THE WIRE FRAUD BOOM

YAKOV MALKIEL*

The federal wire fraud offense is so ubiquitous in today’s white-collar practice that we rarely pause to contemplate the dramatic arc of its development. The offense left Congress in 1952 on a mission to combat false advertising by radio and television.1 Flexible language allowed the offense to reach a variety of crimes (deemed “frauds”) executed through a variety of interstate methods of communication (deemed “wires”).2

Today, the wire fraud statute allows the federal government to prosecute a wide sweep of financial crimes involving numerous modern methods of communication.3 And in light of recent technological developments, a speedily growing share of our electronic communications travel across state lines. The result is that wire fraud will soon allow the federal government to prosecute almost every American financial crime.4 It is time to reckon with that state of affairs.

* Administrative Magistrate of the Massachusetts Division of Administrative Law Appeals, formerly an associate in the global white-collar practice of White & Case LLP. My then-colleagues or I (or both) made appearances in the cases discussed infra notes 43–45. This Article reflects my observations in a personal capacity only. I am grateful to Michael Kendall, Lauren Papenhausen, Marla Blum, and especially Yan Chu for their excellent ideas and assistance.


4. The appropriate borderlines between criminal and noncriminal financial schemes have been debated for decades (if not forever). See infra Section II.A. The word “crimes” here refers to conduct that courts have agreed to treat as such.
I. Legislative Origins

Today, wire fraud is as prominent as any other offense in the white-collar world, but it was born from modest ambitions.

Congress enacted wire fraud’s predecessor offense, mail fraud, in 1872. The mail fraud statute paralleled other contemporary enactments by extending the national government’s reach into matters previously dominated by the states. Reconstruction’s reinvigorated federalism was clearly at work.

The two essential components of a mail fraud charge are (1) the existence of a “scheme or artifice to defraud,” and (2) use of the mail system. The precise shape of each element has evolved through case law and legislative amendments. In particular, some early applications of mail fraud sought to limit the offense to schemes that, as a matter of design, focused or depended peculiarly on the mail. But a 1909 amendment to the statute made clear that mail fraud reaches fraudulent schemes of any variety, as long as a mailing furthered the scheme in some way.


8. See id. at 780 (stating that existing state laws were insufficient to combat growing post-war criminal activity, so “there existed a perceived need for federal intervention to dispel widespread fraud”).

9. 18 U.S.C. § 1841; see Williams, supra note 2, at 296 (citing United States v. Young, 232 U.S. 155, 161–62 (1914) (recognizing two elements for mail fraud charge following 1909 amendment)); see also Rakoff, supra note 7, at 783–84, 817 (noting that the original mail fraud statute had an additional element—intent to effectuate a scheme through mail correspondence—but Congress amended the statute to its current two-element form).

10. Rakoff, supra note 7, at 791-94 (noting that under the pre-1909 case law, courts applied a “mail dependence requirement” to narrowly construe possible applications).

11. See id. at 816–21. The Court’s holding in Young supported this broader reach of the mail fraud statute by classifying mailing as a mere “jurisdictional element.” Id. at 817 (citing Young, 232 U.S. at 161–62). But see Williams, supra note 2, at 296 (arguing that the Court’s dicta in Young retained some mail-emphasizing analysis) (quoting Young, 232 U.S. at 159).
The idea of enacting a wire fraud offense arrived in Congress through four identical proposals in 1949 and 1951. It too required a “scheme or artifice to defraud.” But instead of a mailing, wire fraud coupled the scheme with an interstate transmission. The statute’s original text required a transmission through an “interstate wire, radio, or television communication.” A 1956 amendment revised this language to require a “wire, radio, or television communication in interstate or foreign commerce.” Courts have understood this phrase to mean that the communication must “cross state lines.”

Congress originally conceived of the wire fraud offense as narrowly targeted. The House Committee on the Judiciary described the anticipated offense as addressing a “relatively isolated area of criminal conduct,” stemming from “[t]he rapid growth of interstate communications facilities, particularly . . . radio and television.” The Committee expected the proposed offense to overlap with existing penalties under the Federal Trade Commission Act for “dissemination by radio of fraudulent advertising of foods, drugs, and medicines.” In most cases, “either State laws or the mail-fraud statutes” would apply as well. The wire fraud statute was therefore expected to see “relatively infrequent occurrence.”

