Congressional Research Service
Informing the legislative debate since 1914

Crime, the Commerce Clause, and the Internet

December 15, 2025

Congressional Research Service
https://crsreports.congress.gov
R48764

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R48764

December 15, 2025

Peter G. Berris
Legislative Attorney

Crime, the Commerce Clause, and the Internet

Congress can enact federal criminal statutes pursuant only to an enumerated constitutional power. One such power is Congress's authority to regulate interstate and foreign commerce under Article I, Section 8, Clause 3 of the Constitution, known as the Commerce Clause. Federal courts have construed the Commerce Clause to grant Congress considerable authority over crimes involving the internet, which is itself a channel and instrumentality of interstate commerce. Given the ubiquity of computers and the omnipresence of the internet, the Commerce Power gives Congress a potential jurisdictional hook to federalize a variety of criminal activities.

In considering the extent to which a commerce-grounded law includes the internet, courts have focused less on the abstract reach of the Commerce Clause and more on discerning congressional intent as manifested in particular statutory language. Much of the federal caselaw examining Congress's use of the commerce power to criminalize internet-based conduct looks to the exact jurisdictional language employed in a particular statute. *See, e.g.*, United States v. Haas, 37 F.4th 1256, 1264 (7th Cir. 2022) ("[The defendant] begins with a truism: the particular wording of the interstate-commerce element of a statute establishes what the government must prove."). For example, some statutes used to prosecute crimes involving the internet, like the wire fraud statute (18 U.S.C. § 1343), require proof that the offending communication is transmitted "in interstate or foreign commerce." Others, like 18 U.S.C. § 2252A(a)(1), which criminalizes conduct involving Child Sexual Abuse Material (CSAM)—require proof that the offending content is "transport[ed] or ship[ped] *using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce* by any means, including by computer." Federal courts diverged on whether mere internet use is satisfactory proof of transmission in interstate or foreign commerce, or whether such criminal statutes require proof of transmission across a state border. *See, e.g.*, *Haas*, 37 F.4th at 1264–65 (collecting caselaw and describing circuit split). By amending the jurisdictional language in federal CSAM laws to have a broader scope, Congress superseded that particular disagreement, but the divergence remains with respect to other laws used to prosecute crimes, such as wire fraud and interstate threats.

That divergence is relevant when Congress seeks to criminalize the transmission of images, messages, or other content through its commerce power. It has a choice over the precise jurisdictional language used, which in turn may affect the legal scope of the statute. If Congress uses jurisdictional language like that employed in the current CSAM statutes, courts would likely interpret it to include mere internet use. *See, e.g.*, United States v. Clark, 24 F.4th 565, 573, 574–75 (6th Cir. 2022) (collecting cases where federal courts concluded that a 2008 Amendment expanded the jurisdictional sweep of the CSAM provisions to include conduct involving the internet). In contrast, at least some federal courts would likely interpret jurisdictional language like that used in the wire fraud statute as requiring proof that the transmission actually crossed a state line. *See, e.g.*, United States v. Kieffer, 681 F.3d 1143, 1155 (10th Cir. 2012) ("[O]ne individual's use of the internet, 'standing alone,' does not establish an interstate transmission"). On a practical level, however, the inherently cross-border nature of the internet might limit the number of cases in which the distinction between mere internet use and cross-border transmissions actually makes a difference. *C.f.* United States v. Kammersell, 196 F.3d 1137, 1139 (10th Cir. 1999) (describing the argument that a broad reading of jurisdictional language in a statute covering interstate transmissions would "cover almost any communication made by telephone or modem" because "so many . . . locally-sent Internet messages are routed out of state"). That is because even courts that require an interstate transmission under some statutes would generally accept an instance where the offending message is sent and received in a single state, as long as it has been briefly routed through a second state. *See, e.g.*, United States v. Nissen, 432 F. Supp. 3d 1298, 1321 (D.N.M. 2020) ("Section 875(c)'s interstate commerce element is satisfied when a communication actually crosses state lines, however briefly.").

The Computer Fraud and Abuse Act, with its focus on crimes targeting internet-connected computers, provides a slightly different jurisdictional approach that might be a relevant model should Congress choose to prohibit other conduct targeting such devices.

Contents

Federal Criminal Law and the Commerce Power 1
The Internet and Internet Use as a Jurisdictional Basis Under the Commerce Power 4
Selected Statutory Examples 6
CSAM Statutes 6
Wire Fraud 10
Interstate Threats 11
The Computer Fraud and Abuse Act 13
Congressional Considerations 15

Contacts

Author Information 18

Computers are ubiquitous; the internet is omnipresent. That reality has potentially significant implications for federal criminal law,[1] where prohibitions must be premised on a source of constitutional authority.[2] One such source is Congress's power to regulate interstate and foreign commerce under Article I, Section 8, Clause 3 of the Constitution.[3] As a general matter, federal courts have construed the internet and computers as regulable pursuant to that power.[4] In other words, Congress can (and does) use the internet, or internet use, as a jurisdictional basis to criminalize conduct like making a violent threat, which—due to its traditionally local nature—ordinarily would be left to the states.[5] The type and extent of internet use that will satisfy jurisdictional requirements varies by statute.[6]

To illustrate the impact of different jurisdictional language with respect to the reach of a particular provision into the internet, this report examines four different types of statutes applicable to crimes involving the internet: (1) Child Sexual Abuse Material (CSAM) laws;[7] (2) wire fraud; (3) interstate threats; (4) and the Computer Fraud and Abuse Act (CFAA). It focuses first on CSAM laws, given the circuit split that developed over their jurisdictional scope and that ultimately resulted in a legislative amendment.[8] That judicial disagreement is crucial for understanding the reach of the next two statutes covered, as it has shaped the legal discourse on the jurisdictional scope of the wire fraud[9] and interstate threats statute with respect to the internet.[10] The report turns last to the CFAA, since that law represents a different manifestation of Congress's commerce authority in the realm of the internet. The report concludes with congressional considerations.

Federal Criminal Law and the Commerce Power

When enacting criminal laws, state legislatures have a luxury that Congress does not—a general police power.[11] The police power refers to the "inherent and plenary power of a sovereign to make all laws necessary and proper to preserve the public security, order, health, morality, and

[1] *Cf.* United States v. Kammersell, 196 F.3d 1137, 1139 (10th Cir. 1999) (describing the argument that a broad reading of jurisdictional language in a statute covering interstate transmissions would "cover almost any communication made by telephone or modem" because "so many . . . locally-sent Internet messages are routed out of state").

[2] *See infra* "Federal Criminal Law and the Commerce Power."

[3] *See infra* "Federal Criminal Law and the Commerce Power."

[4] *See infra* "Federal Criminal Law and the Commerce Power."

[5] *See infra* "Selected Statutory Examples."

[6] *See infra* "Selected Statutory Examples."

[7] Federal criminal statutes often refer to "child pornography" or "visual depiction[s]" of "sexually explicit conduct." *E.g.*, 18 U.S.C. §§ 2251, 2252A. These terms are defined in 18 U.S.C. § 2256. For consistency and clarity, given this report's main focus on jurisdictional language, this report simplifies the elements of these statutes and uses the term "Child Sexual Abuse Material," or "CSAM," which is the chosen terminology of the National Center for Missing & Exploited Children (NCMEC). *See* Nat'l Ctr. for Missing & Exploited Children, *Child Sexual Abuse Material*, https://www.missingkids.org/theissues/csam [https://perma.cc/9CPT-8DDN] (last visited Sept. 24, 2025) ("Outside of the legal system, NCMEC chooses to refer to these images as Child Sexual Abuse Material (CSAM) to most accurately reflect what is depicted—the sexual abuse and exploitation of children.").

[8] *See infra* "CSAM Statutes."

[9] *See infra* "Wire Fraud."

[10] *See infra* "Interstate Threats."

[11] United States v. Morrison, 529 U.S. 598, 618 n.8 (2000) ("Moreover, the principle that ' "[t]he Constitution created a Federal Government of limited powers," ' while reserving a generalized police power to the States, is deeply ingrained in our constitutional history." (quoting New York v. United States, 505 U.S. 144, 155 (1992))).

justice."[12] The Constitution reserves the police power to state governments, meaning that legislating to prohibit crime is a task that lies primarily within the purview of the states.[13] In contrast, the Constitution provides no such general police power to the federal government.[14] Instead, Congress can enact federal criminal statutes pursuant only to "one or more of its powers enumerated in the Constitution."[15] Federal criminal statutes—whether expressly or not—must therefore have a jurisdictional basis connecting the prohibited conduct to a source of constitutional authority.[16]

The Commerce Clause, found in Article I, Section 8, Clause 3 of the Constitution, grants Congress the power to "regulate Commerce with foreign Nations, and among the several States."[17] This provision gives Congress fairly broad authority,[18] and many federal criminal statutes rely on Congress's authority under the Commerce Clause as a jurisdictional basis.[19] In *United States v. Lopez*, the Supreme Court held that Congress's authority to regulate interstate commerce under the clause extends to "three broad categories of activity"[20]:

---

[12] *Police Power*, BLACK'S LAW DICTIONARY (12th ed. 2024); *see also* Metro. Life Ins. Co. v. Massachusetts, 471 U.S. 724, 756 (1985) ("The States traditionally have had great latitude under their police powers to legislate as ' "to the protection of the lives, limbs, health, comfort, and quiet of all persons." '" (quoting Slaughter-House Cases, 83 U.S. (16 Wall.) 36, 62 (1873)).

