Use or Disclosure of E-mails Hacked by a Foreign Adversary

Neither the Wiretap Act nor the Stored Communications Act prohibits federal law enforcement officers from using or disclosing e-mails that were originally acquired by a foreign adversary's unlawful hacking into electronic storage in the United States and later obtained by the federal government through authorized foreign-intelligence activities.

August 28, 2020

MEMORANDUM OPINION FOR THE ATTORNEY GENERAL

You have asked whether the Wiretap Act, 18 U.S.C. §§ 2510–2523, or the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701–2713, restricts how federal law enforcement officers may use or disclose certain e-mails that were acquired in a foreign-intelligence operation. We understand that the federal government obtained these e-mails in the course of conducting authorized foreign-intelligence activities, which resulted in the acquisition of a number of documents from a foreign source through a means that would not itself be regulated or limited by the Wiretap Act or the SCA. The Department of Justice has been advised by U.S. intelligence officials that the foreign source acquired the e-mails from a foreign adversary, which, there is reason to believe, had unlawfully hacked into e-mail accounts in the United States. Because the foreign adversary originally acquired those e-mails in violation of federal law, you have asked whether the Wiretap Act or the SCA restricts the use or disclosure of those e-mails by federal law enforcement officials in connection with investigations they are conducting.[1]

The Wiretap Act contains strict protections governing the use of wire, oral, and electronic communications that are intercepted while in transit. The SCA restricts unauthorized access to stored electronic communications. Based upon the facts as we understand them, neither the Wiretap

[1] Because the federal government had no involvement in the original hacking of the e-mails, the Fourth Amendment to the U.S. Constitution does not restrict the government's use or disclosure of the information. *See, e.g.*, *United States v. Jacobsen*, 466 U.S. 109, 113 (1984) (recognizing that the Fourth Amendment "is wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official" (internal quotation marks omitted)).

Act nor the SCA prohibits the use or disclosure of the e-mails in question by federal officers. The Wiretap Act's prohibitions on the use or disclosure of intercepted communications apply only to communications acquired by a contemporaneous interception, not to those acquired by hacking into computer servers that store communications. At the same time, while the SCA prohibits unauthorized access to those servers, it does not contain a separate prohibition on how a hacker, much less an unrelated third party, may use or disclose e-mails that were acquired by such an illegal intrusion.

I.

The Wiretap Act was originally enacted by title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197, 211, and updated in relevant parts by title I of the Electronic Communications Privacy Act of 1986 ("ECPA"), Pub. L. No. 99-508, 100 Stat. 1848. The statute prohibits the interception of wire, oral, and electronic communications, as well as their subsequent use and disclosure, subject to various conditions and exceptions. *See* 18 U.S.C. § 2511. The Wiretap Act regulates the use and disclosure of intercepted electronic communications even when the person who acquired them had no role in their interception. Except as otherwise authorized, the statute bars, among other things, any person from "intentionally disclos[ing], or endeavor[ing] to disclose, to any other person," or "intentionally us[ing], or endeavor[ing] to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of [section 2511(1)]." *Id.* § 2511(1)(c)–(d). There are a number of exceptions to this restriction, both as a matter of statute, *see, e.g.*, *id.* § 2517, and under the First Amendment, *see Bartnicki v. Vopper*, 532 U.S. 514, 535 (2001). But generally speaking, the Wiretap Act imposes restrictions on how law enforcement officers may make use of communications intercepted in violation of its provisions.

The Wiretap Act's restriction on use or disclosure, however, applies only to communications that were "intercept[ed]" in violation of section 2511(1). 18 U.S.C. § 2511(1)(c)–(d). The term "intercept" means "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other

device." *Id.* § 2510(4). And an "electronic communication" is defined as including "any transfer" of information "transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system." *Id.* § 2510(12). As the Ninth Circuit has recognized, "the ordinary meaning of 'intercept' . . . is 'to stop, seize, or interrupt in progress or course before arrival.'" *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002) (quoting *Webster's Ninth New Collegiate Dictionary* 630 (1985)). That plain-language understanding is consistent with the statutory definition of "intercept," which speaks of the acquisition of the contents of an "electronic . . . communication," which in turn is defined as a "transfer" of electronic information.

