Additional Questions Concerning Use of the EINSTEIN 2.0 Intrusion-Detection System

The deployment of an intrusion-detection system known as the EINSTEIN 2.0 program on the unclassified computer networks of the Executive Branch is consistent with the federal and state laws discussed in this opinion.

Under the best reading of the statute, the EINSTEIN 2.0 program would not violate section 705 of the Communications Act, because it would fall within section 705's exception permitting a person to "divulge" a communication through "authorized channels of transmission or reception," which allows either the sender or the recipient of an Internet communication to convey the required authorization by consenting to a communication's disclosure, including by clicking through an approved log-on banner or signing the computer-user agreement in order to gain access to a government-owned information system.

If section 2702(a)(3) of the Stored Communications Act applied to the EINSTEIN 2.0 program, the exception in section 2702(c)(1)(C) permitting disclosure based on "the lawful consent of the customer or subscriber" would also apply, because in this context the government, and no other party, should be understood as the "customer or subscriber" of the Internet service provider.

If a state law imposed requirements on the EINSTEIN 2.0 program exceeding those imposed by these federal statutes, it would stand as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress and therefore be unenforceable under the Supremacy Clause of the Constitution.

August 14, 2009

MEMORANDUM OPINION FOR THE
ASSOCIATE DEPUTY ATTORNEY GENERAL

You have asked us to address whether the deployment of an intrusion-detection system known as the "EINSTEIN 2.0" program on the unclassified computer networks of the Executive Branch is consistent with (1) section 705(a) of the Communications Act of 1934, as amended, 47 U.S.C. § 605(a) (2006); (2) the provision of the Stored Communications Act codified at 18 U.S.C. § 2702(a)(3) (2006); and (3) state laws concerning interception or electronic surveillance. For the reasons given below, we conclude that it is.[1]

[1] We solicited the views of the Criminal Division and National Security Division on each of these questions. Both components concur in our conclusions.

I.

You have asked whether by engaging in any of the activities that are part of the EINSTEIN 2.0 program,[2] the Department of Agriculture ("USDA"), the Department of Homeland Security ("DHS"), or the relevant Internet service provider ("ISP") would violate section 705(a) of the Communications Act of 1934, as amended, 47 U.S.C. § 605(a) (2006). Although this is a novel question, and the statute is hardly a model of clarity, we conclude that under the best reading of the statute, the EINSTEIN 2.0 activities would not violate section 705.

In pertinent part, section 705 provides:

> Except as authorized by chapter 119, title 18 [i.e., the Wiretap Act], no person receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception,
>
> (1) to any person other than the addressee, his agent, or attorney,
>
> (2) to a person employed or authorized to forward such communication to its destination,
>
> (3) to proper accounting or distributing officers of the various communicating centers over which the communication may be passed,
>
> (4) to the master of a ship under whom he is serving,
>
> (5) in response to a subpena issued by a court of competent jurisdiction, or
>
> (6) on demand of other lawful authority.

47 U.S.C. § 605(a).[3] The Communications Act defines "person" in 47 U.S.C. § 153(32) (2006) to "include[] an individual, partnership, associa-

[2] These activities are described in detail in a memorandum of this Office. *See Use of the EINSTEIN 2.0 Intrusion-Detection System to Protect Unclassified Computer Networks in the Executive Branch*, 33 Op. O.L.C. 63 (2009) ("EINSTEIN 2.0 Opinion").