[13] *See* U.S. CONST. amend. X ("The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people."); *Morrison*, 529 U.S. at 618 ("Indeed, we can think of no better example of the police power, which the Founders denied the National Government and reposed in the States, than the suppression of violent crime and vindication of its victims.").

[14] *Morrison*, 529 U.S. at 618.

[15] *Id.* at 607.

[16] For further information on this topic, including a review of several common jurisdictional bases, see generally CRS Report R48177, *Components of Federal Criminal Law*, coordinated by Peter G. Berris, at 2–19 (2024) (collecting and describing examples of jurisdictional bases).

[17] U.S. CONST. art. I, § 8, cl. 3. The Commerce Power also extends to "Commerce . . . with the Indian Tribes." *Id.*

[18] The Commerce Clause has been one of the most frequently cited sources of legislative power in Constitutional Authority Statements. *See* CRS Report R44729, *Constitutional Authority Statements and the Powers of Congress: An Overview*, by Whitney K. Novak, at 12 (2023). The power is subject to "outer limits." United States v. Lopez, 514 U.S. 549, 557 (1995). More broadly, in some recent terms the Supreme Court has adopted a narrow reading of certain federal criminal provisions, including some grounded at least in part in the commerce power. *See generally* CRS Legal Sidebar LSB11033, *The Supreme Court's Narrow Construction of Federal Criminal Laws: Historical Practice and Recent Trends*, by Dave S. Sidhu (2023) (describing Supreme Court holdings narrowing the CFAA and wire fraud statute). For instance, in *Van Buren v. United States*, the Supreme Court adopted the narrower of two readings of the CFAA's prohibited conduct. 593 U.S. 374, 396 (2021). Although *Van Buren* was decided on textual grounds, the Court expressed concern that a broad reading of the CFAA would have sweeping implications, given the statute's considerable jurisdictional reach. *See id.* at 379, 394 (explaining that the CFAA's inclusion of computers "used in or affecting interstate or foreign commerce or communication" reaches "all computers that connect to the Internet," and explaining how a broad reading of the statute's prohibited conduct, on top of its expansive jurisdictional scope, could potentially encompass even routine misconduct on websites); *see also* CRS Legal Sidebar LSB10616, *Van Buren v. United States: Supreme Court Holds Accessing Information on a Computer for Unauthorized Purposes Not Federal Crime*, by Peter G. Berris (2021) (summarizing *Van Buren* opinion).

[19] *E.g.*, 18 U.S.C. § 33(a) (imposing fines, imprisonment, or both for certain acts of destruction to "any motor vehicle which is used, operated, or employed in interstate or foreign commerce"); *id.* § 1030(a)(6) (prohibiting computer password trafficking if "such trafficking affects interstate or foreign commerce" or if it impacts a federal government computer); *id.* § 1201(a)(1) (proscribing kidnapping when a "person is willfully transported in interstate or foreign commerce"); *id.* § 1343 (criminalizing intentional participation in schemes to defraud involving wire, radio, or television communications transmitted in interstate or foreign commerce); *see also* United States v. DiSanto, 86 F.3d 1238, 1244 (1st Cir. 1996) ("Congress has often invoked its authority under the Commerce Clause to federalize criminal activity."), *superseded by rule*, FED. R. CRIM. P. 12 (2014 Amendments), *as stated in*, United States v. Cardona, 88 F.4th 69, 77 n.7 (1st Cir. 2023).

[20] 514 U.S. at 558.

1. "Channels of interstate commerce,"[21] which are generally the "physical conduits" necessary for interstate commerce to take place,[22] such as highways and telecommunications networks;[23]
2. "Instrumentalities of interstate commerce, or persons or things in interstate commerce,"[24] such as "automobiles, airplanes, boats . . . shipments of goods . . . 'pagers, telephones, and mobile phones'";[25] and
3. "Those activities having a substantial relation to interstate commerce, i.e., those activities that substantially affect interstate commerce."[26]

Under the third category, Congress may regulate *intra*state conduct if it involves an economic activity that substantially affects interstate commerce in the aggregate.[27] For example, even purely local conduct, such as an individual's "production of [a] commodity meant for home consumption," may fall within Congress's commerce power if Congress has a rational basis to conclude that in the aggregate such conduct substantially affects "supply and demand in the national market for that commodity."[28]

In *United States v. Morrison*, the Supreme Court outlined four relevant considerations in determining whether conduct prohibited by a statute substantially affects interstate commerce[29]:

1. Whether the prohibited activity is commercial or relates to an economic enterprise.[30]
2. Whether the statute at issue contains an "express jurisdictional element" limiting its reach to conduct affecting interstate commerce through case-specific inquiry.[31] (The presence of an express jurisdictional factor weighs significantly in favor of a statute being an appropriate exercise of Congress's interstate commerce authority.)[32]

---

[21] *Id.*

[22] Cong. Rsch. Serv., *Channels of Interstate Commerce*, CONSTITUTION ANNOTATED, https://constitution.congress.gov/browse/essay/artI-S8-C3-6-2/ALDE_00013419/ (last visited Sept. 29, 2025).

[23] United States v. Roof, 225 F. Supp. 3d 438, 452 (D.S.C. 2016).

[24] *Lopez*, 514 U.S. at 558.

[25] United States v. Ballinger, 395 F.3d 1218, 1226 (11th Cir. 2005) (quoting United States v. Pipkins, 378 F.3d 1281, 1295 (11th Cir. 2004), *vacated*, 544 U.S. 902 (2005)).

[26] *Lopez*, 514 U.S. at 558–59 (citation omitted). At least some federal courts have interpreted the extent of Congress's power over foreign commerce under the clause to be different from its power over interstate commerce. *See, e.g.*, United States v. Rife, 33 F.4th 838, 843–44 (6th Cir. 2022) (holding that Congress's power over foreign commerce contains no equivalent to the third *Lopez* category), *cert. denied*, 143 S. Ct. 356 (2022) (mem.); *see also* CRS Legal Sidebar LSB10767, *Congress's Foreign Commerce Clause Power Questioned*, by Charles Doyle, at 1–2 (2022) (surveying case law and discussing *Rife*).

[27] Taylor v. United States, 579 U.S. 301, 306 (2016).

[28] Gonzales v. Raich, 545 U.S. 1, 19, 22 (2005).

[29] 529 U.S. 598, 610–12 (2000). For an example of how lower courts may apply these factors in practice, see generally United States v. Roof, 225 F. Supp. 3d 438, 452–56 (D.S.C. 2016) (applying *Morrison* factors in evaluating facial commerce clause challenge to 18 U.S.C. § 247).

[30] *Morrison*, 529 U.S. at 610.

[31] *Id.* at 611–12; *Roof*, 225 F. Supp. 3d at 452; *accord* United States v. Gibert, 677 F.3d 613, 625 (4th Cir. 2012) ("We next consider . . . whether the statute at issue contains an express element limiting the statute's reach to activities having an explicit connection with or effect on interstate commerce.").

[32] *See* United States v. Coleman, 675 F.3d 615, 620 (6th Cir. 2012) ("Where a statute lacks a clear economic purpose, the inclusion of an explicit jurisdictional element suffices to 'ensure, through case-by-case inquiry, that the [violation] (continued...)

3. Whether the statute's "express congressional findings" concern the effect of the prohibited conduct on interstate commerce.[33] (According to at least one federal district court, "[c]ongressional findings may weigh in favor of the validity of a statute," but their absence "cannot weigh against the validity of a statute.")[34]
4. The degree of attenuation between the prohibited conduct and its effect on interstate commerce.[35]

The Internet and Internet Use as a Jurisdictional Basis Under the Commerce Power

Federal courts have interpreted Congress's legislative authority under the Commerce Clause to include crimes involving the internet.[36] The internet, or internet use, can potentially fit into all three *Lopez* categories.[37] Broadly speaking, the internet qualifies as a regulable channel of commerce.[38] The internet is an instrumentality of commerce, as are internet-enabled devices such as computers and smartphones.[39] Conduct substantially relating to commerce may potentially

---

in question affects interstate commerce.'" (quoting United States v. Lopez, 514 U.S. 549, 561 (1995)); *see also* United States v. Hill, 927 F.3d 188, 204 (4th Cir. 2019) ("Notably, Defendant has not identified any case—nor have we found any such case—in which a federal criminal statute including an interstate commerce jurisdictional element has been held to exceed Congress's authority under the Commerce Clause.").

[33] *Morrison*, 529 U.S. at 612 (quoting *Lopez*, 514 U.S. at 562).

[34] *Roof*, 225 F. Supp. 3d at 454.

[35] *Morrison*, 529 U.S. at 612.