13. Williams, supra note 2, at 305.
15. See Matthew Angelo et al., Mail and Wire Fraud, 57 AM. CRIM. L. REV. 1023, 1025 (2020) (“[T]he wire fraud statute also requires proof of an interstate nexus because, in enacting the statute, Congress relied solely on its Commerce Clause power.”).
20. Id. at 2.
22. H.R. Rep. No. 388, at 2; see also id. at 11 (reporting a statement from a DOJ official that cases of radio and television frauds “were easily within the jurisdiction of the State”).
23. Id. at 2.
The proposals for a wire fraud offense all appear to have originated at the Federal Communications Commission (“FCC”).24 The FCC described the impetus for the statute as “situations in which persons have used radio facilities for the perpetration or attempted perpetration of obvious frauds.”25 The immediate concern revolved around radio ads: “A recent article contained in Broadcasting magazine for January 1, 1951, indicates . . . that several preholiday offers are now under investigation . . . .”26

The debate on the House floor reflected the same vision of a statute designed to combat false advertising by radio and television. Congressman Arthur Miller began the debate by voicing concern about the offense’s borderlines, which Congressman Byron Rogers sought to allay:

Mr. MILLER of Nebraska. . . . I would like to have an explanation of the bill, because I think most of us recognize there are many radio advertisements that tread closely on grounds of fraud. . . .

Mr. ROGERS of Colorado. For the information of the gentleman from Nebraska, this bill merely extends to radio the mail fraud type of law that now applies whenever you commit fraud through the United States mail. . . .

Mr. MILLER of Nebraska. Does the gentleman think it tightens up the code for advertising over the radio?

Mr. ROGERS of Colorado. This prohibits fraudulent radio and television advertising where the mails are not employed as an element in perpetrating the scheme.27

Congressman Rogers then fielded a softball question that invited him to underscore the same targeted view:

Mr. CUNNINGHAM. . . . [W]ill the gentleman state whether or not this bill would prevent fraudulent advertising by radio?

Mr. ROGERS of Colorado. Precisely. The principal objective of this bill is to eliminate fraudulent radio advertising in the same

24. A letter from the FCC to Speaker of the House Sam Rayburn dated February 13, 1951 recommended the enactment of a wire fraud offense (titled “Fraud by Radio”), with proposed statutory language. Id. at 4–5. The same language appeared in the Senate’s three bills, and the House made only minor tweaks in House Bill 2948 (introduced two weeks after the FCC’s letter).
25. Id. at 4.
26. Id. at 5.
manner as schemes to use the mails to defraud are presently barred.\textsuperscript{28}

The wire fraud offense took effect on July 16, 1952, as part of a session law largely devoted to amending the Communications Act.\textsuperscript{29} An exciting future awaited.

\textit{II. Doctrinal Features}

The thesis of this Article is that the scope of the wire fraud offense has exploded to encompass nearly every American financial crime. Recent technological developments have catalyzed this explosion, but the incendiary material was already present in the form of earlier-established doctrinal features of the fraud offenses. Those features relate to each of the offenses’ two key elements, namely the “scheme” and the interstate transmission.

\textit{A. The Scheme: Its Breadth}

The scheme to defraud is now notorious for its malleability.\textsuperscript{30} In 1980, fresh out of the United States Attorney’s Office, Judge Jed Rakoff wrote: “To federal prosecutors of white collar crime, the mail fraud statute is our Stradivarius, our Colt 45, our Louisville Slugger, our Cuisinart—and our true love.”\textsuperscript{31} Courts have construed the offense flexibly, as covering a variety of traditional and non-traditional “frauds”: “consumer frauds, stock frauds, land frauds, bank frauds, insurance frauds, and commodity frauds,” as well as “blackmail, counterfeiting, election fraud, and bribery.”\textsuperscript{32}