[3] Section 705 contains additional prohibitions, such as on the "intercept[ion] [of] any radio communication and divulg[ing] or publish[ing]" of its contents, and on the use for personal benefit of radio communications intercepted or received without authorization.

tion, joint-stock company, trust, or corporation." "[C]ommunication by wire" is defined as "the transmission of writing, signs, signals, pictures, and sounds of all kinds by aid of wire, cable, or other like connection between the points of origin and reception of such transmission, including all instrumentalities, facilities, apparatus, and services (among other things, the receipt, forwarding, and delivery of communications) incidental to such transmission." *Id.* § 153(52).[4]

Although the scope of section 705's prohibition is not entirely clear on its face, case law supports reading the provision as a general bar on a "person receiving, assisting in receiving, transmitting, or assisting in transmitting" wire or radio communications from "divulg[ing]" or "publish[ing]" such communications to persons other than the addressee, his agent or attorney, except "through authorized channels of transmission or reception," as "authorized by" the Wiretap Act, or in the circumstances enumerated in clauses (2) through (6). In *United States v. Finn*, 502 F.2d 938, 942 (7th Cir. 1974), for instance, the court identified the "absurdities" that would result from a literal reading of the text, including that "[c]lauses (2) through (6) would be rendered meaningless, for all of those categories are completely covered by the more general clause (1)." Similarly, reading clause (6) as a prohibition "would forbid divulgence of a communication 'on demand of other lawful authority,'" thereby "render[ing] all such demands unlawful and by its own terms [] eliminat[ing] the very category to which it refers." Instead, the court concluded, clauses (2) through (6) should be read "as exceptions to the general prohibition of clause (1)," a construction the court viewed as "the only way to give effect to the Congressional intent." *Id. Finn* is consistent with a line of precedents interpreting the pre-Wiretap Act version of this provision,

---

Except for the first sentence of section 705 quoted above, these additional provisions extend only to "radio" communications, which are not at issue here. *See* 47 U.S.C. § 605(a); *id.* § 153(33) (defining "radio communication" to "mean[] the transmission by radio of writing, signs, signals, pictures, and sounds of all kinds").

[4] This definition of "wire communication" is substantially similar to the definition of "electronic communication" under the Wiretap Act, 18 U.S.C. § 2510(12) (2006), which includes "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." *Cf. id.* § 2510(1) (defining "wire communication" under the Wiretap Act to mean an "aural transfer").

which contained substantially similar language. For instance, in *Nardone v. United States*, 302 U.S. 379, 380–81 (1937), the Supreme Court characterized the version of section 705 then in effect as providing that "no person who, as an employee, has to do with the sending or receiving of any interstate communication by wire shall divulge or publish it or its substance to anyone other than the addressee or his authorized representative or to authorized fellow employees, save in response to a subpoena issued by a court of competent jurisdiction or on demand of other lawful authority."[5] *See also Hanna v. United States*, 404 F.2d 405, 408–09 (5th Cir. 1968) ("[I]nformation thus lawfully obtained may be divulged 'in response to a subpoena issued by a court of competent jurisdiction, or on demand of other lawful authority.'" (quoting section 705)); *Bubis v. United States*, 384 F.2d 643, 646–47 (9th Cir. 1967) ("[N]o . . . person shall divulge or publish the existence, contents, substance, purport, or effect of any such communication to anyone other than the addressee or his authorized representative, or to authorized fellow employees, or in response to a subpoena issued by a court of competent jurisdiction, or on

[5] The version of the statute at issue in *Nardone* provided that:

> No person receiving or assisting in receiving, or transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception, to any person other than the addressee, his agent, or attorney, or to a person employed or authorized to forward such communication to its destination, or to proper accounting or distributing officers of the various communicating centers over which the communication may be passed, or to the master of a ship under whom he is serving, or in response to a subpena issued by a court of competent jurisdiction, or on demand of other lawful authority; and no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person; and no person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by wire or radio and use the same or any information therein contained for his own benefit or for the benefit of another not entitled thereto; and no person having received such intercepted communication or having become acquainted with the contents, substance, purport, effect, or meaning of the same or any part therof, knowing that such information was so obtained, shall divulge or publish the existence, contents, substance, purport, effect, or meaning of the same or any part thereof, or use the same or any information therein contained for his own benefit or for the benefit of another not entitled thereto . . . .

Communications Act of 1934, Pub. L. No. 73-416, § 605, 48 Stat. 1064, 1103–04.

demand of other lawful authority."); *Brandon v. United States*, 382 F.2d 607, 611 (10th Cir. 1967) (similar).

