Use of the EINSTEIN 2.0 Intrusion-Detection System to Protect Unclassified Computer Networks in the Executive Branch

An intrusion-detection system known as EINSTEIN 2.0 used to protect civilian unclassified networks in the Executive Branch against malicious network activity complies with the Fourth Amendment to the Constitution, the Wiretap Act, the Foreign Intelligence Surveillance Act, the Stored Communications Act, and the pen-register and trap-and-trace provisions of 18 U.S.C. § 3121 *et seq*., provided that certain log-on banners or computer-user agreements are consistently adopted, implemented, and enforced by executive departments and agencies using the system.

January 9, 2009

MEMORANDUM OPINION FOR THE COUNSEL TO THE PRESIDENT

As part of the Comprehensive National Cybersecurity Initiative, the Department of Homeland Security ("DHS"), in coordination with the Office of Management and Budget, is in the process of establishing an intrusion-detection system known as EINSTEIN 2.0 in order to detect unauthorized network intrusions and data exploitations against the Executive Branch's civilian unclassified computer systems ("Federal Systems").[1] In January 2007, you asked this Office to undertake a legal review of proposed EINSTEIN 2.0 operations; since that time we have provided ongoing informal advice regarding the legality of those operations, which are now underway. This memorandum formalizes the informal advice we have provided regarding whether EINSTEIN 2.0 operations comply with the Fourth Amendment to the Constitution of the United States, title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Pub. L. No. 90-351, 82 Stat. 197, 211, *codified as amended at* 18 U.S.C. § 2510 *et seq*. ("Wiretap Act")); the Foreign Intelligence Surveillance Act of 1978 (Pub. L. No. 95-511, 92 Stat. 1783, *codified as amended at* 50 U.S.C. § 1801 *et seq*. ("FISA")); the Stored Communications Act (18 U.S.C. § 2701 *et seq*. ("SCA")); and the pen-register and trap-and-trace provisions of 18 U.S.C. § 3121 *et seq*. ("Pen/Trap Act").

[1] As used this memorandum, the term "Federal Systems" includes all Executive Branch federal government information systems except for National Security Systems of executive departments and agencies and Department of Defense information systems.

We examine these legal issues in the context of an executive department's or agency's use of a model computer log-on banner or a model computer-user agreement developed by lawyers from the Department of Justice ("DOJ"), DHS, and other departments and agencies with expertise in cybersecurity issues. We conclude that as long as executive departments and agencies participating in EINSTEIN 2.0 operations consistently adopt, implement, and enforce the model log-on banner or computer-user agreement—or log-on banners or computer-user agreements with terms that are substantially equivalent to those models—the use of EINSTEIN 2.0 technology to detect computer network intrusions and exploitations against Federal Systems complies with the Fourth Amendment, the Wiretap Act, FISA, the SCA, and the Pen/Trap Act.

I.

Over the past several years, Federal Systems have been subject to sophisticated and well-coordinated computer network intrusions and exploitations on an unprecedented scale. The Intelligence Community has determined that those malicious network activities pose a grave threat to national security. *See also* Center for Strategic and International Studies, *Securing Cyberspace* 11–15 (2008) (discussing national security implications of federal network vulnerabilities). Those malicious network activities occur at the hands of hostile foreign nations (including foreign intelligence services), transnational criminal groups and enterprises, and individual computer hackers. Recent intrusions and exploitations have resulted in the theft of significant amounts of unclassified data from many executive departments and agencies, as well as information regarding the vulnerabilities of Federal Systems. The unclassified networks of the Departments of Defense, State, Homeland Security, and Commerce, among others, have suffered intrusions against their networks and exploitations of their data. Accordingly, the Homeland Security Council has determined that the deployment of a multi-layered network defense system is necessary to protect Federal Systems against these ongoing computer intrusions and exploitations carried out by a broad array of cyber adversaries.

