In the
United States Court of Appeals
For the Seventh Circuit

No. 10-1347

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

DAVID S. SZYMUSZKIEWICZ,

Defendant-Appellant.

Appeal from the United States District Court
for the Eastern District of Wisconsin.
No. 07-CR-171—**Lynn Adelman**, *Judge*.

ARGUED JUNE 2, 2010—DECIDED SEPTEMBER 9, 2010

Before EASTERBROOK, *Chief Judge*, and POSNER and KANNE, *Circuit Judges*.

EASTERBROOK, *Chief Judge*. David Szymuszkiewicz was in trouble at work. His driver's license had been suspended for driving while drunk. This threatened his job because, as a revenue officer, Szymuszkiewicz was required to travel to delinquent taxpayers' homes. He worried he might be fired. One response, a jury found, was to monitor email messages sent to his supervisor,

Nella Infusino. She found out by accident when being trained to use Microsoft Outlook, her email client. She discovered a "rule" that directed Outlook to forward to Szymuszkiewicz all messages she received. Szymuszkiewicz was convicted under the Wiretap Act for intentionally intercepting an electronic communication. See 18 U.S.C. §2511(1)(a). The district judge denied his motion for a judgment of acquittal. 2009 U.S. Dist. LEXIS 60755 (E.D. Wis. June 30, 2009).

The district judge rightly rejected Szymuszkiewicz's attack on the sufficiency of the evidence. He had both motive and opportunity; direct evidence is not required. Szymuszkiewicz had access to Infusino's computer when she left her desk and could have set up a forwarding rule while she was away. Szymuszkiewicz denies knowing of Outlook's capacity for rules, but other IRS employees testified that this was common knowledge, and one witness testified that Szymuszkiewicz was sophisticated about computers. A motive to spy could foster a motive to learn the necessary steps. Szymuszkiewicz maintains the forwarding must have been a mistake. He occasionally stood in as acting manager, and so emails to Infusino would sometimes reach him legitimately. But agents found emails to Infusino stored in a personal folder of Szymuszkiewicz's Outlook client—in other words, Szymuszkiewicz not only received the emails but also moved them from his inbox to a separate folder for retention—which is not what would have happened had all of Szymuszkiewicz's access been legitimate.

Although forwarding lasted three years, most of the emails discovered on Szymuszkiewicz's computer were sent in the first half of each year, and none discusses his employment. He did not learn anything worthwhile. But an intentional interception is enough; the prosecutor need not show that the spy obtained valuable information. *In re Pharmatrak, Inc.*, 329 F.3d 9, 23 (1st Cir. 2003); *United States v. Townsend*, 987 F.2d 927 (2d Cir. 1993). The jury could have chosen to believe Szymuszkiewicz's contention that he received Infusino's emails legitimately, or by mistake, but the evidence supported the more sinister inference that he obtained them intentionally and without her knowledge.

Szymuszkiewicz contends that he should have been charged under the Stored Communications Act, 18 U.S.C. §§ 2701–12, rather than the Wiretap Act. He asserts that the rule on Infusino's computer directed the email system to forward her emails to him only "after the message arrive[d]." As a result, he says, he did not "intercept" anything, for (at least in football) "interception" means catching a thing in flight, and any message would have reached its destination (Infusino's inbox) before a copy was made for him. The Stored Communications Act covers illegitimate access to information that has come to rest on a computer system, making it the right statute, Szymuszkiewicz concludes.

It is risky to defend against one crime by admitting another. A court may be tempted to order a technical correction in the judgment if proof of one offense establishes all elements of the other. (Szymuszkiewicz's sen-

tence, 18 months' probation, could have been meted out under the Stored Communications Act, which allows a year's imprisonment for even the least serious violation. 18 U.S.C. §2701(b)(2)(A). And the sentencing guidelines for the two crimes, though not identical, both place a person low on the sentencing table.) But it is unnecessary to pursue that possibility, because Szymuszkiewicz's argument is based on the belief that Infusino's computer did the forwarding after each email arrived there. The evidence permitted the jury to find, however, that every message to Infusino went through the IRS's regional server in Kansas City, and that the server retained the message in its own files and dispatched two copies: one for Infusino and another for Szymuszkiewicz. Outlook's default is for an email client to send all rules to the server, which implements them. Only a rule that cannot be executed fully by the server requires help from a client machine. Microsoft Corporation, *E-Mail Rules Protocol Specification [MS-OXORULE]* §1.3.3 (2010). The prosecutor introduced a log from the Kansas City server showing that, when a message to Infusino arrived, the server sent a copy to Szymuszkiewicz within the same second; no action by Infusino's computer was necessary. The log shows that the rule Szymuszkiewicz created was implemented on the server side (per Outlook's norm), rather than the client side. The copying *at the server* was the unlawful interception, catching the message "in flight" (to use Szymuszkiewicz's preferred analogy).