Although our research has not uncovered any case law applying section 705 in the context of cybersecurity activities, we conclude that the EINSTEIN 2.0 program falls within section 705's authorization to "divulge" a communication through an "authorized channel[] of transmission or reception." We assume for purposes of this analysis—but do not decide—that federal-systems Internet traffic would constitute "communication[s] by wire" under section 705, that the EINSTEIN 2.0 program would involve "divulg[ence] or publi[cation]" of the contents of such communications, that DHS or USDA would be a "person receiving, assisting in receiving, transmitting, or assisting in transmitting" such communications, and that the program would not be "authorized by" the Wiretap Act.[6]

---

[6] A number of those assumptions may not be necessary, and thus there may be additional bases for concluding that the EINSTEIN 2.0 program would not violate section 705. An argument might be made, for instance, that program activities are "authorized by" the Wiretap Act for purposes of section 705 because they are not affirmatively prohibited by that Act. *Compare United States v. Freeman*, 524 F.2d 337, 340 & n.5 (7th Cir. 1976) (phrase "[e]xcept as authorized by [the Wiretap Act]" in section 705 "permits" telephone companies to protect their rights or property pursuant to the relevant exception in 18 U.S.C. § 2511(2)(a)(i)), *with* EINSTEIN 2.0 Opinion, 33 Op. O.L.C. at 103 (concluding that "the better reading" of a related exception in FISA for conduct "authorized by" the Wiretap Act was to refer to affirmative "orders" obtained under that Act, rather than activities that "merely are not prohibited by those statutes"). Although we need not, and do not, resolve this question here, we note that such a reading of section 705 would not only incorporate the Wiretap Act's consent exception, *see* 18 U.S.C. § 2511(2)(a)(ii) (2006), but would also appear to import wholesale all of the statutory exceptions found in that Act, *cf., e.g.*, *id.* § 2511(2)(a)(i) ("rights or property"), essentially collapsing section 705 and the Wiretap Act into a single standard, notwithstanding that section 705(a) retained, by its plain terms, an independent limitation regarding wire communications.

It might separately be contended that any disclosure of communications by the service provider to DHS would occur on "demand of other lawful authority," although here DHS has entered into an agreement with USDA and thus arguably is not "demand[ing]" disclosure of communications. *Cf. Brown v. Continental Tel. Co.*, 670 F.2d 1364, 1365–66 (4th Cir. 1982) (request for records and telephone bills served on telephone company by Attorney for the Commonwealth was a "demand of . . . lawful authority" under section 705 because the statute's plain text contemplated the release of protected information "to appropriate authorities in response to a demand less compelling than a subpoena"). And with respect to any conduct of USDA or DHS that is potentially within the scope of section 705, there is some question whether the first sentence of section 705 applies to

We begin with the text of section 705, which expressly permits a "divulge[nce] or publi[cation]" of a wire communication made "through authorized channels of transmission or reception." We believe the plain language of section 705 is fairly interpreted to include the EINSTEIN scanning sensors as a "channel[] of transmission or reception" of Internet communications, particularly where a party to the communication has, as here, expressly authorized such scanning. In reaching this conclusion, we have considered the potential ambiguities concerning both what constitutes a "channel of transmission or reception" and what constitutes a channel that has been "authorized" for purposes of section 705.