[36] *See, e.g.*, United States v. Hornaday, 392 F.3d 1306, 1311 (11th Cir. 2004) ("Congress clearly has the power to regulate the internet, as it does other instrumentalities and channels of interstate commerce, and to prohibit its use for harmful or immoral purposes regardless of whether those purposes would have a primarily intrastate impact."); *see also* United States v. Trotter, 478 F.3d 918, 921 (8th Cir. 2007) (per curiam) ("As both the means to engage in commerce and the method by which transactions occur, 'the Internet is an instrumentality and channel of interstate commerce.'" (quoting United States v. MacEwan, 445 F.3d 237, 245 (3rd Cir. 2006)).

[37] *See* United States v. Sutcliffe, 505 F.3d 944, 953 (9th Cir. 2007) ("We are therefore in agreement with the Eighth Circuit's conclusion that '[a]s both the means to engage in commerce and the method by which transactions occur, "the Internet is an instrumentality and channel of interstate commerce." '" (quoting *Trotter*, 478 F.3d at 921)); *Hornaday*, 392 F.3d at 1311 (similar). Given the status of the internet as a channel and instrumentality of interstate commerce, federal courts sometimes do not reach the question of when internet use might also satisfy the third *Lopez* category of activities substantially affecting interstate commerce. *E.g.*, United States v. Kammersell, 7 F. Supp. 2d 1196, 1200 (D. Utah 1998), *aff'd*, 196 F.3d 1137 (10th Cir. 1999). In some federal criminal statutes potentially applicable to internet crimes, however, Congress has added language to capture conduct affecting interstate commerce. *See infra* "CSAM Statutes." In general, such language "signals an intent to exercise [Congress's] commerce power to the full," which would inherently include the third *Lopez* category. United States v. Wright, 625 F.3d 583, 592 (9th Cir. 2010) (quoting Circuit City Stores, Inc. v. Adams, 532 U.S. 105, 115 (2001)), *superseded by statute*, Act of Oct. 8, 2008, Pub. L. No. 110-358, § 103, 122 Stat. 4001, *as stated in*, United States v. Brown, 785 F.3d 1337, 1351 (9th Cir. 2015).

[38] *See supra* notes 36–37 and accompanying text; *see also* United States v. MacEwan, 445 F.3d 237, 245 (3d Cir. 2006) ("In addressing the transmission of child pornography images over the Internet, we need not proceed to an analysis of *Lopez*'s third category when Congress clearly has the power to regulate such an activity under the first two.").

[39] *See supra* notes 36–38 and accompanying text; United States v. Stackhouse, 105 F.4th 1193, 1199 (9th Cir.) (explaining that both "landlines and cellphones" are instrumentalities of Congress), *cert. denied*, 145 S. Ct. 558 (2024); United States v. Bosaw, No. 23-3416, 2024 WL 4224150, at *2 (7th Cir. Sept. 18, 2024) (describing iPhone as an instrumentality of commerce); United States v. Evans, 476 F.3d 1176, 1180 (11th Cir. 2007) (similar); United States v. Hair, 178 F. App'x 879, 886 (11th Cir. 2006) (per curiam) ("In this case, there was evidence presented to the jury that [the defendant] used his computer and the internet to transport and receive images of child pornography. These are clearly instrumentalities of interstate commerce." (citing *Hornaday*, 392 F.3d at 1311)); United States v. Gilbert, 181 F.3d 152, 158 (1st Cir. 1999) ("[A] telephone is an instrumentality of interstate commerce and this alone is a sufficient (continued...)

include the use of the internet.[40] More specifically, as discussed below, courts have upheld federal criminal statutes against Commerce Clause challenges when an internet communication crossed state lines,[41] when a defendant used the internet to commit an offense,[42] and when the target device of a cybercrime was internet-connected.[43]

The legal fault lines are less about whether the internet is a satisfactory basis for a commerce-grounded statute as a constitutional matter, and more about how much internet use Congress intended to criminalize in a particular statute.[44] In other words, much of the federal caselaw examining Congress's use of the commerce power to criminalize internet-based conduct looks to the exact jurisdictional language employed in a particular statute.[45] For example, some statutes used to prosecute crimes involving the internet, like the wire fraud statute, require proof that the offending communication is transmitted "in interstate or foreign commerce."[46] Others, like those criminalizing conduct involving CSAM, require proof that the offending content is "transport[ed] or ship[ped] using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer."[47]

The precise jurisdictional language impacts the scope of a criminal law.[48] Federal courts generally agree that "statutes with language such as 'affecting commerce' or 'any facility of interstate commerce' require proof only that the criminal activity involved an instrumentality or channel of interstate commerce."[49] Thus, use of the internet, in and of itself, may be sufficient to satisfy the jurisdictional elements of such statutes.[50] Federal courts are divided, however, as to whether the same is true when statutes "contain language such as 'in interstate commerce.'"[51] Three federal appellate courts have held that mere internet use satisfies such statutes, but two others have held that "the government must prove that the online communication crossed state lines, not simply that it was made on the Internet."[52]

---

basis for jurisdiction based on interstate commerce."); Mendoza v. Detail Sols., LLC, 911 F. Supp. 2d 433, 440 (N.D. Tex. 2012) (mem.) (describing computers as examples of instrumentalities of interstate commerce).

[40] *See supra* note 37 and accompanying text.

[41] *See infra* "CSAM Statutes." Although the interstate transmission cases discussed in this report typically involve communications sent between states, some prosecutions have involved internet communications sent from abroad to the United States. *E.g.*, United States v. Elbaz, 52 F.4th 593, 600 (4th Cir. 2022).

[42] *See infra* "CSAM Statutes."

[43] *See infra* "The Computer Fraud and Abuse Act."

[44] *See infra* "Selected Statutory Examples."

[45] United States v. Haas, 37 F.4th 1256, 1264 (7th Cir. 2022) ("[The defendant] begins with a truism: the particular wording of the interstate-commerce element of a statute establishes what the government must prove.").

[46] 18 U.S.C. § 1343.

[47] 18 U.S.C. § 2252A(a)(1).

[48] *See Haas*, 37 F.4th at 1264 ("Congress's choice of language in any given statute is thus critical. How it articulates the interstate-commerce element of a statute tells us what that statute will reach.").

[49] *Id.* at 1264; *see also* United States v. Wright, 625 F.3d 583, 592 (9th Cir. 2010) ("Where Congress uses the phrases 'affecting commerce' or 'involving commerce,' it ' "signals an intent to exercise [its] commerce power to the full." '" (quoting Circuit City Stores, Inc. v. Adams, 532 U.S. 105, 115 (2001))); Allied-Bruce Terminix Cos., Inc. v. Dobson, 513 U.S. 265, 277 (1995) ("Thus, the Court interpreted the words 'involving commerce' as broadly as the words 'affecting commerce'; and, as we have said, these latter words normally mean a full exercise of constitutional power.").

[50] *See, e.g.*, *Definition of Interstate or Foreign Commerce*, PATTERN CRIMINAL JURY INSTRUCTIONS OF THE SEVENTH CIRCUIT 675 (2023 ed.) [hereinafter SEVENTH CIRCUIT JURY INSTRUCTIONS] ("Several circuits have now held that use of the internet satisfies the interstate commerce nexus.")

[51] *Haas*, 37 F.4th at 1264–65 (collecting caselaw and describing Circuit Split).

[52] *Id.* at 1265; *see also* United States v. Schaefer, 501 F.3d 1197, 1201 (10th Cir. 2007) ("Congress's use of the 'in (continued...)

Selected Statutory Examples

This section discusses four different types of statutes to illustrate how federal courts have interpreted commerce requirements with respect to different types of crimes involving the internet. Three of the examples involve statutes governing the transmission of certain content in interstate or foreign commerce, namely CSAM, threats, and messages to perpetrate fraud. The fourth example focuses primarily on crimes targeting devices that are used in interstate or foreign commerce.

CSAM Statutes

A number of federal statutory provisions criminalize the production, distribution, or possession of CSAM in various contexts. For instance, 18 U.S.C. § 2251 criminalizes certain conduct associated with the exploitation of children to create CSAM. As additional examples, 18 U.S.C. §§ 2252 and 2252A prohibit conduct including knowingly transporting, shipping, receiving, or distributing CSAM.[53] For conciseness, this report generally refers to these three statutes collectively as the CSAM Provisions.[54]

The exact wording of the CSAM Provisions varies by subsection, but before an October 2008 amendment (discussed below), they generally required proof that the CSAM had been transported or shipped in interstate or foreign commerce (hereinafter the pre-2008 jurisdictional language).[55] In addition, a 1988 law amended portions of §§ 2251 and 2252 to include language about computers.[56] For instance, that legislation changed § 2252(a), which criminalizes transportation and shipment of certain CSAM, to include instances of transportation or shipment "in interstate or foreign commerce *by any means including by computer* or mails."[57]

Some CSAM defendants challenged whether the pre-2008 jurisdictional language encompassed internet use alone.[58] Several federal appellate courts held that use of the internet to transmit CSAM could effectively satisfy the requirements of the pre-2008 jurisdictional language,

---

commerce' language, as opposed to phrasing such as 'affecting commerce' or a 'facility of interstate commerce,' signals its decision to limit federal jurisdiction and require actual movement between states to satisfy the interstate nexus."), *overruled on other grounds by*, United States v. Sturm, 672 F.3d 891 (10th Cir. 2012).