Every federal court of appeals to address the issue has read "intercept" as requiring that a communication be acquired contemporaneously with its transmission. *See Boudreau v. Lussier*, 901 F.3d 65, 78 (1st Cir. 2018); *Luis v. Zang*, 833 F.3d 619, 627–29 (6th Cir. 2016); *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 113 (3d Cir. 2003); *United States v. Steiger*, 318 F.3d 1039, 1047–49 (11th Cir. 2003); *Konop*, 302 F.3d at 878; *Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 36 F.3d 457, 461–62 (5th Cir. 1994). As the Sixth Circuit has explained, "[t]he term 'intercept' . . . applies only to electronic communications, not to electronic storage." *Luis*, 833 F.3d at 627; *see* 18 U.S.C. § 2510(17) (defining "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof " and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication"). Thus, the Wiretap Act's prohibitions apply only to electronic information acquired during its "transfer." The prohibitions "do[] not apply to the acquisition of electronic signals that are no longer being transferred," i.e., those maintained in electronic storage. *Luis*, 833 F.3d at 627. In short, the Wiretap Act's prohibitions on subsequent use and disclosure capture only those electronic communications caught "in flight." *Id.*

This interpretation of the term "intercept" is consistent with the statutory history and historical practice. Before Congress enacted the ECPA, which extended the Wiretap Act to cover electronic communications, courts had read "intercept" to cover only acquisition contemporaneous with transmission. *See, e.g.*, *United States v. Turk*, 526 F.2d 654, 658 (5th Cir. 1976). When it enacted the ECPA in 1986, Congress retained that

definition—except with respect to wire communications, the definition of which was amended to "include[] any electronic storage of such [wire] communication." Pub. L. No. 99-508, sec. 101(a)(1)(D), § 2510(1), 100 Stat. at 1848. The ECPA did not include electronic storage in the definitions of either oral or electronic communications. *See* 18 U.S.C. § 2510(2), (12) (1988). The ECPA thus expanded the prior construction of "intercept" "with respect to wire communications only." *Konop*, 302 F.3d at 877 (emphasis omitted). Congress's omission of the storage component from the definitions of oral and electronic communications suggests that oral and electronic communications are not "intercept[ed]" when they are accessed in storage.

Were there any doubt, in 2001, Congress further amended the Wiretap Act by eliminating "electronic storage" from the definition of wire communication. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, sec. 209, § 2510(1), 115 Stat. 272, 283. This, too, reinforced the contemporaneity requirement. "By eliminating storage from the definition of wire communication, Congress essentially reinstated the pre-ECPA definition of 'intercept.'" *Konop*, 302 F.3d at 878. The apparent purpose of the amendment "was to reduce protection of voice mail messages to the lower level of protection provided other electronically stored communications." *Id.* (citing H.R. Rep. 107-236, pt. 1, at 158–59 (2001)). That amendment thus illustrated that "intercept" refers to the acquisition of a contemporaneous transfer of an electronic communication, rather than the acquisition of a communication that has already arrived and been preserved in electronic storage.

Reading "interception" as requiring contemporaneous acquisition is also consistent with the structure of title 18. The Wiretap Act concerns "wire and electronic communications interception." *See* 18 U.S.C. ch. 119 (chapter heading). The SCA concerns unauthorized access to "stored wire and electronic communications." *See* 18 U.S.C. ch. 121 (chapter heading). These distinct regimes include very different substantive requirements for, and procedural mechanisms by which, law enforcement officers may access or acquire electronic communications while they are being transferred versus while they are stored. *Compare id.* §§ 2516, 2518 (authorization and procedures for government interception of electronic communications), *with id.* § 2703 (same, for government acquisition of communications in electronic storage). In particular, "[t]he level of pro-

tection provided stored communications under the SCA is considerably less than that provided communications covered by the Wiretap Act." *Konop*, 302 F.3d at 879. If "acquisition of a stored electronic communication were an interception under the Wiretap Act, the government would have to comply with the more burdensome, more restrictive procedures of the Wiretap Act to do exactly what Congress apparently authorized it to do under the less burdensome procedures of the SCA." *Id.* Even if there could be circumstances where the Wiretap Act and the SCA overlap, *see id.* at 889 (Reinhardt, J., concurring in part and dissenting in part), Congress plainly intended that a different regime would apply to stored electronic communications.