As to the first issue, we are aware of a narrower construction of the phrase "channel[] of transmission or reception" that would be limited to the channel through which the communication actually passes from recipient to sender. Under such a reading, section 705 would prohibit, *inter alia*, forwarding of a mirror copy of federal systems Internet traffic to EINSTEIN 2.0 sensors for processing, *see* EINSTEIN 2.0 Opinion, 33 Op. O.L.C. at 67–68, or DHS's disclosure to another federal agency if that disclosure did not involve transmitting the communication to its recipient, unless one of the other express exceptions in the statute applied. But the text of the section does not by terms compel that narrower reading, given the placement of the relevant phrase. That phrase is located where it could be read to qualify the prohibition against divulgence to third parties, and thus to indicate that the channels being referenced are those that might be used to reach third parties. Indeed, the phrase itself, in its second appearance in the section, is not limited to channels of transmission by "wire,"

---

government employees. *Compare United States v. Hall*, 488 F.2d 193, 195 (9th Cir. 1973) (superseded on other grounds) ("The legislative history [] explicitly shows that Congress intended to exclude law enforcement officers from the purview of the new [section 705]"); S. Rep. No. 90-1097, at 108 (1968) ("[The first sentence of section 705] is designed to regulate the conduct of communications personnel."); *and Int'l Cablevision, Inc. v. Sykes*, 75 F.3d 123, 131 n.4 (2d Cir. 1996) (similar), *with Nardone*, 302 U.S. at 381 ("Taken at face value the phrase 'no person' [in the pre-Wiretap Act version of section 705] comprehends federal agents[.]"); *and United States v. Sugden*, 226 F.2d 281 (9th Cir. 1955) (interpreting pre-Wiretap Act version of section 705 to permit FCC agents to "listen [to radio communications] for the purpose of enforcing the [Communications] [A]ct" but to require exclusion of evidence, in a criminal prosecution unrelated to violations of that Act, obtained by FCC agents who intercepted defendant's short range radio transmissions). We need not, and do not, resolve these issues in light of our conclusion that the exercise falls within section 705's "authorized channels of transmission" provision.

suggesting a potentially broad conception of the means by which communications may be passed along. Furthermore, the text is not clear that the channel in question must be the one through which the original communication travels, as the text specifically refers to the divulgence, not of the communication itself, but of its substance or meaning. Insofar as the phrase "channels of transmission or reception" qualifies the divulgence, as its placement indicates, it is clearly intended to refer to channels other than those through which the communication flows.

As to whether the channel would be "authorized" for purposes of section 705, the dictionary defines "authorized" as "having authority[;] . . . recognized as having authority[;] . . . approved," and defines "authority" as, inter alia, "justifying grounds: basis, warrant." *Webster's Third New International Dictionary* 146 (3d ed. 1993). The statute does not specify the source or nature of the "authoriz[ation]" required. As a matter of ordinary meaning, the term "authorized" is certainly broad enough to encompass either the sender or receiver of a communication expressly authorizing—by means of indicating consent to—divulgence or publication. This reading is also supported by the terms of section 705's second sentence, which states that "[n]o person not being *authorized by the sender* shall intercept any radio communication and divulge or publish" that communication. 47 U.S.C. § 605(a) (emphasis added). That Congress chose the unqualified term "authorized" in the first sentence, while expressly limiting which party could authorize disclosure in the second, suggests an intent that the term be given a broader reading in the former instance.[7] We therefore would interpret the phrase "authorized channels of transmission or reception" to permit either the sender or the recipient of an Internet communication to convey the required authorization by consenting to a communication's disclosure in the context of the EINSTEIN 2.0 system.

Although we are not aware of any judicial precedent directly on point, we draw support for this reading of the statute from case law analyzing

[7] Our reading of "authorized" arguably also draws support from, and is entirely consistent with, the use of the word "authorizing" in the text of section 705(b), which contemplates a "marketing system" for satellite communications in which "agents have been lawfully designated for the purpose of authorizing private viewing by individuals" and "individuals receiving [satellite] programming ha[ve] obtained authorization for private viewing under that [marketing] system." 47 U.S.C. § 605(b).

