisions readily adapt to AI-driven schemes.[346]

CONCLUSION

Modern fraud runs on cloud infrastructure and global networks, where data fragments, routes, and recombines across borders as a matter of course.[347] Treating internet-based conduct as categorically "in interstate commerce" is not an expansion of federal power but a faithful application of existing statutes to contemporary technology.[348] The economic risks are acute, with AI-driven fraud losses projected to surge into the tens of billions and downstream costs borne by consumers, health programs, and financial markets.[349] The *Smith* and *Charolia* prosecutions illustrate the stakes.[350] Looking ahead to 2026, enforcement priorities further confirm that federal authorities will continue to focus on AI-enabled fraud, particularly in areas such as health care where generative and predictive tools may facilitate false claims and billing misconduct.[351] The categorical approach ensures that the WFA, the CFAA, and the money laundering statutes remain enforceable at scale, while still requiring a basic evidentiary showing that the internet or national financial systems were used.[352] DOJ charging policies confine prosecutions to cases with clear federal interests, judicial oversight guards against venue manipulation and charge stacking, and sentencing guidelines calibrate punishment to the scale and impact of the offense.[353] These safeguards prevent federal overreach while ensuring that AI-enabled schemes cannot exploit technical happenstance to escape accountability.[354]

[343] *Id.* ¶¶ 4–5 (Counts One Through Four).
[344] 8 U.S.C. § 1030(e)(2)(B); United States v. Trotter, 478 F.3d 918, 920–22 (8th Cir. 2007).
[345] 18 U.S.C. § 1956(h); *Smith*, No. 24 Cr. 504, ¶ 31 (charging conspiracy to commit money laundering).
[346] *See* discussion *supra* Section I.A.2.
[347] *See supra* Introduction.
[348] *See* cases cited *supra* Section II.A
[349] *See supra* Introduction.
[350] *See* cases cited *supra* Section I.A.2.
[351] D. Jacques Smith, Nadia Patel & Meghan F. Hart, *False Claims Act Enforcement in 2026 to Focus on DEI, AI Fraud*, ARENTFOX SCHIFF (Jan. 9, 2026), https://www.afslaw.com/perspectives/alerts/false-claims-act-enforcement-2026-focus-dei-ai-fraud.
[352] *See* discussion *supra* Section II.B.
[353] *See* discussion *supra* Section II.B.
[354] *See supra* Section II.B.


THE CRIMINAL LAW PRACTITIONER
EST. 2009


THE CRIMINAL LAW PRACTITIONER
EST. 2009