The first layer of this network-defense system is known as EINSTEIN 1.0 and already is in place across segments of several Executive Branch agencies. EINSTEIN 1.0 is a semi-automated process for detecting—albeit after the fact—inappropriate or unauthorized inbound and outbound

network traffic between participating departments and agencies and the Internet. The United States Computer Emergency Readiness Team ("US-CERT"), an organizational component of DHS, administers EINSTEIN 1.0.

EINSTEIN 1.0 analyzes only "packet header" information—and not packet "payload" (content) information—for inbound and outbound Internet traffic of participating agencies.[2] The header information collected by EINSTEIN 1.0 technology includes: the source and destination IP addresses for the packet, the size of the data packet, the specific Internet protocol used (for e-mail, the Simple Mail Transfer Protocol and, for use of the World Wide Web, the Hypertext Transport Protocol), and the date and time of transmission of the packet (known as "the date/time stamp"). EINSTEIN 1.0 collects this information only after packets already have been sent or received by a user and, thus, does not provide real-time information regarding network intrusions and exploitations against Federal Systems. US-CERT analysts examine the header information to identify suspicious inbound and outbound Internet traffic, particularly network backdoors and intrusions, network scanning activities, and computer network exploitations using viruses, worms, spyware, bots, Trojan horses, and other "malware."

EINSTEIN 1.0 contains several limitations. First, it does not provide real-time reporting regarding intrusions and exploitations against Federal Systems. Second, it does not cover all Federal Systems, and, therefore, does not provide complete awareness regarding malicious network activity directed against those systems. Third, because EINSTEIN 1.0 does not scan packet content, it does not offer complete intrusion and exploitation detection functionality.

---

[2] The Internet consists of millions of computers connected by a network of fiber-optic cables and other data-transmission facilities. Data transmitted across the Internet are broken down into "packets" that are sent out from one computer to another. Each packet is directed (routed) to its intended source from its respective destination by an Internet Protocol address ("IP address"). An IP address is a unique numerical address, akin to a phone number or physical address, identifying each computer on the Internet. Each packet may follow a different route to its ultimate IP address destination, traveling over the networks of several different Internet backbone providers and Internet Service Providers ("ISPs") before arriving at the destination. Upon arrival at the destination, the packets are reconstituted. *See generally* Jonathan E. Nuechterlein & Philip J. Weiser, *Digital Crossroads* 121–28 (2005).

We understand that many executive departments and agencies supplement EINSTEIN 1.0 with their own intrusion-detection systems, which are designed to identify network intrusions and exploitations conducted against their own computer systems. In addition, individual departments and agencies also operate their own network filters to block certain unauthorized content, such as Internet pornography and file-sharing activities, among others. We understand, however, that there is little or no coordination or communication among Executive Branch entities conducting these individualized network defense activities. Accordingly, multiple departments facing the same intrusion or exploitation might have no idea that they are all facing a coordinated malicious network operation. Nor would departments or agencies that have not yet been subject to the intrusion or exploitation have advanced warning of the activity, such that they could upgrade their defenses. Hence, the lack of cybersecurity collaboration within the Executive Branch leads to inefficient network defensive measures that contribute to the ongoing vulnerability of Federal Systems.

To rectify this situation, DHS, in conjunction with OMB, is deploying throughout the Executive Branch an intrusion-detection system known as EINSTEIN 2.0 to provide greater coordination and situational awareness regarding malicious network activities directed against Federal Systems. EINSTEIN 2.0 is a robust system that is expected to overcome the technical limitations of EINSTEIN 1.0. EINSTEIN 2.0 technology is comprised of computers ("sensors") configured with commercial "off-the-shelf" intrusion-detection software as well as government-developed software. That technology will be located at certain Internet access points known as Trusted Internet Connections ("TICs"), which connect Federal Systems to the Internet.

EINSTEIN 2.0 intrusion-detection sensors will observe in near-real time the packet header and packet content of all incoming and outgoing Internet traffic of Federal Systems ("Federal Systems Internet Traffic") for the "signatures" of malicious computer code used to gain access to or to exploit Federal Systems.[3] *See generally* NIST Special Publication No.