consent by either the sender or receiver of a communication in determining whether interception or divulgence of a telephone call violated certain related provisions in section 705. In *Rathbun v. United States*, 355 U.S. 107 (1957), for instance, the Supreme Court held that the second clause of the version of section 705 then in effect (which provided that "no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person," *see supra* note 5) was not violated where the *recipient* of a phone call asked the police to listen to the call on an extension telephone in his home. The Court concluded, notwithstanding the statute's specific reference to the "authoriz[ation] [of] the sender," that "there ha[d] been no 'interception' as Congress intended that the word be used." 355 U.S. at 109. The Court looked to another related provision of section 705, which then prohibited any person from "receiv[ing] or assist[ing] in receiving any interstate or foreign communication by wire or radio and us[ing] the same or any information therein contained for his own benefit." That provision, the Court explained, gave "[t]he clear inference . . . that one entitled to receive the communication may use it for his own benefit or have another use it for him." *Id.* at 110. In dictum the Court further observed that even the defendant in that case conceded that under section 705 "either party may record the [telephone] conversation and publish it." *Id.*

Similarly, in *Weiss v. United States*, 308 U.S. 321 (1939), the Court held evidence to be inadmissible in a criminal trial where federal agents had violated the same provision of section 705 as in *Rathbun* (the prohibition against any person "not being authorized by the sender" intercepting and divulging communications) by tapping the defendant's intrastate phone calls. In rejecting the government's argument that the defendant's trial testimony about the intercepted conversations constituted consent, the Court relied on the fact that "divulgence was not consented to *by either of the parties* to any of the telephone conversations." *Id*. at 330 (emphasis added). More recently, in *United States v. Hodge*, 539 F.2d 898 (6th Cir. 1976), the court rejected a defendant's claim that agents of the Drug Enforcement Agency had violated section 705 by recording telephone conversations between the defendant and a government informant. (The informant in the case had consented to the DEA monitoring.) The court quoted section 705 in full before tersely dismissing the defendant's claim, explaining that "[i]t is well settled that there is no violation of the

[Communications] Act if the interception was, as here, authorized by a party to the conversation." *Id*. at 905.[8]

Although these cases do not interpret the phrase in section 705 upon which we rely here, they provide at least indirect support for reading the word "authorized," which appears without qualification as to the scope of the persons encompassed by it, to permit the recipient of a communication (either a federal agency, in the case of communications directly to that agency, or individual federal employees, in the case of communications to those employees) to consent to and thereby authorize the communication's disclosure in the context of the EINSTEIN 2.0 program.[9] At a minimum, our reading of the unqualified word "authorized" is consistent with what appears to have been the prior understanding that the statute was not, absent an express limitation regarding the scope of any consent exception, intended to require two-party consent for any such exception to apply.

As we explain below, we believe that under our reading of section 705, the manifestations of consent by USDA in conjunction with those of

---

[8] A modern line of cases brought by plaintiff corporations to prevent the unauthorized reception or transmission of satellite television signals has focused on the consent of the sending party in determining whether a "divulg[ence]" was "authorized." *See, e.g.*, *National Satellite Sports, Inc. v. Eliadis, Inc.*, 253 F.3d 900, 916–17 (6th Cir. 2001) (holding that private cable company had violated section 705 by selling the broadcast transmission of a boxing match to a commercial customer, when the company was only authorized by the program's originator to distribute it to residential customers). We do not read these cases as negating the relevance of the precedents discussed above, which contemplate consent by either party to communications such as telephone calls. For one thing, the modern case law does not purport to overrule or limit the precedents discussed above. More significantly, in this line of cases there is no contention that the recipient of a licensed commercial broadcast—who often acts pursuant to a contractual agreement with the originator—is "authorized" to distribute the material beyond the terms of that agreement.