Wire fraud inherited the flexible definition of the “scheme to defraud” that developed in mail fraud cases. In 1955, a defendant argued that his scheme to defraud was unrelated to false radio advertising; he had simply used a telephone call in furtherance of a “previously formed scheme or artifice.”\textsuperscript{33} The Tenth Circuit acknowledged that, according to its legislative history, “the primary purpose in the enactment of the [wire fraud] statute was the

\begin{footnotesize}
\begin{itemize}
  \item \textsuperscript{28} Id. (statements of Rep. Cunningham and Rep. Rogers).
  \item \textsuperscript{31} Rakoff, \textit{supra} note 7, at 771.
  \item \textsuperscript{32} Id. at 772.
  \item \textsuperscript{33} Rose v. United States, 227 F.2d 448, 449 (10th Cir. 1955).
\end{itemize}
\end{footnotesize}
prevention of fraud through the use of radio.”34 The language of the statute, however, was “too clear for doubt,” and the court discerned no “Congressional intent or purpose to narrow the channel of the statute” beyond the statutory text.35 Wire fraud was to follow in mail fraud’s expansive footsteps.

The trend of giving free rein to the “fraud” element of both offenses persisted in the late twentieth century, over pushback from the Supreme Court. Especially in the 1970s and 1980s, federal prosecutors marshaled the fraud statutes to battle public and private corruption.36 The theory underlying these prosecutions was that, where a politician or employee behaves dishonestly, the victim—the public or the employer—is defrauded out of an “intangible right” to honest services.37

In its 1987 decision McNally v. United States, the Supreme Court rejected the view that the fraud statutes encompass deprivations of honest services.38 Yet Congress swiftly enacted a new provision expressly extending the fraud offenses to any “scheme or artifice to deprive another of the intangible right of honest services.”39 Corruption was “fraud” again.

Another rejoinder from the Supreme Court followed in 2010. In Skilling v. United States, the Court held that the honest services theory of fraud must be “pare[d] . . . down to its core” to avert a constitutional vagueness problem.40 That core, in the Court’s view, consisted of “bribery and kickback” schemes only.41 The “bribery” and “kickback” categories are not easy to define,42 but honest services has proven to be a vibrant, flexible

34. Id. at 449.
35. Id.
37. Id. at 461–62.
40. 561 U.S. 358, 404 (2010) (“[T]he Court acknowledges that [the defendant’s] vagueness challenge has force, for honest-services decisions were not models of clarity or consistency. It has long been the Court’s practice, however, before striking a federal statute as impermissibly vague, to consider whether the prescription is amenable to a limiting construction.”).
41. Id. at 412; see also id. at 368, 409.
theory. By way of illustration, recent prosecutions in the District of Massachusetts alone have charged honest-services wire fraud based on allegations that: an employee violated company rules by disclosing client information; physicists prescribed medically unnecessary opioids to their patients; and parents made payments to colleges to facilitate the admission of their children as athletic recruits.

Powered by the mail fraud case law and the “honest services” theory, wire fraud now covers nearly every variety of financial wrongdoing. It is the white-collar prosecutor’s newest, truest love: her Stratocaster, her Nikes, her Dyson, her iPhone.


46. The debates over the proper scopes of the scheme to defraud and the honest services theory continue. In 2020, the Supreme Court concluded that prosecutors in the “Bridgegate” case had stretched the scheme to defraud too far. Kelly v. United States, 140 S. Ct. 1565 (2020) (analyzing the forms of “money and property” that may serve as the objects of prosecutable schemes). Even as this Article prepares to go to press, two pertinent cases are awaiting Supreme Court merits decisions. See Percoco v. United States, No. 21-1158, https://www.supremecourt.gov/docket/docketfiles/html/public/21-1158.html (argued Nov. 28, 2022) (addressing the breadth of the category of people who may owe a duty of honest
B. The Transmission: Its Recipient

A less obvious feature of the fraud offenses is their flexibility with regard to the recipient of the mailing or wire. This aspect of the offense has grown in importance only recently.

The original paradigm of the mail fraud offense likely involved an ad or circular mailed to the intended victim. Congress had the same paradigm in mind for wire fraud, except that the defendant would be transmitting the solicitation to a radio-listening or television-watching audience. As a result, defendants could plausibly maintain, as one wire fraud defendant did in 1974, that the offense is “only applicable to schemes to defraud . . . persons to whom communications are directed.”

That defendant’s argument failed based on reasoning adopted long before wire fraud’s enactment. In a series of mail fraud cases, courts authorized charges and convictions where defendants directed mailings to people other than the victims. For instance, two decisions that bookended the nineteenth century upheld convictions arising from the defendants’ offers to mail counterfeit money to complicit recipients. The anticipated victims in such cases would have been, not the recipients of the mailings, but future third-party payees.