[3] By the term "malicious computer code," we mean not only "malware," such as viruses, spyware, and Trojan horses, but also malicious network intrusion and exploitation activities, such as identifying network backdoors and network scanning activities, and so-called "social engineering" activities, such as "phishing" exploits that seek usernames, passwords, social security numbers, or other personal information.

800-94 (2007) (discussing signature-based detection techniques). Because Internet traffic is IP address-based, we understand that only Federal Systems Internet Traffic destined to or sent from an IP address associated with an executive department or agency participating in EINSTEIN 2.0 ("EINSTEIN 2.0 Participant") would be scanned by EINSTEIN 2.0 technology. Thus, EINSTEIN 2.0 technology will scan only the Federal Systems Internet Traffic for EINSTEIN 2.0 Participants that connect to the Internet at TICs.

DHS has the responsibility for determining which signatures to program into the EINSTEIN 2.0 sensors, pursuant to procedures developed by DHS. Signatures may be derived from several sources, including commercial computer security services, publicly available computer security information, privately reported incidents to US-CERT, in-depth analysis by US-CERT analysts, and other federal partners involved in computer defense. We understand that from information obtained through these sources, DHS will create signatures based upon known malicious computer code to guide the operations of EINSTEIN 2.0 sensors.

EINSTEIN 2.0 sensors will not scan actual Federal Systems Internet Traffic for malicious computer code as that traffic is in transmission, but instead will scan a temporary copy of that traffic created solely for the purpose of scanning by the sensors. The "original" Federal Systems Internet Traffic will continue to its destination without being scanned by EINSTEIN 2.0 sensors; thus, EINSTEIN 2.0 operations will not disrupt the normal operations of Federal Systems. But EINSTEIN 2.0 technology will create a temporary mirror image of all Federal Systems Internet Traffic of EINSTEIN 2.0 Participants for parallel scanning by the sensors. The temporary copy of Federal Systems Internet Traffic is created only for identifying known signatures. When EINSTEIN 2.0 sensors identify Federal Systems Internet Traffic containing packets with malicious computer code matching a signature, EINSTEIN 2.0 technology is designed to generate—in near-real time—an automated alert about the detected signature. The alert generally will not contain the content of the packet, but will include header information, such as the source or remote IP address associated with the traffic that generated the alert, metadata regarding the type of signature that was detected, and the date/time stamp.

In addition to generating automated alerts, EINSTEIN 2.0 operations will both acquire and store data packets from the mirror copy of Federal

Systems Internet Traffic that are associated with a detected signature. Those packets, which may include the full content of Internet communications, such as e-mails, may be reviewed by analysts from US-CERT and other authorized persons involved in computer network defense. We understand that no packets other than those associated with a known signature will be acquired and stored. Accordingly, we understand that the vast majority of packets that are not associated with malicious computer code matching a signature will be deleted promptly. *See* DHS, *Privacy Impact Assessment for EINSTEIN 2*, at 12 (May 18, 2008) (stating that all "clean traffic" is promptly deleted).

We have been informed that EINSTEIN 2.0 operations are expected to improve substantially the government's ability to defend Federal Systems against intrusions and exploitations. EINSTEIN 2.0 operations will supplement—and not replace—the current individualized computer network security defenses of executive departments and agencies with a centralized and coordinated network defense system operated by DHS. That centralization and coordination of information regarding all Federal Systems Internet Traffic is expected to facilitate real-time situational awareness regarding malicious network activity across all Federal Systems. Improved situational awareness in turn will facilitate improved defensive measures, such as minimizing network vulnerabilities and alerting users of Federal Systems about particular malicious computer code detected against particular EINSTEIN 2.0 Participants. By sharing information throughout the Executive Branch regarding signatures detected in Federal Systems Internet Traffic, EINSTEIN 2.0 operations should facilitate improved defenses against known malicious computer code.