[53] 18 U.S.C. §§ 2252; 2252A.

[54] These three statutes are the primary focus of the jurisdictional caselaw described in this section, but a number of other statutes relevant to CSAM and child exploitation can be found in the United States Code. *E.g.*, 18 U.S.C. § 2251A.

[55] 18 U.S.C. § 2251(a), (b) (2003) (limiting applicability of provisions to situations where defendant knew, or had reason to know, that CSAM would "be transported in interstate or foreign commerce or mailed . . . or transported in interstate or foreign commerce by any means, including by computer"); *id.* § 2252(a)(1) (2003) (criminalizing knowingly transporting CSAM in "interstate or foreign commerce by any means including by computer or mails"); *id.* § 2252(a)(2) (2003) (barring receipt or distribution of CSAM that "has been shipped or transported in interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproduces any visual depiction for distribution in interstate or foreign commerce or through the mails"); *id.* § 2252(a)(3)(B) (2003) (authorizing penalties for knowing sale or possession "with intent to sell any visual depiction that has been mailed, or has been shipped or transported in interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means, including by computer"); *id.* § 2252(a)(4)(B) (2003) (making it a crime to "knowingly possess[] 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported in interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer"); *id.* § 2252A (2003) (similar).

[56] Anti-Drug Abuse Act of 1988, Pub. L. No. 100-690, §§ 7511–7512, 102 Stat. 4181.

[57] *Id.*; 18 U.S.C. § 2252(a) (2003) (emphasis added).

[58] *See generally infra* notes 59–72 and accompanying text.

requiring transport or shipment in interstate or foreign commerce, even absent evidence that the CSAM actually crossed a state line.[59] In taking this view, the First Circuit[60] explained that "[t]ransmission of photographs by means of the Internet is tantamount to moving photographs across state lines and thus constitutes transportation in interstate commerce."[61] The Third Circuit expressed similar reasoning, observing that "because of the very interstate nature of the Internet, once a user submits a connection request to a website server or an image is transmitted from the website server back to [the] user, the data has traveled in interstate commerce."[62] Therefore, the Third Circuit concluded that the pre-2008 jurisdictional language of § 2252A(a)(2)(B) encompasses instances where "images of child pornography [leave] the website server and [enter] the complex global data transmission system that is the Internet" because it means that "the images [are] being transmitted in interstate commerce."[63]

In contrast, two federal appellate courts held that the pre-2008 jurisdictional language of the CSAM provisions required proof of more than mere internet use.[64] For instance, in *United States v. Schaefer*,[65] the Tenth Circuit examined the pre-2008 jurisdictional language of 18 U.S.C. § 2252(a)(2) and (a)(4)(b) (governing receipt and possession of CSAM, respectively).[66] The Tenth Circuit held that "an Internet transmission, standing alone" does not satisfy the commerce requirements of those provisions.[67] The court acknowledged that "in many, if not most, situations the use of the Internet will involve the movement of communications or materials between states."[68] Nevertheless, the Tenth Circuit concluded that "[a]fter establishing a computer or Internet connection as the method of transport, the government must still prove that the Internet

[59] *See* United States v. Haas, 37 F.4th 1256, 1264–65 (7th Cir. 2022) ("The First, Second, Third, and Fifth Circuits have taken the position . . . that the government can satisfy the 'in interstate commerce' element of a statute simply by showing that the Internet was used."); *see also* United States v. Harris, 548 F. App'x 679, 682 (2d Cir. 2013) (unpublished summary order) (agreeing that internet use satisfied the requirement of the "pre-October 2008 version of 18 U.S.C. § 2252(a)(2) . . . that child pornography had been 'transported in interstate . . . commerce.'"); United States v. MacEwan, 445 F.3d 237, 244 (3d Cir. 2006) (constructing jurisdictional language of pre-2008 § 2252A(a)(2)(B)); United States v. Runyan, 290 F.3d 223, 239 (5th Cir. 2002) ("We join the First Circuit in holding that '[t]ransmission of photographs by means of the Internet is tantamount to moving photographs across state lines and thus constitutes transportation in interstate commerce' for the purposes of [pre-2008] 18 U.S.C. § 2251."); United States v. Carroll, 105 F.3d 740, 742 (1st Cir. 1997) (interpreting jurisdictional language of pre-2008 § 2251(a)).

[60] This CRS report references a significant number of decisions by federal appellate courts of various regional circuits. For purposes of brevity, references to a particular circuit in the body of this CRS report (e.g., the First Circuit) refer to the U.S. Court of Appeals for that particular circuit.

[61] *Carroll*, 105 F.3d at 742. There was evidence in *Carroll*, however, that actual transportation across state borders would have happened. *See id.* at 742 (describing evidence that defendant had been planning to transport photographic negatives from New Hampshire to Massachusetts for development, scanning, and distribution by computer). In a subsequent case, the First Circuit clarified that "[t]he government . . . cannot excise completely the requirement that the child pornography cross a state or national border." United States v. Lewis, 554 F.3d 208, 214 (1st Cir. 2009). But, the First Circuit explained, the government may be able to prove interstate transmission if it introduces evidence of internet use by the defendant. *Id.*

[62] *MacEwan*, 445 F.3d at 244.

[63] *Id.*

[64] *See Haas*, 37 F.4th at 1265 ("The Ninth and Tenth Circuits, on the other hand, have sided with Haas: they hold that the government must prove that the online communication crossed state lines, not simply that it was made on the Internet").

[65] 501 F.3d 1197, 1200 (10th Cir. 2007), *overruled on other grounds by*, United States v. Sturm, 672 F.3d 891 (10th Cir. 2012).

[66] 18 U.S.C. § 2252(a)(2), (a)(4)(b).

[67] *Schaefer*, 501 F.3d at 1200–01.

[68] *Id.* at 1201.

transmission also moved the images across state lines."[69] In reaching that conclusion, the Tenth Circuit reasoned that "Congress's use of the 'in commerce' language, as opposed to phrasing such as 'affecting commerce' or a 'facility of interstate commerce,' signals its decision to limit federal jurisdiction and require actual movement between states to satisfy the interstate nexus."[70] The court also rejected the argument that Congress's 1988 amendment to the provision—adding wording about computer use—negated that requirement.[71] Rather, according to the Tenth Circuit, "Congress simply wanted to be 'doubly sure' we recognized that the statute contemplates more than traditional methods of sending and receiving images."[72]

Following *Schaefer* (and according to some legislative history *because* of *Schaefer*),[73] Congress amended the jurisdictional language of the CSAM Provisions.[74] It added the phrase "using any means or facility of interstate or foreign commerce or" and replaced "in interstate commerce" with "in or affecting interstate commerce."[75] For example, the amended version of 18 U.S.C. § 2252A now authorizes penalties for anyone who

> **(1)** knowingly transports or ships *using any means or facility of interstate or* foreign commerce or *in or affecting interstate or foreign commerce* by any means including by computer or mails, any visual depiction, if--
>
> > **(A)** the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and
> >
> > **(B)** such visual depiction is of such conduct . . . .[76]

As noted above, this type of jurisdictional language, particularly the phrase "affecting interstate or foreign commerce," has been interpreted by courts to signal congressional intent that it wanted to exert the broadest constitutional reach of its commerce power in a particular provision.[77] As

---

[69] *Id.*

[70] *Id.*

[71] *Id.* The First Circuit interpreted the effect of the 1988 amendment similarly, even though it was on the other side of the split than the Tenth Circuit regarding the pre-2008 jurisdictional language. *See* United States v. Lewis, 554 F.3d 208, 214 (1st Cir. 2009) ("The clause does evince a particular concern with computer transmission of child pornography, but its placement—modifying 'has been shipped or transported . . . in interstate commerce' cannot indicate that special rules apply to computer shipment or transmission.").

[72] *Schaefer*, 501 F.3d at 1202.

[73] *See, e.g.*, 154 CONG. REC. 21798 (2008) (statement of the Rep. Judy Biggert) ("The judges who decided [*Schaefer*] pointed out that the use of the phrase 'in commerce' instead of 'affecting commerce' in the law signaled Congress' intent to limit Federal jurisdiction in the prosecution of child pornographers. . . . As co-chair of the Missing and Exploited Children's Caucus, I can assure you, Mr. Speaker, nothing could be further from the truth."); *id*. at 21797 (statement of Rep. Chris Cannon) ("H.R. 4120, the 'Effective Child Pornography Prosecution Act of 2007,' responds to [*Schaefer*] by expanding jurisdiction for prosecuting Internet child pornography crimes."); 153 CONG. REC. 31040 (2007) (statement of Rep. John Conyers) ("Members of the committee, H.R. 4120, the Effective Child Pornography Prosecution Act, addresses a truly unfortunate and, in my view, wrongly decided decision by the 10th Circuit Court of Appeals in the case of *United States v. Schaefer*.").

[74] Act of Oct. 8, 2008, Pub. L. No. 110-358, § 103, 122 Stat. 4001.

[75] *Id.*

[76] 18 U.S.C. § 2252 (emphasis added).