Another early-twentieth-century decision sustained a mail fraud conviction where the defendants invited a company’s customers by mail to boycott the company. And around the time of wire fraud’s enactment, the Supreme Court upheld a mail fraud conviction in which the defendant deposited a check—the proceeds of the crime—in a Texas bank, which then

services toward the general public); Ciminelli v. United States, No. 21-1170, https://www.supremecourt.gov/docket/docketfiles/html/public/21-1170.html (argued Nov. 28, 2022) (addressing the validity of the theory that a scheme to defraud may target the victim’s “right to control” an asset).

47. See supra Part I.
49. See, e.g., United States v. Jones, 10 F. 469 (C.C.S.D.N.Y. 1882); Milby v. United States, 120 F. 1, 2–3 (6th Cir. 1903).
50. See Jones, 10 F. at 470; Milby, 120 F. at 2–3.
51. Jones, 10 F. at 470 (upholding the conviction despite “the absence of any evidence to show an intention on the part of the accused to defraud [the mailing’s recipient]”); Milby, 120 F. at 4–5 (“[Although] the person ordering counterfeit money would know what he was to get . . . . the allegation of the indictment as to defrauding others by the subsequent circulation of the counterfeit money brings it within the statute.”). But see Stockton v. United States, 205 F. 462, 467–68 (7th Cir. 1913) (reversing the conviction of a purveyor of loaded dice whose scheme relied on the mail).
mailed the check to California.53 In both situations, the mailing clearly did not carry a communication to the victim.

A great majority of financial crimes arise from the coordinated actions of multiple individuals.54 Such individuals naturally communicate with each other in furtherance of their scheme. This truism has generated only occasional mail fraud prosecutions, because mail is not a common method of communication among accomplices. The same holds true for radio or television, the mediums that inspired Congress to enact the wire fraud statute. By contrast, accomplice-to-accomplice communications by interstate wire have become inordinately common, as a result of developments discussed in the next part.55

III. The Wire Comes of Age

Technological advances of the late twentieth century have caused a dramatic increase in the scope of the wire fraud offense. New technologies make wire transmissions, including those among accomplices, both ubiquitous and increasingly disposed to cross state lines.

A. Ubiquity

Today, constant streams of information travel from one person to another via electronic means of communication. Among the best known are email, cellphone calls, text messages, dedicated messaging applications (such as WhatsApp), and messaging features of numerous other applications (such as Instagram).56

53. Pereira v. United States, 347 U.S. 1, 8–9 (1954). But see Kann v. United States, 323 U.S. 88, 95 (1944) ("[T]he mailing has ordinarily had a much closer relation to further fraudulent conduct than has the mere clearing of a check.").

54. Conspiracy, the essence of which is a communicated agreement, has long been “one of the most commonly charged federal crimes.” White Collar Crime: A Survey of Law—Conspiracy, 18 AM. CRIM. L. REV. 206, 206 (1980). Indeed, it may be that the proliferation of communication technologies, as discussed in this Article, has made conspiracy an even more popular theory of prosecution.

55. Neither the case law nor this author have devoted much attention to the possibility that a wire to and from the same individual might satisfy wire fraud’s elements. It might be a stretch to deem such a wire a “communication.” See 18 U.S.C. § 1343. But prosecutors may think otherwise.

In the context of this Article, it is ironic that electronic communications are commonly described as "wireless." As early as the 1990s, courts viewed emails without hesitation as "wires" for purposes of the wire fraud offense.\(^{57}\) Courts have since also classified cellphone calls, text messages, and other electronic communications as "wires."\(^{58}\)

The theory that has led interpreters to categorize wireless communications as wires generally remains unarticulated. Perhaps the courts think of emails and cellphones as forms of technology that involve wiring somewhere down the line.\(^{59}\) In any event, the courts' attitude is consistent with Congress's choice to lump "wires" together with transmissions by radio or television.\(^{60}\) This juxtaposition makes clear that the focus of wire fraud's jurisdictional requirement is the use of an interstate communications infrastructure, whether physically wired or not.