As part of enrolling in EINSTEIN 2.0 operations, each EINSTEIN 2.0 Participant is required to enter into a memorandum of agreement ("MOA") with DHS. We understand that the MOA will require an EINSTEIN 2.0 Participant to certify that it has implemented procedures to provide appropriate notice to its employees that by using government-owned information systems, the employee acknowledges and consents to the monitoring, interception, and search of his communications transiting through or stored on those systems, and that the employee has no reasonable expectation of privacy in his use of those systems.[4] Those procedures

[4] Throughout this memorandum we refer to "Executive Branch employees" and to the "employees" of EINSTEIN 2.0 Participants. By using the word "employees," we do not

are to include computer-user agreements, log-on banners, and computer-training programs. We understand that DHS must receive that certification from each EINSTEIN 2.0 Participant before any of the Participant's Federal Systems Internet Traffic can be scanned by EINSTEIN 2.0 technology.

EINSTEIN 2.0 Participants will not be required to use a specific banner or user agreement. We have been advised that given the diversity of missions and organizations among departments and agencies within the Executive Branch and the varying technical constraints faced by those entities, there simply is no one-size-fits-all solution for providing notice to and obtaining the consent of employees for EINSTEIN 2.0 operations. We have been informed, however, that the MOA will include model log-on banner and model computer-user agreement language for EINSTEIN 2.0 Participants to consider in crafting their own banners and user agreements. The model language, which was developed by lawyers from DOJ with the input and advice of lawyers from DHS and other interested departments and agencies, is as follows:

- You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.
- Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.
- By using this information system, you understand and consent to the following:
  - You have no reasonable expectation of privacy regarding communications or data transiting or stored on this information system.

---

mean to limit the requirement to provide appropriate notice and consent to only those persons in a common law employment relationship with the federal government. Rather, the term "employees" in this memorandum should be understood to include "employees" as well as "officers," "contractors," and "agents" of EINSTEIN 2.0 Participants.

- At any time, and for any lawful government purpose, the Government may monitor, intercept, and search any communication or data transiting or stored on this information system.
- Any communications or data transiting or stored on this information system may be disclosed or used for any lawful government purpose.

[click button: I AGREE]

The model computer-user agreement language contains the same substantive terms as the model log-on banner, except that it requires a computer user to sign a document indicating that the user "understand[s] and consent[s]" to the foregoing terms. Although we understand that EINSTEIN 2.0 Participants will not be required to use the exact model log-on banner and model computer-user agreement language, each EINSTEIN 2.0 Participant must certify that its log-on banners, computer-user agreements, and other computer policies contain language that demonstrates consent is "clearly given" and "clearly obtained" before EINSTEIN 2.0 becomes operational for the Participant's Federal Systems Internet Traffic.[5]

DOJ has advised that with the consistent adoption, implementation, and enforcement of appropriate consent and notification procedures, EINSTEIN 2.0 operations would comply with the Fourth Amendment to the Constitution of the United States, the Wiretap Act, FISA, the SCA,

[5] For example, DOJ already has in place a log-on banner that we believe would satisfy the MOA's certification criteria. DOJ's banner at present provides:

- You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.
- Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.
- By using this information system, you understand and consent to the following:
  - You have no reasonable expectation of privacy regarding any communications transmitted through or data stored on this information system.
  - At any time, the Government may monitor, intercept, search and/or seize data transiting or stored on this information system.
  - Any communications transmitted through or data stored on this information system may be disclosed or used for any U.S. Government-authorized purpose.

[click button: I AGREE]

and the Pen/Trap Act. The Department arrived at these conclusions after a lengthy review by the Office of the Deputy Attorney General, this Office, and, with respect to the statutes for which they have expertise, the National Security Division and the Computer Crimes and Intellectual Property Section of the Criminal Division. This memorandum explains the reasoning for those conclusions.

II.

We first explain the reasoning behind DOJ's conclusion that the deployment, testing, and use of EINSTEIN 2.0 technology complies with the Fourth Amendment where each EINSTEIN 2.0 Participant consistently adopts and implements the model log-on banner or model computer-user agreement—or a log-on banner or computer-user agreement containing substantially equivalent terms establishing that the consent of its employees is "clearly given" and "clearly obtained."

A.