[77] *See* Allied-Bruce Terminix Cos., Inc. v. Dobson, 513 U.S. 265, 277 (1995) ("Thus, the Court interpreted the words 'involving commerce' as broadly as the words 'affecting commerce'; and, as we have said, these latter words normally mean a full exercise of constitutional power."); *cf.* United States v. Haas, 37 F.4th 1256, 1264 (7th Cir. 2022) ("Statutes with language such as 'affecting commerce' or 'any facility of interstate commerce' require proof only that the criminal activity involved an instrumentality or channel of interstate commerce."); *Schaefer*, 501 F.3d at 1201 ("Congress's use of the 'in commerce' language, as opposed to phrasing such as 'affecting commerce' or a 'facility of interstate commerce,' signals its decision to limit federal jurisdiction and require actual movement between states to satisfy the interstate nexus.").

several members stated, the amendment was intended to close a loophole created by the original "in commerce" language[78] and guarantee that the "prohibitions against child pornography reach the full extent of [Congress's] constitutional authority."[79]

It appears that the 2008 amendment has had its intended effect: the Tenth Circuit has described *Schaefer* as superseded by statute,[80] and federal courts have concluded that internet use is sufficient to satisfy the jurisdictional requirements of the current CSAM provisions.[81]

An Analog Analogue: Carjacking

Some federal criminal statutes, less relevant to the digital space, contain similar jurisdictional language to the pre-2008 CSAM provisions. One example, 18 U.S.C. § 2119—sometimes described as the federal carjacking statute—makes it a crime to take a vehicle from a "person or presence of another by force and violence or by intimidation."[82] Section 2119 also requires proof that the motor vehicle had been "transported, shipped, or received in interstate or foreign commerce."[83] In practice, this commerce element appears to present a fairly low bar. For example, several federal courts have concluded that the commerce requirement is met if the carjacking occurs in a state other than where the vehicle was manufactured.[84] A discussion of that statute, along with the jurisdictional requirements of other federal theft laws, may be found in CRS In Focus IF12914, *Federal Criminal Theft Laws*, by Peter G. Berris (2025).

[78] 153 CONG. REC. 31041 (2007) (statement of Rep. Nancy Boyda) ("This legislation closes the judicial loophole that allowed a guilty man who hurt our children . . . to go free.").

[79] *Id.* (statement of Rep. John Conyers); 154 CONG. REC. 21797 (2008) (statement of Rep. Zoe Lofgren) ("This small change will have great legal significance, allowing that statute to reach the full extent of Congress' commerce clause powers.").

[80] United States v. Kieffer, 681 F.3d 1143, 1153 (10th Cir. 2012). In other statutory contexts, as discussed below, the Tenth Circuit has reaffirmed the "narrow proposition for which *Schaefer* still stands, namely that one individual's use of the internet, 'standing alone,' does not establish an interstate transmission." *Id.* at 1155; *accord* United States v. Kroeker, No. 24-3060, 2025 WL 1878790, at *6 n.2 (10th Cir. July 8, 2025) (explaining that a Tenth Circuit case that overturned one holding in *Schaefer* "did not undermine *Schaefer*'s other holding that the government cannot prove an image traveled between the states by merely showing that a defendant got it from the internet").

[81] *See, e.g.*, United States v. Clark, 24 F.4th 565, 573, 574–75 (6th Cir. 2022) (collecting cases where federal courts concluded that the 2008 Amendment expanded the jurisdictional sweep of the CSAM provisions to include intrastate conduct involving the internet, and determining that the post-2008 version of § 2252(a)(2) "merely require[s] that a defendant used a means or facility of interstate commerce (such as the internet) to distribute the child pornography"); United States v. Wasson, 426 F. Supp. 3d 822, 828 (D. Kan. 2019) ("In response, the Government argues that it met the interstate commerce element of both offenses [under § 2252A] because it presented evidence that [the defendant] uploaded, downloaded, and sent the images using well-known, internet-based communications services, and the internet is an instrument of interstate commerce. The Court agrees."), *aff'd*, 847 F. App'x 523 (10th Cir. 2021). There is at least one notable post-2008 case involving pre-2008 violations, where the federal court required proof of more than mere internet use. *E.g.*, United States v. Wright, 625 F.3d 583, 600 (9th Cir. 2010). Specifically, in 2010, the Ninth Circuit agreed with *Schaefer* and held that the pre-2008 iteration of 18 U.S.C. § 2252A(a)(1) (transporting or shipping certain CSAM in various contexts) "required the government to prove that the child pornography images actually crossed state lines." *Id.*

[82] 18 U.S.C. § 2119.

[83] *Id.*

[84] *See, e.g.*, United States v. Forty-Febres, 982 F.3d 802, 807 (1st Cir. 2020) ("Finally, the prosecution certified that [the] Toyota Corolla was manufactured in Japan . . . [and] had thus 'been transported, shipped, or received in interstate or foreign commerce,'. . . satisfying the final element of [18 U.S.C. § 2119]"); United States v. Rahim, 431 F.3d 753, 759 (11th Cir. 2005) ("The government presented testimony that the vehicle was manufactured in Ohio and located in Georgia during the carjacking, and the district court denied [the defendant's] motion for acquittal.").

Wire Fraud

One frequently used prosecutorial tool is the federal wire fraud statute,[85] 18 U.S.C. § 1343, which authorizes criminal penalties for knowing or willing participation in a scheme to defraud using interstate wires.[86] Courts have interpreted "scheme to defraud" to include the "common understanding" of depriving someone of money or property by "dishonest methods," such as trickery and deceit.[87] Phone calls (cellular or landline), faxes, emails, instant messages, texts, and wire transfers may all qualify as wire transmissions for § 1343 purposes.[88] To violate the wire fraud statute, it need only be reasonably foreseeable that the interstate wires would be used in furtherance of the scheme to defraud,[89] which generally requires that the wires be "incident[al] to an essential part of the scheme."[90]

Section 1343 has similar jurisdictional language to the pre-2008 CSAM provisions, requiring proof that the offending content is transmitted "by means of wire, radio, or television communication *in interstate or foreign commerce*."[91] Federal courts have disagreed on whether § 1343's requirement of transmission "in interstate or foreign commerce" includes mere internet use.[92] For example, the First Circuit observed the close resemblance between the jurisdictional language of § 1343 and of the pre-2008 CSAM provisions, and saw "no reason to distinguish the wire fraud statute."[93] Just as it had in the CSAM context, the First Circuit held that internet use was alone sufficient, meaning that prosecutors satisfied the jurisdictional requirements of § 1343 with proof that iMessages were transmitted via the internet.[94]

The Tenth Circuit has reached the opposite conclusion by reference to its own pre-2008 CSAM precedent.[95] It analogized the jurisdictional language of § 1343 to that contained in the pre-2008 CSAM provisions and said that it had "no quarrel with the narrow proposition for which *Schaefer* still stands, namely that one individual's use of the internet, 'standing alone,' does not establish an

[85] According to data compiled on Syracuse University's TRACFed, wire fraud was the lead charge in well over one thousand prosecutions brought in each fiscal year since 2021. TRAC, PROSECUTIONS FOR 2025 (2025), https://tracreports.org/results/9x2068da996946.html [https://perma.cc/A8HH-6EGV].

[86] 18 U.S.C. § 1343.

[87] Carpenter v. United States, 484 U.S. 19, 26–27 (1987).

[88] *18 U.S.C. § 1343 Wire Communication*, SEVENTH CIRCUIT JURY INSTRUCTIONS, *supra* note 50, at 641.

[89] *See* United States v. Taylor, 942 F.3d 205, 214 (4th Cir. 2019) ("It is 'not necessary for the defendant to be directly or personally involved in the wire communication as long as that communication was reasonably foreseeable in the execution or the carrying out of the alleged scheme to defraud in which the defendant is accused of participating.'").

[90] United States v. Turner, 551 F.3d 657, 666 (7th Cir. 2008) (quoting Schmuck v. United States, 489 U.S. 705, 710–11 (1989)).

[91] 18 U.S.C. § 1343 (emphasis added).

[92] *Compare* Efron v. Embassy Suites (Puerto Rico), Inc., 47 F. Supp. 2d 200, 205 (D.P.R. 1999) ("However, none of these facsimile transmissions are alleged to have traveled on interstate phone lines, a necessary component of the actus reus needed for indictment under the wire fraud statute."), *aff'd*, 223 F.3d 12 (1st Cir. 2000), *and* Ctr. Cadillac, Inc. v. Bank Leumi Tr. Co. of New York, 808 F. Supp. 213, 227 (S.D.N.Y. 1992) ("Wire fraud requires the additional element of a communication crossing state lines."), *aff'd*, 99 F.3d 401 (2d Cir. 1995), *and* United States v. Lewis, 554 F.3d 208, 213–14 (1st Cir. 2009) (collecting similar authorities), *with* United States v. Kieffer, 681 F.3d 1143, 1155 (10th Cir. 2012) ("Accordingly, we have no quarrel with the narrow proposition for which *Schaefer* still stands, namely that one individual's use of the internet, 'standing alone,' does not establish an interstate transmission.").

[93] United States v. O'Donovan, 126 F.4th 17, 35 (1st Cir. 2025).