A portion of the information now communicated by wire would have traveled in older times by mail. For instance, mail was a feasible method of dissemination for many solicitations that today circulate by email or app. And mail once delivered a large amount of banking information that today travels electronically.\(^{61}\)

\(^{57}\) See, e.g., United States v. Riggs, 743 F. Supp. 556, 562 (N.D. Ill. 1990); United States v. Hsu, 155 F.3d 189, 192-93 (3d Cir. 1998); United States v. Martin, 228 F.3d 1, 16 (1st Cir. 2000).


\(^{59}\) Cf. United States v. Martinez, No. ACM-39973, 2022 WL 1043620, at *9 (A.F. Ct. Crim. App. Apr. 6, 2022) ("[T]he defendant] used a text messaging application, which used the Internet, implicating wire communications."); United States v. Seidlitz, 589 F.2d 152, 156 (4th Cir. 1978) (noting that electronic messages "were wire or telephone communications since in each instance the defendant was exchanging messages with the computers over commercial telephone circuits").

\(^{60}\) 18 U.S.C. § 1343.

In other instances, electronic mediums have replaced less-modern wires. Communications that once would have relied on telex, telegram, and landline are now more likely to travel by email or by cellphone. Approximately four billion people are estimated to use email worldwide, including more than ninety percent of adult Americans. The number of cellphones worldwide has long exceeded that of humans. Sources now estimate cellphone users at more than ninety percent of the population in most countries, including about 280 million U.S. users.

Some new communications, especially by text message, may never have been sent in a pre-cellular world. A constant flow of updating and coordinating texts steers today’s meetings, outings, and other projects. We message each other to adjust our ETAs or to propose last-minute changes of venue. It was not so long ago that meetings and outings were coordinated to the best of our abilities in advance, with little room for subsequent adjustment.

An earlier section of this Article discussed wire fraud’s flexibility with regard to the recipient of the wire transmission. More specifically, a communication among accomplices suffices to satisfy the “wire” element. The types of schemes that the fraud offenses cover tend to be complex. Even financial crimes that involve no other transmissions are overwhelmingly


65. See supra Section II.B.

66. See, e.g., United States v. Abdallah, 840 F. Supp. 2d 584, 605 (E.D.N.Y. 2012), aff’d, 528 F. App’x 79 (2d Cir. 2013) (“It is axiomatic that an interstate telephone call, during which defendant discusses the fraudulent scheme and directs his accomplice to place fraudulent stock orders to further the scheme, constitutes the crime of wire fraud.”); United States v. Phillips, 647 F. App’x 917 (11th Cir. 2016) (holding that e-mails sent between accomplices satisfied interstate transmission element).
likely to involve some communications among the perpetrators. Today, those communications are almost certain to take place by “wires,” specifically email, cellphone calls, text messages, and messaging apps.67

B. Interstatedness

Federal prosecutors’ jurisdiction over wire-driven frauds depends on the wires traveling “in interstate or foreign commerce,”68 i.e., crossing state lines. That requirement is the focus of the final chapter of wire fraud’s development. In a nutshell, recent technological developments have made it rare for wire communications not to cross state lines.

It is useful to distinguish here between long-distance (interstate) schemes and local (intrastate) schemes. For present purposes, long-distance schemes are those that rely upon interactions among people located in separate states. Those people may be the accomplices only, or they may also include victims. Local schemes involve only intrastate interactions.

Long-distance schemes tend to rely on interstate communications by wire or mail irrespective of recent technological developments. It is true that such communications are now mostly relocated to new technologies. But this development does not much change the scope of the federal criminal law. For the most part, since their enactment, mail and wire fraud have already covered these long-distance schemes.

Even so, there is one way in which recent technological advances may have enlarged the universe of federally prosecutable long-distance schemes. Some long-distance schemes may rely on communications that, in precellular times, would not have taken place at all. For example, some interstate accomplices may use texts or other electronic messages to convey coordinating details that, but for these technologies, would have been shared in person, or not at all.69

Local schemes are where technological developments have dramatically reshaped wire fraud’s reach. Even when they are used locally, new technology communications tend to travel to faraway data hubs on the way

67. See United States v. Hoffman, 901 F.3d 523, 546 n.12 (5th Cir. 2018) (“With today’s rampant use of email and other technology . . . it will usually not be hard to identify scores of wires that further a scheme.”).
68. 18 U.S.C. § 1343.
69. See, e.g., United States v. Kenner, 13-CR-607, 2019 WL 4894238, at *2 (E.D.N.Y. Oct. 4, 2019) (relying on “[c]ontemporaneous text messages between [the accomplices]”; Hoffman, 901 F.3d at 546 (“An interstate email that says ‘Meet me at the bowling alley tonight’ can serve as the necessary wire if the parties planned the fraud while bowling a few frames that evening.”).
from sender to recipient. As a result, the interstate communication requirement may be satisfied even when the recipient and the sender are right next to each other.