[9] In light of this case law, we do not believe the existence of an express consent exception in the Wiretap Act requires a contrary interpretation of "authorized channel[] of transmission or reception" in section 705. When Congress reenacted the language of section 705 in the 1968 Wiretap Act, it did so against the settled background of case law interpreting the pre-Wiretap Act statute to allow consensual interception. By reenacting statutory text that was in large part identical to the preexisting language, and by indicating no disapproval of settled case law, Congress can be understood to have left in place the established meaning of the text it employed rather than to have impliedly precluded recognition of a consent exception.

individual federal employees using government information systems are sufficient to avoid a violation of that provision by the ISP, DHS, or USDA, in conjunction with the authorized operation of the EINSTEIN 2.0 system. First, with respect to potential violations by the service provider, we believe any "divulge[nce]" of communications would occur through an "authorized channel[] of transmission or reception." As to any disclosure by the provider of communications between third parties and USDA, the agency has "authorized" the service provider to disclose such communications to DHS by virtue of the Memorandum of Agreement between USDA and DHS, which memorializes USDA's consent to the scanning of its Internet traffic for cybersecurity purposes. As to disclosure by the service provider of communications addressed to or sent by individual employees, we have previously concluded that a federal employee's valid, voluntary consent to the scanning of Internet traffic is apparent from his clicking through an approved log-on banner or signing the computer-user agreement in order to gain access to a government-owned information system, *see* EINSTEIN 2.0 Opinion, 33 Op. O.L.C. at 98, and we believe this consent would foreclose any claim that the service provider would violate section 705 by transmitting communications through the intrusion-detection sensors operated by DHS because it would authorize any resulting divulgence.

We similarly conclude that the same consents—by USDA and USDA employees—"authorize" DHS to "divulge" the communications to any other authorized agency without running afoul of the prohibition in section 705. As to communications involving the agency itself, USDA has expressly consented to any such disclosures by DHS through the Memorandum of Agreement and other documents detailing the operation of the EINSTEIN 2.0 program. As to communications involving individual employees, the model log-on banner and computer-user agreement discussed in our EINSTEIN 2.0 Opinion state expressly that "[a]ny communications or data transiting or stored on this information system may be disclosed or used for any lawful government purpose." 33 Op. O.L.C. at 70. The scope of the employee's consent to disclosure for any "lawful government purpose" is informed by our separate conclusion in the context of 18 U.S.C. § 2511 that DHS is "authorized by law" to conduct an exercise involving EINSTEIN technology, as described in the implementation plan governing that exercise, by virtue of several affirmative statutory authorities, particularly a recent appropriations statute providing

funding for the precise exercise in question, as well as DHS's organic statute and the Federal Information Security Management Act.

Finally, we believe the log-on banner and computer-user agreements discussed above would also be sufficient to foreclose any claim that USDA would violate section 705 by divulging to DHS, through its participation in EINSTEIN 2.0, the contents of communications addressed to its employees.

This reading of section 705 is consistent with the conclusion in our EINSTEIN 2.0 Opinion that the EINSTEIN 2.0 program would not violate parallel non-disclosure provisions contained in the Wiretap Act. Section 2511(3) of title 18, U.S. Code, provides that "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication . . . while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient," except "with the lawful consent of the originator or any addressee or intended recipient of such communication," or "to a person employed or authorized, or whose facilities are used, to forward such communication to its destination." Our EINSTEIN 2.0 Opinion concluded that EINSTEIN 2.0 would not unlawfully "divulge" the contents of Internet communications within the meaning of section 2511(3), both because the participating agency and its employees would have manifested consent to the scanning, and "because the federal government is 'authorized,' and its 'facilities are used, to forward such communications to [their] destination.'" 33 Op. O.L.C. at 96. With respect to individual federal employees, we further noted that Internet communications cannot reach employees at work without routing through the government's computer systems. *Id*. Thus, even if section 705 is not read by terms to incorporate this exception, we find it significant that the exception we conclude section 705 adopts is hardly a novel one in this area. We are also not aware of any legislative history that indicates a congressional intention to preclude recognition of such an exception here.

II.