[94] *Id.* at 36. *O'Donovan* involved honest services wire fraud, a topic discussed in other CRS products. *See* CRS Report R45479, *Bribery, Kickbacks, and Self-Dealing: An Overview of Honest Services Fraud and Issues for Congress*, by Michael A. Foster (2020).

[95] *Kieffer*, 681 F.3d at 1155.

interstate transmission."[96] In October 2025, the Tenth Circuit applied similar reasoning in holding that § 1343 did not reach the conduct of a defendant who modified business records on a Utah website.[97] The government had offered evidence that the defendant and other users accessed the website from Utah and argued that the website was "publicly available and that changes made to it are broadcast and available across state lines."[98] The court stated that this evidence failed to prove that the defendant's "communication actually traveled outside Utah" when he "modified the information on the website."[99] Further, because the government did not prove that the relevant website access involved out-of-state servers, the court distinguished from a prior case holding that an interstate transmission may occur for § 1343 purposes if the host server of a fraudulent website is in a different state than other computers used in a fraudulent scheme.[100]

As a result of this disagreement, it appears that federal prosecutors in some jurisdictions likely need to establish more than mere internet use to prove a violation of § 1343. In practice, however, prosecutors could demonstrate the requisite connection to commerce with proof of a transmission across state lines,[101] which could still include instances where a communication is sent and received in the same state *if* that communication is routed through equipment in another state.[102]

Interstate Threats

The interstate threats statute, 18 U.S.C. § 875, authorizes criminal penalties for certain types of threats when they are transmitted "in interstate or foreign commerce."[103] For example, § 875(c) prohibits threats to kidnap or injure another, assuming they are "transmit[ted] in interstate or foreign commerce."[104] Thus, the jurisdictional language of § 875 is virtually identical to that used in the pre-2008 CSAM provisions and in § 1343.[105] One federal district court in the Third Circuit approved of a jury instruction stating that "use of the Internet, standing alone, is enough to satisfy the interstate commerce element of § 875(c)."[106] On appeal, the Third Circuit agreed (although its

[96] *Id.* at 1153, 1155.

[97] United States v. Baker, 155 F.4th 1188, 1203 (10th Cir. 2025).

[98] *Id.*

[99] *Id.*

[100] *Id.* (discussing *Kieffer*, 681 F.3d at 1153–55).

[101] MODEL CRIMINAL JURY INSTRUCTIONS § 6.18.1343-1 (3d. Cir. 2024), https://www.ca3.uscourts.gov/sites/ca3/files/2023Chap%206%20Fraud%20Offenses%20final.pdf [https://perma.cc/L5JA-B974].

[102] Some of the cases on this point involve pre-internet technologies. *See, e.g.*, United States v. Bryant, 766 F.2d 370, 374 (8th Cir. 1985) (describing wire fraud prosecution premised on telegrams sent and received in Missouri but routed through Virginia); *see also* United States v. Davila, 592 F.2d 1261, 1263 (5th Cir. 1979) (rejecting the defendant's "contention that the [wire fraud] statute was not meant to cover wires sent from point to point within a single state" when they were routed incidentally through a different state). Despite concluding that mere internet use alone does not prove interstate transmission, the Tenth Circuit has recognized situations in which a factual record may establish that internet use in a particular case did involve sufficient interstate transmission. *See Kieffer*, 681 F.3d at 1154 (explaining that a jury could reasonably conclude that interstate transmission occurred for § 1343 purposes where the host server for a fraudulent website is in a different state than the end users).

[103] 18 U.S.C. § 875.

[104] *Id.* § 875(c).

[105] *Supra* "CSAM Statutes"; "Wire Fraud."

[106] United States v. Elonis, 897 F. Supp. 2d 335, 343 (E.D. Pa. 2012), *aff'd*, 730 F.3d 321 (3d Cir. 2013), *rev'd and remanded*, 575 U.S. 723 (2015), *and aff'd*, 841 F.3d 589 (3d Cir. 2016).

opinion was later reversed and remanded on other grounds by the Supreme Court).[107] Other federal courts have reached similar conclusions.[108]

In the context of pre-internet technology such as telephones and radio, some federal courts have interpreted § 875 to require that a threat cross state borders.[109] An inference that at least some federal courts would apply that rule to internet threats may be drawn from one of the CSAM cases discussed above. In *United States v. Wright*, the Ninth Circuit held that a pre-2008 CSAM provision "required the government to prove that the child pornography images actually crossed state lines."[110] In reaching that conclusion, the court drew support from precedent holding that § 875 "required the government to prove that the threats themselves . . . traveled across state lines."[111] Further, it seems likely that the Tenth Circuit would demand proof of more than mere internet use to satisfy § 875 given the provision's similarity to § 1343, where it has interpreted the statute to contain such a requirement.[112]

Regardless, in practice, in evaluating commerce challenges to § 875, federal courts have sometimes not reached the issue of whether mere internet use suffices, given evidence that the threat actually crossed state lines.[113] This is because internet communications are often routed through servers physically located in a different state from the sender or recipient.[114] As such, even where a sender and recipient are within the same state, § 875 can be satisfied by proof that the threatening communication is routed, even briefly,[115] through equipment or computers located in a second state.[116]

[107] *Elonis*, 730 F.3d at 335 ("Based on our conclusion that proving internet transmission alone is sufficient to prove transmission through interstate commerce, the District Court did not err in instructing the jury.").

[108] *See* United States v. Baker, 514 F. Supp. 3d 1369, 1377–78 (N.D. Fla. 2021) ("Placing a communication on the internet in a virtual 'location' that can be accessed by any member of the public—from anywhere in the United States or the world—satisfies the requirement that the communication be transmitted in interstate or foreign commerce."); United States v. Jeffries, No. 3:10-CR-100, 2011 WL 13186518, at *15 (E.D. Tenn. May 24, 2011) ("In the context of 875(c) violations, several courts have held that the interstate requirement was satisfied when the communication was sent over the Internet."); *see also* United States v. Haas, 37 F.4th 1256, 1264–65 (7th Cir. 2022) (examining whether use of the internet without proof that the message crossed state lines could suffice for § 875(c) purposes given the inherent "cross-border nature" of the internet, but declining to resolve the issue, which it observed has divided other circuits in related contexts).

[109] *See* United States v. Kinney, No. 22-CR-31-DKW, 2023 WL 2405614, at *1 (D. Haw. Mar. 8, 2023) (collecting cases).

[110] United States v. Wright, 625 F.3d 583, 600 (9th Cir. 2010).

[111] *Id.* at 593.

[112] *See supra* notes 95–96.

[113] *See, e.g.*, *Haas*, 37 F.4th at 1265 (holding that the defendant's use of the internet "to transmit a post from Illinois to Russia would be more than sufficient to uphold the jury's verdict"); *see also* United States v. Kinney, No. 22-CR-31-DKW, 2023 WL 2405614, at *1 (D. Haw. Mar. 8, 2023) ("However, the flaw in [the Defendant's] argument . . . is that the Government's evidence in this case consisted of more than the sole fact that the Internet was used. Rather, as [the Defendant] himself concedes, and as he stipulated at trial, the Instagram posts at issue here did travel across state lines when they were uploaded to out-of-state servers.").

[114] *See* United States v. Kammersell, 196 F.3d 1137, 1138 (10th Cir. 1999) (noting that "[e]very message sent via AOL automatically goes from the state of origin to AOL's main server in Virginia before going on to its final destination").

[115] United States v. Nissen, 432 F. Supp. 3d 1298, 1321 (D.N.M. 2020) ("Section 875(c)'s interstate commerce element is satisfied when a communication actually crosses state lines, however briefly.").

[116] *See, e.g.*, *id.* (determining that a telephone call fit within the jurisdictional scope of § 875 despite being sent and received in New Mexico, because it was routed through a "switch" in Texas); *see also Kammersell*, 196 F.3d at 1139 (holding that § 875 applied where a threatening instant message "was transmitted from Utah to Virginia to Utah").

The Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act (CFAA) is a primary tool in prosecuting cybercrimes at the federal level.[117] Although prosecutors may use the CFAA to charge hackers,[118] and courts and observers have described the CFAA as an anti-hacking statute,[119] the word "hacking" does not appear in any of its various provisions.[120] Instead, the statute criminalizes several categories of conduct involving unauthorized access to a computer.[121] Like the statutes discussed previously, the CFAA is grounded (at least in large part)[122] on the commerce power.[123] It is somewhat distinct, however, in that the jurisdictional nexus Congress relied on for many of the CFAA's provisions involves the status of the targeted computer itself, rather than the transmission of content in interstate or foreign commerce.[124] Specifically, numerous provisions of the CFAA prohibit conduct targeting "protected computers."[125] Among other things, the CFAA defines protected computers as those that are either "exclusively for the use of a financial institution or the United States Government" or that are "used in or affecting interstate or foreign commerce or communication . . . ."[126] Courts, including the Supreme Court, have construed the latter phrase to include any computer connected to the internet.[127] Given that construction, and the CFAA's broad

[117] *See* U.S. Dep't of Just., Just. Manual § 9-48.000 (2022) (describing importance of CFAA in "address[ing] cyber-based crimes"); 18 U.S.C. § 1030.