It was not inevitable that the wire fraud statute would reach such cases. It would have been reasonable to theorize that only the locations of the sender and recipient determine whether a wire is interstate or intrastate in nature. But the courts have not taken that view. Their contrary approach dates back at least as far as 1957. In that year, the Ninth Circuit addressed a case where defendants advanced their fraud scheme by dispatching a telegram from California to Mexico City. At the time, the wire fraud statute did not yet reach “foreign” commerce; it was limited to “interstate” wires. The pitfall for the defendants was that the telegram traveled through Western Union facilities in Texas. Ever since, courts have agreed that a wire’s itinerary may satisfy the interstate-transmission element, regardless of the communicators’ locations.

The case law’s application of this premise to new technologies has focused on schemes furthered by email. Email systems are built by design to reach recipients indirectly: every message leaving a sender’s email system travels to a server, where recipients may retrieve it.

Wire fraud defendants have offered defenses based on the theory that the senders and recipients of pertinent emails were located in the same state.

---

70. Wentz v. United States, 244 F.2d 172, 173–74 (9th Cir. 1957).
71. Id. at 174–75; see supra notes 15–17 and accompanying text. Today, wire fraud may reach international schemes even when they are perpetrated from the foreign country. See United States v. Elbaz, 52 F.4th 593, 604 (4th Cir. 2022) (analyzing that wire fraud convictions based on foreign transmissions to victims in Maryland were “permissible domestic applications of wire-fraud statute”).
72. Wentz, 244 F.2d at 173–76. The court noted that the telegram was reduced to “tangible form” in Texas, a detail that arguably distinguishes Wentz from electronic-communication cases. See id. at 173.
73. Following Wentz, courts will sometimes examine “the path” of the wire transmission. See United States v. Van Cauwenberghe, 827 F.2d 424, 430 (9th Cir. 1987) (“In our case, evidence at trial demonstrated that the telex . . . followed a path consisting of three transmissions: (1) a foreign transmission from Geneva to New York City; (2) an intra-city transmission across New York City; and (3) an interstate transmission from New York City to Los Angeles.”).
75. See United States v. Hoffman, No. CR 14-022, 2015 WL 8306094, at *16 (E.D. La. Dec. 9, 2015) (entering an acquittal where an email’s sender and recipients “were located in the State of Louisiana,” and absent evidence “that the email in question traveled an interstate
But prosecutors are generally savvy to that argument. In email-based cases, prosecutors tend to offer evidence that the email server resided in a different state than the sender and the recipient. For instance, in *United States v. Laedeke*, prosecutors successfully showed that, although the sender and recipient of the pertinent emails were both in Montana, the server was in New York. In *United States v. Hoffman* and *United States v. Valdes-Ayala*, prosecutors put on evidence that the relevant email providers operated no servers in the state where neighboring accomplices communicated with each other. Both the Fifth Circuit and First Circuit accepted this evidence as sufficient to establish an interstate communication.

Even this kind of showing may not be required. Influential case law supports the position that internet-based communications are *always* interstate communications. The district court in *United States v. Fumo* offered a formative analysis:

> [T]he Internet, standing alone, is an instrumentality of interstate commerce. . . . Regardless of whether an e-mail is sent and received within the same state, “fluctuations in internet traffic” could result in the e-mail actually crossing state lines prior to