We believe the EINSTEIN 2.0 system would also comply with the provision of the Stored Communications Act ("SCA"), codified at 18 U.S.C. § 2702(a)(3), that provides that "a provider of remote computing service

or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by [section 2702(a)(1) or (a)(2)]) to any governmental entity." Insofar as the EINSTEIN 2.0 system examines, in real time, Internet traffic-flow data that is not retained by the ISP, there may be grounds to assert that this provision is simply inapplicable, because the data in question is not a "record or other information" within the possession of the ISP. Even assuming, however, that section 2702(a)(3) by its terms may apply to EINSTEIN 2.0, we believe that the statutory exception permitting disclosure based on "the lawful consent of the customer or subscriber" would apply. 18 U.S.C. § 2702(c)(1)(C) (2006). That is because we believe that in this context the government, and no other party, should be understood as the "customer or subscriber" of the ISP for purposes of this exception. On this view, even assuming that non-content information obtained from or with the assistance of the ISP regarding Internet traffic that passed onto or off of the government's system would qualify as "record[s] or other information" under the SCA, these "record[s] or other information" would "pertain[] to" the government as a "subscriber to or customer of [the ISP's] service," and the government could therefore provide "lawful consent" to divulge this information. 18 U.S.C. § 2702(c)(2).

This construction of the statute fits naturally with the plain text: insofar as a government agency has contracted with an ISP for Internet service, the government is indisputably a "customer" (if not also a subscriber) of the ISP. In accordance with this view, the Ninth Circuit has characterized a municipality as a "subscriber" of a text-messaging service where the municipality contracted with the service to provide two-way text pagers to police officers and other municipal employees. *See Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 895, 903 (9th Cir. 2008).

Insofar as end users such as individual employees hold a protected privacy interest in non-content information, the employer's consent to disclosure might violate some legal obligation of the employer, but it would not create liability for the ISP under the SCA, since the ISP had obtained the necessary consent of its "customer or subscriber." In any event, in our case, the individual employees have also consented to the disclosure, so disclosure should not violate any SCA-protected interest of theirs (even if they are also somehow "customers or subscribers" of the ISP). Nor

does there appear to be any Fourth Amendment issue with the disclosure. Not only have the employees here consented to the disclosure, but courts have generally concluded that there is no reasonable expectation of privacy in non-content information provided to an ISP. *See, e.g.*, *United States v. Perrine*, 518 F.3d 1196, 1204–05 (10th Cir. 2008) (collecting cases); *Freedman v. America Online, Inc.*, 412 F. Supp. 2d 174, 181–82 (D. Conn. 2005).

We recognize the concern that non-content information pertaining to one customer or subscriber (such as the government in our case) could include information pertaining to other customers or subscribers of the ISP insofar as those other parties have sent or received traffic from the first customers/subscriber's computers. But we do not believe the SCA should be read to require separate consent from both customers/subscribers in that circumstance. Such records or information "pertain" to the customer/subscriber providing consent, even if they reveal information about other customers/subscribers too, so under the plain text of the statute one-party consent seems sufficient for disclosure. Indeed, any other interpretation would yield the odd result that a customer's ability to consent to disclosure of its information would depend on whether other parties it telephoned or emailed happened to be customers of the same provider. Also, unlike content information, which relates to discrete messages each with a particular sender and particular recipients, the "record or other information" covered by section 2702(a)(3) often involves an aggregation of data—the total record of a customer/subscriber's Internet traffic or phone calls, for example—that is unique to the individual customer/subscriber and for which (as a result) no other party could provide meaningful consent. Information regarding other customers/subscribers who have not provided consent could of course be disclosed under this analysis only to the extent that such information is contained in a "record or other information" pertaining to the customer or subscriber who has provided lawful consent (here, the government).