[118] *E.g.*, Press Release, U.S. Dep't of Just., Idaho Man Sentenced for Computer Hacking and Extortion Scheme (Nov. 13, 2024), https://www.justice.gov/archives/opa/pr/idaho-man-sentenced-computer-hacking-and-extortion-scheme [https://perma.cc/9VHU-6E8E].

[119] *E.g.*, United States v. Nosal (Nosal I), 676 F.3d 854, 857 (9th Cir. 2012); Ivan Evtimov et al., *Is Tricking a Robot Hacking?*, 34 BERKELEY TECH. L.J. 891, 904 (2019).

[120] *See* 18 U.S.C. § 1030 (proscribing various conduct without use of the word "hacking").

[121] *Id.*

[122] Some CFAA provisions, such as § 1030(a)(1), protect federal government interests and may be grounded in other sources of authority. *See generally* Berris, *supra* note 16, at 8–10 (summarizing various sources of constitutional authority for criminal laws protecting government property and personnel).

[123] United States v. Mitra, 405 F.3d 492, 496 (7th Cir. 2005).

[124] Section 1030(a)(7), an exception that does criminalize certain communications transmitted in commerce, is discussed below. In addition, the CFAA expressly criminalizes other conduct, including particular types of transmissions. *E.g.*, 18 U.S.C. § 1030(a)(5) (knowingly causing the transmission of "a program, information, code, or command," and thereby "intentionally caus[ing] damage without authorization to a protected computer"). For example, § 1030(a)(1), criminalizing cyber espionage, requires proof that the information obtained is "communicated, delivered, or transmitted" or that the defendant attempted to "communicate, deliver, [or] transmit" it. 18 U.S.C. § 1030(a)(1). Although the transmission under these provisions is part of the prohibited conduct, it appears that the relevant jurisdictional bases still focus on the status of the targeted computer rather than any interstate nature of the offending transmission. *See generally* CRS Report R47557, *Cybercrime and the Law: Primer on the Computer Fraud and Abuse Act and Related Statutes*, by Peter G. Berris, at 11–13, 18–21 (2023) (discussing elements of § 1030(a)(1), (5)).

[125] 18 U.S.C. § 1030.

[126] *Id.* § 1030(e)(2). A 2020 amendment to the CFAA expanded the definition of "protected computer" to include any computer that "is part of a voting system; and . . . is used for the management, support, or administration of a Federal election; or . . . has moved in or otherwise affects interstate or foreign commerce." Defending the Integrity of Voting Systems Act, Pub. L. No. 116-179, 134 Stat. 855 (2020) (codified in relevant part at 18 U.S.C. § 1030(e)(2)(C)). Some of this 2020 language could theoretically raise interesting questions about cyberattacks on computers that were transported in interstate commerce but that otherwise do not satisfy the definition of a protected computer, although that jurisdictional inquiry is outside the scope of this report.

[127] *See, e.g.*, Van Buren v. United States, 593 U.S. 374, 379 (2021) (interpreting the definition of protected computer in the context of one subsection of the CFAA to include "all computers that connect to the Internet"); hiQ Labs, Inc. v. LinkedIn Corp., 31 F.4th 1180, 1195 (9th Cir. 2022) ("The term 'protected computer' refers to any computer 'used in or affecting interstate or foreign commerce or communication[]'—effectively any computer connected to the Internet." (internal citations omitted) (quoting 18 U.S.C. § 1030(e)(2)(B))).

definition of computers,[128] most modern computing devices are subject to the CFAA's protections, including not only laptops and desktops but also devices such as smart appliances and fitness trackers connected to the *Internet of Things*[129]—"a system of interrelated devices connected to a network and/or to one another, exchanging data without necessarily requiring human-to-machine interaction."[130]Another important type of computer that fits within the definition of protected computer is a server—a computer that manages website data and other information.[131] For example, one court concluded that the web servers storing and sharing the member data of a large social media website qualified as protected computers.[132]

One CFAA provision—§ 1030(a)(7)—employs a similar jurisdictional approach to the wire fraud and interstate threats statutes.[133] In broad terms, it criminalizes making certain threats pertaining to unauthorized access to a protected computer, such as threats to damage a computer through the use of ransomware.[134] As a result, the provision's jurisdictional nexus turns less on the extent to which the target device implicates commerce, and more on the extent to which the threat does so.[135] In particular, § 1030(a)(7) requires proof that the defendant transmitted the threat "in interstate or foreign commerce."[136] There appears to be little caselaw interpreting the requirements of this language in the context of § 1030(a)(7).[137] In an unreported order stemming

[128] For a discussion of the CFAA definition of computers, *see* Berris, *supra* note 124, at 5.

[129] Although federal cases specifically examining the CFAA's applicability in the context of the Internet of Things are scarce, a number of observers have concluded that internet-enabled objects qualify as protected computers. Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1577–78 (2010); *see also* Sara Sun Beale & Peter Berris, *Hacking the Internet of Things: Vulnerabilities, Dangers, and Legal Responses*, 16 DUKE L. & TECH. REV. 161, 170 (2018) (discussing the extent to which internet-enabled objects fit within the scope of the CFAA). In one case, federal prosecutors used the CFAA to charge defendants who allegedly gained unauthorized access to Ring smart devices. Indictment, United States v. Nelson and McCarthy, No. 2:22-cr-00598-JAK (C.D. Cal. Dec. 16, 2022). Another example from case law is *United States v. Peterson*. 776 F. App'x 533 (9th Cir. 2019). In *Peterson*, the U.S. Court of Appeals for the Ninth Circuit considered a vagueness challenge to a condition of supervised release imposed on a defendant convicted of possessing child pornography. *Id.* at 533. The condition at issue restricted the defendant from accessing a computer as defined by the CFAA. *Id.* at 534. In agreeing with the defendant that the condition was potentially overbroad, the court observed that a wide range of objects fall within the definition of computer under the CFAA, including "refrigerators with Internet connectivity, Fitbit™ watches" and certain automobiles. *Id.* at 535 n.3. Although the court did not discuss these devices in relation to the phrase "protected computer," it described them in a manner that would satisfy the definition of protected computer under the CFAA; as the court indicated, Internet of Things devices are (1) computers and (2) connected to the internet. *Id.* at 534. For a similar example, see United States v. Wells, 29 F.4th 580, 588 (9th Cir. 2022), *cert. denied*, 143 S. Ct. 267 (2022) (mem.).

[130] CRS In Focus IF11239, *The Internet of Things (IoT): An Overview*, by Patricia Moloney Figliola (2020).

[131] *hiQ Labs*, 31 F.4th at 1195.

[132] *Id.*

[133] 18 U.S.C. § 1030(a)(7).

[134] *See* Berris, *supra* note 124, at 23–24.

[135] *Id.* at 25.

[136] 18 U.S.C. § 1030(a)(7).

[137] *See* SkyHop Techs., Inc. v. Narra, 58 F.4th 1211, 1224 (11th Cir. 2023) ("Our Circuit has not yet had an opportunity to discuss the scope of § 1030(a)(7)(A)"). As of September 23, 2025, a search of the Westlaw database for cases citing to § 1030 using the phrase "transmits in interstate or foreign commerce" yielded only eleven cases, only two of which were reported. 18 U.S.C. § 1030 (West, Westlaw through Pub. L. No. 116-179) ("Citing References" filtered by "Cases" and "transmits in interstate or foreign commerce"). Similarly, a search for cases citing the CFAA and mentioning "1030(a)(7)" yielded only nine reported cases. *Id.* ("Citing References" filtered by "Cases" and "1030(a)(7)" and "Reported"). Few of the cases identified through these and similar searches addressed the question of what conduct satisfies the jurisdictional language of § 1030(a)(7); this section of the report describes the most relevant examples.

from a civil dispute,[138] one federal district court seemed to assume that mere internet use satisfied the jurisdictional language of § 1030(a)(7).[139] It seems possible that at least some federal courts might disagree, given their diverging interpretation of the functionally identical jurisdictional language in the interstate threats, wire fraud, and pre-2008 CSAM contexts discussed above.[140] Regardless, as with the wire fraud and interstate threats statutes, threats that actually cross state borders may satisfy § 1030(a)(7)'s jurisdictional requirements.[141]

Before 2008, § 1030(a)(2)(C)—criminalizing obtaining information through unauthorized access to a protected computer—required proof that the "conduct involved an interstate or foreign communication."[142] According to DOJ, that "limitation precluded prosecution in serious cases where sensitive or proprietary information was stolen from within a single state, as is often the case with 'insider' thefts."[143] Congress amended the provision and removed the requirement.[144]

Congressional Considerations

When Congress seeks to criminalize the transportation of images, messages, or other content through its commerce power, it can potentially rely on its power to regulate interstate and foreign commerce.[145] If it does so, the internet can likely provide a sufficient nexus.[146] Congress has a choice over the extent to which it wants to exert that commerce power. It could limit the prohibited conduct to transportation in interstate or foreign commerce, which at least some courts interpret to require proof of interstate transmission.[147] The wire fraud and interstate threats statute employ this approach, as did the pre-2008 CSAM provisions.[148] If Congress wants a particular provision to reach mere internet use, it could follow the model of the 2008 amendments to the CSAM provisions and include language covering the use of "any means or facility of interstate or

[138] "[M]ost of the published cases interpreting § 1030 arise in the civil context rather than the criminal context." ORIN S. KERR, COMPUTER CRIME LAW 31 (5th ed. 2022).