We note that this conclusion presumes that a stored electronic communication is an "electronic communication" under the Wiretap Act in the first place. Yet under one reading of the statute, "[o]nce the transmission of the communication has ended, the communication ceases to be a communication at all. The former communication instead becomes part of 'electronic storage.'" *Luis*, 833 F.3d at 627. Some courts, however, have concluded that even though an interception requires contemporaneous acquisition, in large part because "electronic communication" is defined as a communication in "transfer," an electronic communication can nevertheless include a stored communication. *See Konop*, 302 F.3d at 876; *Steiger*, 318 F.3d at 1047. And the SCA separately refers to an "electronic communication while it is in electronic storage," which seems to preclude the conclusion that the two categories are mutually exclusive. 18 U.S.C. § 2701(a); *see also id.* § 2703(a) (referring to an "electronic communication[] that is in electronic storage"). It may be that this textual oddity has no happy resolution. The Wiretap Act, after all, "is famous (if not infamous) for its lack of clarity." *Steve Jackson Games*, 36 F.3d at 462. In any event, regardless of the resolution of this point, the bottom-line conclusion of the First, Third, Fifth, Sixth, Ninth, and Eleventh Circuits remains the same: an "interception" requires the acquisition of a communication contemporaneous with its transmission.

Because the Wiretap Act's prohibitions on the use or disclosure of intercepted electronic communications apply only to communications acquired through a contemporaneous interception, those prohibitions do not apply to federal officers' use or disclosure of the e-mails in question. Although some cases may present technical questions concerning what constitutes contemporaneity based upon the technology at issue, *cf. Unit-*

ed States v. Councilman, 418 F.3d 67, 69 (1st Cir. 2005) (en banc) (concluding that messages in "temporary, transient electronic storage" constituted electronic communications in transit), we understand that here, the foreign hackers obtained the e-mails by accessing e-mail accounts where the e-mails were already being held in electronic storage. The e-mails in question were not acquired contemporaneously with their transmission. The Wiretap Act thus poses no bar on their use or disclosure by the investigators.[2]

II.

The SCA, enacted by title II of the ECPA, prohibits unauthorized access to electronic communications facilities. *See* 18 U.S.C. § 2701(a). Specifically, the SCA prohibits any person from "intentionally access[ing] without authorization a facility through which an electronic communication service is provided" and from "intentionally exceed[ing] an authori-

[2] Even if the restrictions in sections 2511(c) and (d) could apply to the e-mails at issue, the Wiretap Act contains exceptions for certain uses and disclosures by investigative and law enforcement officers. *See* 18 U.S.C. § 2517(1), (2). Evaluating the applicability of those exceptions would require consideration of whether the federal investigators obtained the e-mails "by any means authorized by this chapter," and determinations about the meaning of the phrases "investigative or law enforcement officer" and "appropriate to the proper performance of [their] official duties." *Id.*; *see Title III Electronic Surveillance Material and the Intelligence Community*, 24 Op O.L.C. 261, 263–70 (2000) (discussing the meaning of "investigative or law enforcement officer" and "appropriate to the proper performance of [their] official duties"); *compare Forsyth v. Barr*, 19 F.3d 1527, 1543 (5th Cir. 1994) (interpreting "by any means authorized by this chapter"), *with Berry v. Funk*, 146 F.3d 1003, 1012 (D.C. Cir. 1998) (disagreeing with *Forsyth*'s interpretation), *and Chandler v. U.S. Army*, 125 F.3d 1296, 1300 (9th Cir. 1997) (reading *Forsyth* narrowly). We need not address those questions here because the Wiretap Act's prohibitions apply only to electronic communications that were acquired during their transmission.

In addition, the Supreme Court has held that the First Amendment in some circumstances protects disclosure of intercepted communications notwithstanding sections 2511(c) and (d). *See Bartnicki*, 532 U.S. at 535 (concluding that the government could not constitutionally punish "disclosures of lawfully obtained information of public interest by one not involved in the initial illegality"). We similarly need not resolve what force, if any, those First Amendment concerns would have here. *See Boehner v. McDermott*, 484 F.3d 573, 579 (D.C. Cir. 2007) (en banc) (concluding that, under *United States v. Aguilar*, 515 U.S. 593 (1995), "those who accept positions of trust involving a duty not to disclose information they lawfully acquire while performing their responsibilities have no First Amendment right to disclose that information").

zation to access that facility," and "thereby obtain[ing], alter[ing], or prevent[ing] authorized access to a wire or electronic communication while it is in electronic storage in such system." *Id.* The SCA also contains restrictions on disclosure by providers of electronic communication services and remote computing services. *See id.* § 2702(a).