---

77. Id. at *2.
78. 901 F.3d at 546 (“To prove that the email crossed state lines, the government called [a] Yahoo paralegal. When [she] was asked whether Yahoo had any email servers in Louisiana between 2008 and the present, she responded ‘No.’ When asked whether an email would have to leave the state if it was sent from someone in Louisiana using a Yahoo account to someone else in Louisiana, she responded ‘Yes.’”).
79. 900 F.3d 20, 33 (1st Cir. 2018) (“[A] custodian of records for Microsoft Corporation testified that none of the email services operated by Microsoft . . . have servers located in Puerto Rico. So, if someone in Puerto Rico sent an email to someone else in Puerto Rico, then the email would have to cross state lines during its transmission.”).
80. *Hoffman*, 901 F.3d at 546 (holding that the absence of email server locations in Louisiana was sufficient to show an interstate communication between two persons located in Louisiana); *Valdes-Ayala*, 900 F.3d at 33 (holding that the absence of email server locations in Puerto Rico was sufficient to show an interstate communication between two persons located in Puerto Rico); *see also* United States v. Byrd, 377 F. App’x 374, 376 (5th Cir. 2010) (alluding to evidence that the defendant’s email crossed state lines on the way to a recipient in the same city).
reaching its final destination. Because such a determination is impossible, it is legally sufficient for purposes of the “interstate commerce” requirement that the e-mails at issue were sent and received through the Internet. 82

Other courts share this perspective. 83 Its significance is that it does not matter where the operative email servers are located: any email in furtherance of a fraudulent scheme satisfies the wire fraud offense’s demand for an interstate transmission.

This approach to the internet mirrors the attitude that the architects of the wire fraud statute held toward radio waves. The statute’s original drafters at the FCC described the requisite transmission as a “radio communication or interstate wire communication.” 84 The House revised the bill’s language so that the word “interstate” would modify radio transmissions as well (“interstate wire, radio, or television communication”). 85 The FCC was displeased with this edit, stating: “It has been consistently held that all radio broadcasting is interstate in character . . . . ‘By its very nature broadcasting transcends state lines and is national in its scope and importance . . . .’” 86 The House preferred its own language for practical reasons, but did not dispute the FCC’s analysis. 87 The view that wire fraud reaches every transmission

82. Id. at *9. The Fumo court relied on the Third Circuit’s earlier holding that images on the internet are within “interstate commerce” regardless of whether they “cross[] state lines.” Id. at *8 (citing United States v. MacEwan, 445 F.3d 237, 243–44 (3d Cir. 2006)).


87. Id. at 3.
reliant on a nationwide (or worldwide) infrastructure thus evokes the statute’s roots.88

The courts’ approaches to email are readily transposable to other internet-based methods of communication. Two enormously popular messaging services are WhatsApp, operated by Meta, and iMessage, operated by Apple.99 The architecture of both services parallels email: the sender’s device transmits a message to the service’s servers, where the recipient’s device retrieves the message.90 Both Meta and Apple maintain servers in several U.S. states.91

Local accomplices communicating by WhatsApp or iMessage are likely to satisfy wire fraud’s interstate-communication requirement based on the same theories developed in email cases. No matter how geographically close the sender and recipient are, prosecutors will usually be able to show that a message sent via WhatsApp or iMessage traveled through an out-of-state server. In courts that perceive internet-based communications as always traveling interstate, even this modest showing will not be necessary.92

Another bucket of modern-day wires consists of older-generation cellular technologies, namely cellular-network calls and SMS text messages. The key

88. Courts have expressed a similar attitude in the context of statutes that require the use of a “facility” of interstate commerce. See United States v. Giordano, 442 F.3d 30, 39–40 (2d Cir. 2006) (collecting authorities).


92. See supra notes 81–83 and accompanying text.
feature of these technologies, for present purposes, is that they transport messages through relatively well-defined routes, from cell tower to cell tower. Where wire fraud charges are based on such communications, courts tend to require proof that the trail of relevant cell towers ran across state lines. Some cellular communications between neighboring individuals will indeed take a circuitous, interstate route.

In other instances, local accomplices communicating only by cellular-network calls and SMS messages may remain beyond federal prosecutors’ reach. But the entire category of ventures reliant only on older-generation cellular technologies is shrinking. SMS messaging began to lose popularity to internet-based platforms long ago, especially because these platforms can be used for free on Wi-Fi networks. WhatsApp is now estimated to have more than two billion users. And iMessage is the default method of text-based communication among Apple’s wildly popular iPhones.