What's more, it does not matter which computer did the copying. To see why, we need to take a brief foray

into the world of packet switching, the method by which nearly all electronic communications between computers are now sent. When the Wiretap Act was enacted in 1968, the normal communications pathway was circuit switching: the telephone company's machinery (initially switchboards, then mechanical solenoids, and finally computers) would establish a single electronic pathway, or circuit, between one telephone and another. Computers can communicate over dedicated circuits, but usually they break each message into packets, which can be routed over a network without the need to dedicate a whole circuit to a single message.

Each packet contains some of the message's content, plus information about the packet's destination. Each packet travels independently, moving from router to router within a network to find a path toward the ultimate destination. The Wikipedia entry on packet-switched networks contains a helpful description, plus citations to technical references. The routers, and the computers on both ends, arrange the packets (and their address information), and resend as necessary, so that at least one copy of each of the message's many packets reaches its goal. Lost packets can be repeated, and a whole message can be transmitted by sending each packet through a different route. Every packet may go by a different route. Only at the end are the pieces put back together and an intelligible communication formed. The path of any particular packet, and the order in which it arrives at the end, is irrelevant to the success of the communication. Computers use a recipe known as

a protocol that enables them to agree on how packets are formatted and reassembled. The three principal protocols for email are POP, IMAP, and SMTP, standing for Post Office Protocol, Internet Message Access Protocol, and Simple Mail Transfer Protocol.

One copy of each email sent to Infusino thus would be broken into packets and routed to Kansas City, where a server would reassemble it. Two copies of each message—one for Infusino, one for Szymuszkiewicz—then would be flung across the network. The pace of transmission would depend on the packets' travel, not just the order in which they were originally generated. If, for example, more packets were lost for one message than another, or if one message's packets traveled through more-congested routers, the messages would arrive at different times. Transmission speed also depends on the email protocol selected. The time at which each recipient obtained each message also depended on whether the recipient's computer was connected to the Outlook server when the message reached the server. This would be so both for Outlook's proprietary protocol and for most email systems in use. See Microsoft Corporation, *Mailbox Synchronization Protocol Specification [MS-OXCSYNC]* (2010); Internet Engineering Task Force, *Internet Message Access Protocol*, RFC no. 3501 (v. 4 rev. 1, 2003). The server would hold the message until each client connected.

Szymuszkiewicz's understanding of "interception" as "catching a thing in flight" is sensible enough for football, but for email there is no single "thing" that flies

straight from sender to recipient. When sender and recipient are connected by a single circuit, and the spy puts a "tap" in between, the football analogy makes some sense (though the tap does not prevent the recipient from getting the message; the spy gets a copy, just as Szymuszkiewicz did). For email, however, there are no dedicated circuits. There are only packets, segments of a message that take different routes at different times.

The Wiretap Act's definition of "interception" comprises packet-switch technology as well as circuit-switch technology. See *United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005) (en banc). It defines "interception" as "aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. §2510(4); see also *Doe v. Smith*, 429 F.3d 706 (7th Cir. 2005). An "electronic communication" is, in turn, "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. §2510(12). (We omit irrelevant exceptions.) Email messages are transfers of writings, and forwarding enabled Szymuszkiewicz to acquire those writings' contents. The difference between circuit-switch and packet-switch transmission methods thus is irrelevant under §2510. We agree with *Councilman*'s conclusion on that subject (as well as its conclusion that the Stored Communications Act does not repeal any part of the Wiretap Act by implication; each statute is fully enforceable according to its own terms).

Several circuits have said that, to violate §2511, an interception must be "contemporaneous" with the communication. *Fraser v. Nationwide Mutual Insurance Co.*, 352 F.3d 107, 113 (3d Cir. 2003); *Steve Jackson Games, Inc. v. Secret Service*, 36 F.3d 457 (5th Cir. 1994); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002); *United States v. Steiger*, 318 F.3d 1039, 1047 (11th Cir. 2003). Szymuszkiewicz sees this as support for his "in flight" reading, but it is not. "Contemporaneous" differs from "in the middle" or any football metaphor. Either the server in Kansas City or Infusino's computer made copies of the messages for Szymuszkiewicz within a second of each message's arrival and assembly; if both Szymuszkiewicz and Infusino were sitting at their computers at the same time, they would have received each message with no more than an eyeblink in between. That's contemporaneous by any standard. Even if Infusino's computer (rather than the server) was doing the duplication and forwarding, it was effectively acting as just another router, sending packets along to their destination, and *Councilman*'s conclusion that the Wiretap Act applies to messages that reside briefly in the memory of packet-switch routers shows that the Act has been violated.