By its terms, section 2701 applies only to unauthorized "access" of a facility. Accessing a facility in this sense "requires an intrusion into an electronic communication system." *Walker v. Coffey*, 956 F.3d 163, 168 (3d Cir. 2020). "Designed to prohibit 'hacking' into electronic communication facilities, section 2701 does not cover nonintrusive procurements of electronic communications." *Id.* Unlike the Wiretap Act's protections for intercepted communications, section 2701 does not prohibit the subsequent use or disclosure of electronic communications that have been unlawfully accessed while in electronic storage. As a number of district courts have explained, the "SCA punishes the act of accessing a 'facility through which an electronic communication service is provided' in an unauthorized manner"; it "does not punish disclosing and using the information obtained therefrom." *Cardinal Health 414, Inc. v. Adams*, 582 F. Supp. 2d 967, 976 (M.D. Tenn. 2008); *see also Cousineau v. Microsoft Corp.*, 6 F. Supp. 3d 1167, 1172 (W.D. Wash. 2014); *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 973 (C.D. Cal. 2010); *In re Am. Airlines, Inc., Privacy Litig.*, 370 F. Supp. 2d 552, 558–59 (N.D. Tex. 2005); *Sherman & Co. v. Salton Maxim Housewares, Inc.*, 94 F. Supp. 2d 817, 820 (E.D. Mich. 2000); *Wesley Coll. v. Pitts*, 974 F. Supp. 375, 389 (D. Del. 1997), *aff 'd*, 172 F.3d 861 (3d Cir. 1998); *Educ. Testing Serv. v. Stanley H. Kaplan, Educ. Ctr., Ltd.*, 965 F. Supp. 731, 740 (D. Md. 1997). Section 2702 restricts the disclosure of the contents of communications while in electronic storage, but that restriction applies only to persons or entities that provide electronic communication services or remote computing services to the public. 18 U.S.C. § 2702(a)(1)–(3). Accordingly, "a person who does not provide an electronic communication service can disclose or use with impunity the contents of an electronic communication unlawfully obtained from electronic storage." *Sherman & Co.*, 94 F. Supp. 2d at 820 (internal quotation marks and alteration omitted).[3]

[3] The Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, similarly prohibits "access[ing] a computer without authorization or exceeding authorized access," as well as

Just as the SCA's general prohibition is limited to unauthorized access, rather than use, of a stored communication, the SCA does not require the exclusion of evidence that was obtained in violation of that prohibition, even when law enforcement agents themselves committed the violation (without otherwise violating the Fourth Amendment). The statute expressly provides that the damages remedies and sanctions under the statute "are the only judicial remedies and sanctions for nonconstitutional violations of this chapter." 18 U.S.C. § 2708. As a result, violations of the SCA, standing alone, are not subject to the exclusionary rule. *See United States v. Perrine*, 518 F.3d 1196, 1202 (10th Cir. 2008) ("[V]iolations of the ECPA do not warrant exclusion of evidence."); *Steiger*, 318 F.3d at 1049; *United States v. Smith*, 155 F.3d 1051, 1056 (9th Cir. 1998) ("[T]he Stored Communications Act expressly rules out exclusion as a remedy."). Communications obtained in violation of the SCA may be used as evidence in a criminal proceeding because the statute does not restrict how law enforcement agents may use or disclose such communications.

Here, federal law enforcement officers received certain e-mails from U.S. intelligence officials, who in turn had acquired them in connection with authorized foreign-intelligence activities. Although there is reason to believe that foreign hackers themselves originally acquired the e-mails in violation of the SCA, those hackers were in no way working in concert with, or at the direction of, the federal government, and section 2701 does not constrain the downstream use or disclosure of stored communications. Section 2702 similarly does not apply, since it governs disclosures by persons or entities providing an "electronic communication service" or a "remote computing service" concerning information maintained by their respective services. 18 U.S.C. § 2702(a). Accordingly, the SCA does not restrict how federal law enforcement officers may use or disclose the recovered e-mails.

---

trafficking in passwords, transmitting computer viruses, and threatening to damage computers, *id.* § 1030(a). Like the SCA, the CFAA "does not address the *use* of information after access." *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 205 (4th Cir. 2012); *see also, e.g.*, *Orbit One Commc'ns, Inc. v. Numerex Corp.*, 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010) ("The CFAA expressly prohibits improper 'access' of computer information. It does not prohibit misuse or misappropriation."). In addition, the CFAA contains an exception for "any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States . . . or of an intelligence agency of the United States." 18 U.S.C. § 1030(f).

III.

For these reasons, we conclude that neither the Wiretap Act nor the SCA prohibits federal law enforcement officers from using or disclosing e-mails that were originally acquired by a foreign adversary's unlawful hacking into electronic storage in the United States and later obtained by the federal government through foreign-intelligence activities.

Please let us know if we may be of further assistance.

STEVEN A. ENGEL
Assistant Attorney General
Office of Legal Counsel