95. See Drury, 396 F.3d at 1312 (“[E]ach of the four calls [an accomplice] placed to [a] cellular phone was routed from Georgia through VoiceStream’s Jacksonville, Florida switching center, and then back into Georgia . . . .”).
Smartphone users coordinating crimes are especially likely to send their texts on server-based platforms such as WhatsApp and iMessage because these platforms offer “end-to-end” encryption: messages sent on them are not decodable at the service’s servers or elsewhere along the path from sender to recipient.100 Such messages are thus relatively safe from law enforcement’s eyes.101

Traditional cellphone calls are also losing ground to their alternatives. Today’s smartphone users reportedly text much more often than they call.102 And a variety of internet-based services transmit not only text messages, but also voice or video calls. These include WhatsApp (again),103 FaceTime (Apple’s offering),104 and Viber by Rakuten.105 Local accomplices using these internet-based options will be federally prosecutable, at least when their services’ servers happen to reside in another state. Looking into the future, some observers predict that cellular towers will be replaced by low-orbit satellites, causing all cellphone calls to cross state lines (or even planetary ones).106

C. Combined Effect

The “scheme to defraud” rubric now covers a broad range of behaviors.107 It would be rare for such behaviors not to rely on communications from or

100. Rose, supra note 90; Kumparak, supra note 90.
101. Other applications that are gaining in popularity because of their relative information security include Telegram and Signal. See Jack Nicas et al., Millions Flock to Telegram and Signal as Fears Grow over Big Tech, N.Y. TIMES (Jan. 13, 2021), https://www.nytimes.com/2021/01/13/technology/telegram-signal-apps-big-tech.html.
among the perpetrators. Today, such communications are extremely likely to use modern “wires” such as email, cellphone calls, text messages, and internet-based messaging apps. It is increasingly rare for such wires, even among neighboring communicators, to stay within state lines. The result is that wire fraud is increasingly capable of reaching every American financial crime, no matter how local.

IV. A Time for Reckoning

In the late twentieth century, Congress enacted a slate of new federal criminal statutes. According to a 1998 ABA report, forty percent of all federal crimes had been enacted during the preceding twenty-odd years.

This “federalization” of criminal law raised alarm bells among scholars and practitioners. They observed that criminal law was traditionally considered to be a matter of primary state and local concern. They worried that federal courts would become overburdened, federal prosecutors would acquire immoderate power, and similarly situated offenders would be treated differently by overlapping state and federal jurisdictions. Congress, apparently unmoved, left the new collection of crimes in place.

108. See supra Section III.A.
109. See supra Section III.B.
110. Even when a defendant’s conduct may have been covered by another federal offense, such as federal program bribery under 18 U.S.C. § 666, wire fraud’s expansion may permit prosecutors to “pile on” an additional, overlapping wire fraud charge. The result would be a longer maximum sentence.
115. AM. BAR ASS’N, supra note 111, at 32–35.
The story told in this Article raises parallel questions: Do we want the federal government to possess criminal jurisdiction over nearly all financial crimes? Are national or local authorities best situated to police local conduct? Should it be Congress or individual prosecutors who decide which financial crimes are the best uses of the federal government’s prosecutorial and penal resources?

Wire fraud’s expansion is different from late-twentieth-century federalization in a structural sense. Here, Congress enacted no new laws. A veteran statute has instead gained power as a byproduct of technological advances. As a result, Congress has not had occasion to consider the merits of the federalization process occurring today. It is time for a careful evaluation of those merits.117

In the end, this Article’s project is primarily descriptive. I hope to have demonstrated that wire fraud’s explosive potential today departs dramatically from Congress’s original aspirations. The prescriptive implications of the wire fraud boom are necessarily shaped by fundamental principles of federalism and prosecutorial policy. I am confident that this vignette will provoke a variety of nuanced normative reactions. I leave you to develop yours.

---

117 Features of wire fraud have always generated some of the same concerns identified by critics of late-twentieth-century federalization. See Rakoff, supra note 7, at 779 (“It may be argued . . . that the idiosyncrasies of design and interpretation that make the mail fraud statute so effective in combatting fraud likewise render it more liable to irrational, unpredictable or extreme applications and hence, to abuse.”); H.R. REP. NO. 388, at 8 (1951) (“[T]he area of criminal fraud is one in which the States are greatly interested. It would be a serious matter to exclude the States from jurisdiction in this area . . . ”).