In saying that the rerouting of the information *was* contemporaneous with the transit of each email, we do not imply agreement with any statement that the interception must *be* "contemporaneous." Decisions articulating such a requirement are thinking football rather than the terms of the statute. There is no timing requirement in the Wiretap Act, and judges ought not

add to statutory definitions. *Lockhart v. United States*, 546 U.S. 142, 146 (2005); *Union Bank v. Wolas*, 502 U.S. 151, 158 (1991); *H.J. Inc. v. Northwestern Bell Telephone Co.*, 492 U.S. 229 (1989); *Guerrero-Perez v. INS*, 242 F.3d 727, 736–37 (7th Cir. 2001). Forget about packet switching and email for a moment, and think about 1968-vintage telephony, with an old-fashioned answering machine containing an old-fashioned tape recorder on the receiver's end (which is how what today is called "voicemail" used to be set up). Perkins, the phone subscriber with an answering machine, could call his own number and key in a code to have his messages replayed from the tape. Suppose Smith learned the code, called Perkins's number, and listened to all of the messages on the answering machine. That means of acquiring the contents of a phone call is as effective as placing a "tap" on the phone line outside Perkins's house, or placing a hidden transmitter on the bottom of Perkins's phone, and comes within the definition of "interception" in §2510(4) even though the acquisition is not contemporaneous with the message. Under the statute, any acquisition of information using a device is an interception. And if getting access to an answering machine's contents is an interception, so is getting access to an email inbox's contents by automated forwarding.

The Stored Communication Act imposes its own penalties for clandestinely accessing information held "in electronic storage." 18 U.S.C. §2701(a). Playing back the messages on the answering machine would violate the Stored Communications Act—but this does not imply

that the activity does not violate the Wiretap Act too. Overlapping criminal statutes are nothing new. The two statutes have different definitions, different penalties, and different provisions for civil suit; they establish different rules for when (if at all) improperly acquired information may be used in court. There is no need to invent "contemporaneity" to keep them apart.

Our understanding of the Wiretap Act is essential to phone privacy as well as email security. Many phone calls today are made by digitizing speech and transferring the result by packet switching. Transmission by packet switching allows for multiple simultaneous messages over a single circuit and so is cheaper than circuit switching. The adoption of packet switching is not limited to "voice over IP" services such as Vonage or Skype. The fourth-generation protocol for mobile phones, being introduced this year in the United States, is one part of an effort to transmit all voice communications by IP ("Internet Protocol", a packet-switched method) before many more years have passed. See 3rd Generation Partnership Project, *All-IP Network (AIPN) Feasibility Study*, Technical Report no. 22.978 rel. 8 (Dec. 2008). The "interception" of a communication sent in packets must be done by programming a computer to copy the contents it sends along (and reassemble them later), which was exactly what Szymuszkiewicz told Infusino's computer to do with her incoming emails. In saying that the Wiretap Act's definitions treat the acquisition of emails as an interception, we ensure that the Act applies to packet-switched phone calls too.

Only one more point requires attention. The "interception" prohibited by §2511(1)(a) is the acquisition of a communication's contents "through the use of any electronic, mechanical, or other device." 18 U.S.C. §2510(4). The Wiretap Act defines an "electronic, mechanical, or other device" as

> any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than—
>
> (a) any telephone or telegraph instrument, equipment or facility, or any component thereof,
>
> > (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or
> >
> > (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;
>
> (b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal.

18 U.S.C. §2510(5). Szymuszkiewicz argues, citing two cases, that the "device" used to intercept a communica-

tion must differ from the device the intended audience uses to receive the message. See *Crowley v. Cybersource, Inc.*, 166 F. Supp. 2d 1263, 1269 (N.D. Cal. 2001); *Ideal Aerosmith, Inc. v. Acutronic USA, Inc.*, 2007 U.S. Dist. LEXIS 91644 (W.D. Pa. Dec. 13, 2007).

This argument does Szymuszkiewicz no good. The intended audience was Infusino, so on the approach of these decisions her computer was not a "device." But the server in Kansas City counts as a device; so does Szymuszkiewicz's own computer. And if we exclude the Kansas City server on the ground that it was integral to the legitimate transmission of the emails, Szymuszkiewicz's computer remains. He thus accessed nonpublic messages by means of a device capable of understanding them but unnecessary to the communication itself. *United States v. Chiavola*, 744 F.2d 1271, 1275 (7th Cir. 1984); *In re John Doe Trader No. 1*, 894 F.2d 240 (7th Cir. 1990).

More than that: we don't see any need to search for a device that is different from, or not integral to, the legitimate communication. *Crowley* and *Ideal Aerosmith* added this "different device" requirement to the statutory text to avoid what those judges thought would otherwise be a rule that made ordinary usage of a telephone or computer criminal. These judges feared that, unless the "device" must be extraneous to a proper communication, a person answering his own phone at home, and holding a conversation with a friend, would violate the Wiretap Act by acquiring the content of his own conversation using his own phone (a "device").

This fear just shows why it is a mistake to read snippets of a statute in isolation. For another section of the Wiretap Act declares that "it shall not be unlawful . . . for a person . . . to intercept a wire, oral or electronic communication where such person is a party to the communication or where one of the parties . . . has given prior consent." 18 U.S.C. §2511(2)(d). So acquiring the contents of one's own conversation, and sharing them over a speakerphone, is not unlawful, no matter what the word "device" means. It is better to follow the statute than to make up limitations to avert imaginary problems. Thus Szymuszkiewicz acquired the emails by using at least three devices: Infusino's computer (where the rule was set up), the Kansas City server (where the rule caused each message to be duplicated and sent his way), and his own computer (where the messages were received, read, and sometimes stored).

AFFIRMED