[139] *See* Inplant Enviro-Sys. 2000 Atlanta, Inc. v. Lee, No. 1:15-CV-0394-LMM, 2015 WL 13297963, at *4 (N.D. Ga. June 9, 2015) (concluding that plaintiff adequately stated a § 1030(a)(7) violation against defendant who transmitted extortionate communication "in interstate or foreign commerce, as [it was] sent via internet").

[140] *See supra* "CSAM Statutes," "Wire Fraud," and "Interstate Threats." One possible distinction is that § 1030(a)(7) covers threats against protected computers, which themselves are defined in part as devices used in, or affecting, commerce. *Supra* notes 125–127 and accompanying text. However, imputing that jurisdictional basis back to the crux of the prohibited conduct—issuing a threat—might raise a number of questions, including whether it would make surplusage of § 1030(a)(7)'s express requirement of transmission in commerce. *See* CRS Report R45153, *Statutory Interpretation: Theories, Tools, and Trends*, by Valerie C. Brannon, at 30–31 (2023) (describing concept of surplusage in statutory interpretation).

[141] *See SkyHop Techs.*, 58 F.4th at 1227 ("And the complaint easily satisfies the interstate-commerce requirement here: Indyzen transmitted the emails from California to Florida over the internet."). Reviewing legislative history, the Department of Justice has stated that "the threat need not be sent electronically" to satisfy § 1030(a)(7). COMPUT. CRIME & INTELL. PROP. SECTION, CRIM. DIV., U.S. DEP'T OF JUST., PROSECUTING COMPUTER CRIMES 53 (2010), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf [https://perma.cc/JCX2-UNQY].

[142] 18 U.S.C. § 1030 (2007).

[143] PROSECUTING COMPUTER CRIMES, *supra* note 141, at 22.

[144] Identity Theft Enforcement and Restitution Act of 2008, Pub. L. No. 110-326, § 203, 122 Stat. 3560, 3561 (codified as amended at 18 U.S.C. § 1030(a)(2)(C)).

[145] *See supra* "Federal Criminal Law and the Commerce Power."

[146] Depending on the particular activity Congress aims to criminalize, its ability to do so may still be subject to constitutional limits, such as First Amendment protections for speech. For more information, *see generally* CRS In Focus IF11072, *The First Amendment: Categories of Speech*, by Victoria L. Killion (2024).

[147] *Supra* "The Internet and Internet Use as a Jurisdictional Basis Under the Commerce Power."

[148] *Supra* "Selected Statutory Examples."

foreign commerce" or conduct that is "in or affecting interstate commerce."[149] The Computer Fraud and Abuse Act, with its focus on crimes targeting internet-connected computers, provides a slightly different jurisdictional approach that might be a relevant model should Congress choose to prohibit other conduct targeting such devices.[150]

At a high level, the choices that Congress makes with respect to jurisdictional language can have a significant impact on the scope of federal criminal law, given the prevalence of computers and the omnipresence of the internet.[151] When Congress reaches mere internet use as opposed to interstate transmissions—as it chose to do when it amended the CSAM provisions—it arguably reaches relatively local conduct that ordinarily might be left to the states.[152] Under current jurisprudence at least, which treats the internet and computers as manifestations of the commerce power, this is for now more of a policy consideration than a legal one.[153]

On a practical level, the inherently cross-border nature of the internet might limit the number of cases in which the distinction between mere internet use and cross-border transmissions actually makes a difference.[154] Even courts that currently read §§ 1343 and 875 to require a transmission across a state border would interpret those statutes to reach instances where the offending message is sent and received in a single state, as long as it has been briefly routed through a second state.[155] Therefore, even in courts that interpret such statutes to require more than mere internet use, the distinction would matter only if prosecutors are unable to prove that the communication crossed state lines (however briefly). Federal judges have expressed varying opinions over the extent to which inability to demonstrate interstate transmission might actually be an obstacle to prosecution.[156] As discussed above, however, in the context of CSAM, the

[149] Act of Oct. 8, 2008, Pub. L. No. 110-358, § 103, 122 Stat. 4001. At least one bill would have, among other things, expanded the scope of the wire fraud statute's jurisdictional language to include language about facilities of commerce. Anti-Corruption Act of 1995, S. 1378, 104th Cong.

[150] *Supra* "The Computer Fraud and Abuse Act."

[151] *Cf.* United States v. Haas, 37 F.4th 1256, 1264 (7th Cir. 2022) ("Congress's choice of language in any given statute is thus critical. How it articulates the interstate-commerce element of a statute tells us what that statute will reach."); United States v. Kammersell, 196 F.3d 1137, 1139 (10th Cir. 1999) (describing the argument that a broad reading of jurisdictional language in a statute covering interstate transmissions would "cover almost any communication made by telephone or modem" because "so many . . . locally-sent Internet messages are routed out of state").

[152] *See* Berris, *supra* note 16, at 2 ("The Constitution reserves the police power to state governments, meaning that legislating to prohibit crime is a task that lies primarily within the purview of the states.").

[153] *See supra* notes 36–43 and accompanying text.

[154] United States v. Schaefer, 501 F.3d 1197, 1200 (10th Cir. 2007) (acknowledging that "in many, if not most, situations the use of the Internet will involve the movement of communications or materials between states"); *Kammersell*, 196 F.3d at 1139 (describing the argument that a broad reading of jurisdictional language in a statute covering interstate transmissions would "cover almost any communication made by telephone or modem" because "so many . . . locally-sent Internet messages are routed out of state").

[155] *See*, *e.g.*, United States v. Bryant, 766 F.2d 370, 374 (8th Cir. 1985) (describing wire fraud prosecution premised on telegrams sent and received in Missouri but routed through Virginia); *Kammersell*, 196 F.3d at 1139 (holding that § 875 applied where a threatening instant message "was transmitted from Utah to Virginia to Utah").

[156] *Compare* United States v. MacEwan, 445 F.3d 237, 244 (3d Cir. 2006) ("Moreover, as is evident from the trial testimony of the government's expert, unless monitored by specific equipment, it is almost impossible to know the exact route taken by an Internet user's website connection request, such as [the defendant's] requests to connect with various child pornography websites."), *with Schaefer*, 501 F.3d at 1208 (Tymkovich, J., concurring) ("Typically, the evidence of the interstate element is readily presented by the prosecution, or can be gleaned from the record. Most Internet cases, for example, include testimony regarding the location of the servers accessed by defendant, or some other evidence that reveals the interstate character of the particular transmissions at issue.").

possibility that prosecutors might be unable to prove interstate transmission was ultimately unacceptable to Congress, which resolved the issue through expanded jurisdictional language.[157]

Additional CRS Resources

Statutory Interpretation:

- CRS Report R45153, *Statutory Interpretation: Theories, Tools, and Trends*, by Valerie C. Brannon (2023)

Jurisdictional Bases for Federal Criminal Law:

- CRS Report R48177, *Components of Federal Criminal Law*, coordinated by Peter G. Berris (2024)
- CRS Report R45323, *Federalism-Based Limitations on Congressional Power: An Overview*, coordinated by Kevin J. Hickey (2023)
- CRS Legal Sidebar LSB10869, *If You Do the Space Crime, You May Do the Space Time*, coordinated by Peter G. Berris (2022)

CSAM:

- CRS Legal Sidebar LSB10713, *The Fourth Amendment and the Internet: Legal Limits on Digital Searches for Child Sexual Abuse Material (CSAM)*, by Michael A. Foster (2022)

Wire Fraud:

- CRS Legal Sidebar LSB11327, *Kousisis v. United States and the Reach of Federal Fraud Statutes*, by Cassandra J. Barnum (2025)
- CRS In Focus IF13008, *Cryptocurrency Investment Scams*, by Peter G. Berris and Kristin Finklea (2025)
- CRS In Focus IF12168, *Fertility Fraud: Federal Criminal Law Issues*, by Peter G. Berris (2022)
- CRS Report R41930, *Mail and Wire Fraud: A Brief Overview of Federal Criminal Law*, by Charles Doyle (2019)

Interstate Threats:

- CRS Legal Sidebar LSB10781, *Overview of Federal Criminal Laws Prohibiting Threats and Harassment of Election Workers*, by Jimmy Balser (2024)
- CRS Legal Sidebar LSB11063, *School Swatting: Overview of Federal Criminal Law*, by Peter G. Berris (2023)

Computer Fraud and Abuse Act:

- CRS Report R47557, *Cybercrime and the Law: Primer on the Computer Fraud and Abuse Act and Related Statutes*, by Peter G. Berris (2023)
- CRS Report R46932, *Ransomware and Federal Law: Cybercrime and Cybersecurity*, by Peter G. Berris and Jonathan M. Gaffney (2021)

[157] *See supra* note 73 and accompanying text.

Author Information

Peter G. Berris
Legislative Attorney

Disclaimer