Furthermore, the SCA's consent exception for content information expressly allows one-party consent—either the "originator" or the "addressee" or "intended recipient" of the communication may authorize disclosure of its contents, 18 U.S.C. § 2702(b)(3)—and it would be anomalous if the provisions on non-content information, which are generally less restrictive, imposed a more stringent consent requirement than those for content information. *Cf. In re American Airlines, Inc. Privacy Litig.*, 370

F. Supp. 2d 552, 561 (N.D. Tex. 2005) (construing statute to allow any intended recipient of a communication to authorize disclosure of content information). Congress appears to have adopted the current SCA provisions on non-content information in part to bring those provisions more in line with provisions on content information. Before 2001, the SCA provided only that a provider could disclose "a record or other information pertaining to a subscriber to or customer of [the provider's] service (not including [content information]) to any person other than a governmental entity" and that the provider generally could disclose such records or information to a governmental entity "only when the governmental entity . . . ha[d] the consent of the subscriber or customer to such disclosure" or satisfied one of several other enumerated exceptions. *See* 18 U.S.C. § 2703(c) (2000); Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1860 (1986). Congress amended the statute to provide that, even without an affirmative government request, the provider may disclose records and information covered by section 2702(a)(3) "with the lawful consent of the customer or subscriber" or in certain other specified circumstances. *See* 18 U.S.C. § 2702(c)(2) (Supp. I 2001); Pub. L. No. 107-56, § 212(a)(1)(E), 115 Stat. 272, 284 (2001). As explained in the legislative history, Congress intended this change "to allow communications providers to disclose non-content information (such as the subscriber's login records)." H.R. Rep. No. 107-236, pt. 1, at 58 (2001). Under pre-2001 law, the House Judiciary Committee explained, "the communications provider [was] expressly permitted to disclose content information but not expressly permitted to provide non-content information. This change would cure this problem and would permit the disclosure of the less-protected information, parallel to the disclosure of the more protected information." *Id.*; *see also* 147 Cong. Rec. 19,001, 19,009 (statement of Sen. Leahy) (discussing 2001 amendments and observing that "the right to disclose the content of communications necessarily implies the less intrusive ability to disclose non-content records"). In addition, although we are aware of little relevant legislative history bearing directly on the meaning of "consent" in section 2702(a)(3), the legislative history of the SCA as originally enacted suggests that Congress understood background legal principles to allow one-party consent, which arguably supports construing consent provisions of the statute in accordance with that understanding. *See* S. Rep. No. 99-541, at 3 (1986) (observing that "because [information on remote computer systems] is subject to control by a third party computer operator, the

information may be subject to no constitutional privacy protection" (citing *United States v. Miller*, 425 U.S. 435 (1976))).

III.

Finally, we do not believe the EINSTEIN 2.0 program impermissibly infringes state wiretapping and communication privacy laws. *See, e.g.*, Fla. Stat. Ann. § 934.03(3)(d) (West 2009); 18 Pa. Cons. Stat. Ann. § 5704(4) (West Supp. 2009); Md. Code Ann., Cts. & Jud. Proc. § 10-402(c)(3) (Lexis Nexis 2009); Cal. Penal Code § 631(a) (West 1999). To the extent that such laws purported to apply to the conduct of federal agencies and agents conducting authorized EINSTEIN 2.0 operations and imposed requirements that exceeded those imposed by the federal statutes discussed above and in our EINSTEIN 2.0 Opinion, they would "stand[] as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress," and be unenforceable under the Supremacy Clause. *Hines v. Davidowitz*, 312 U.S. 52, 67 (1941); *see also Geier v. Am. Honda Motor Co.*, 529 U.S. 861, 873 (2000); *Old Dominion Branch v. Austin*, 418 U.S. 264 (1974); *Bansal v. Russ*, 513 F. Supp. 2d 264, 283 (E.D. Pa. 2007) (concluding that "federal officers participating in a federal investigation are not required to follow" state wiretapping law containing additional requirements not present in the federal Wiretap Act, because in such circumstances, "the state law would stand as an obstacle to federal law enforcement"); *Johnson v. Maryland*, 254 U.S. 51 (1920); *cf. United States v. Adams*, 694 F.2d 200, 201 (9th Cir. 1982) ("evidence obtained from a consensual wiretap conforming to 18 U.S.C. § 2511(2)(c) is admissible in federal court proceedings without regard to state law").

DAVID J. BARRON
Acting Assistant Attorney General
Office of Legal Counsel