The Fourth Amendment provides in relevant part: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause . . . ." U.S. Const. amend. IV. Government activity implicates the protections of the Fourth Amendment where it constitutes a "search" or a "seizure" within the meaning of the Fourth Amendment. The Supreme Court has said that a "search" occurs where the government infringes upon a person's legitimate expectation of privacy, consisting of both an actual, subjective expectation of privacy as well as an objectively reasonable expectation of privacy—"*i.e.*, one that has a source outside the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society." *Minnesota v. Carter*, 525 U.S. 83, 88 (1998) (internal quotation marks omitted).

We think it plain that computer users exchanging Internet communications through Federal Systems lack a legitimate expectation of privacy in certain specific categories of data that will be subject to scanning by EINSTEIN 2.0 technology. There is no objectively reasonable expectation of privacy in information regarding the to/from addresses for e-mails, the IP addresses of websites visited, the total traffic volume of the user, and

other addressing and routing information conveyed for the purpose of transmitting Internet communications to or from a user. *See Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 904–05 (9th Cir. 2008); *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008); *see also Smith v. Maryland*, 442 U.S. 735, 743–44 (1979) (no legitimate expectation of privacy in dialing, routing, addressing, and signaling information transmitted to telephone companies). E-mail addresses and IP addresses provide addressing and routing information to an Internet Service Provider ("ISP") in the same manner as a telephone number provides switching information to a telephone company. *Forrester*, 512 F.3d at 510. Just as a telephone user has no objectively reasonable expectation of privacy in telephone numbers voluntarily turned over to the phone company to enable switching of a phone call, an Internet user has no such expectation of privacy in routing information submitted to an ISP in order to deliver an Internet communication. *Id.* That routing information also is akin to the addressing information written on the outside of a first-class letter, which also is not constitutionally protected. *Id.* at 511 ("E-mail, like physical mail, has an outside address 'visible' to the third-party carriers that transmit it to its intended location."). With respect to information regarding the total volume of data received and transmitted by an Internet user, that information is no different from the information produced by a pen register regarding the number of incoming and outgoing calls at a particular phone number; and the Supreme Court has long held that an individual has no legitimate expectation of privacy in such information, which already has been exposed to a telecommunications carrier for the purpose of routing a communication. *Id.* Therefore, because there is no legitimate expectation of privacy with respect to the foregoing information transmitted for the purpose of routing Internet communications, the scanning of that information by EINSTEIN 2.0 technology does not constitute a "search" subject to the restrictions of the Fourth Amendment.

With respect to a user's expectation of privacy in the content of an Internet communication (such as an e-mail), we assume for the purposes of this memorandum that a computer user generally has a legitimate expectation of privacy in that content while it is in transmission over the Internet. To date, the federal courts appear to agree that the sender of an e-mail, like the sender of a letter via first-class mail, has an objectively reasonable expectation of privacy in the content of a message while it is in transmission. *See, e.g.*, *United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir.

2004) (analogizing expectation of e-mail user in privacy of e-mail to expectation of individuals communicating by regular mail); *United States v. Maxwell*, 45 M.J. 406, 418 (C.A.A.F. 1996) (sender of an e-mail generally "enjoys a reasonable expectation that police officials will not intercept the transmission without probable cause and a search warrant"); *see also Quon*, 529 F.3d at 905 ("[U]sers do have a reasonable expectation of privacy in the content of their text messages vis-à-vis the service provider.").[6]

Here, EINSTEIN 2.0 technology will scan a mirror copy of the packet content of Federal Systems Internet Traffic—including packets that are part of e-mails—for malicious computer code associated with a signature while the e-mail is in transmission, and, thus, while a sender of the e-mail, we assume, generally retains an expectation of privacy in the content of that communication. Hence, the precise question for us is whether the Executive Branch's automatic scanning of Federal Systems Internet Traffic for malicious computer code would implicate a computer user's legitimate expectation of privacy in the content of his Internet communications. We consider the privacy expectations of two groups of computer users: (1) Executive Branch employees and (2) private individuals communicating with specific Executive Branch employees or with Executive Branch departments or agencies more generally.

---

[6] It also appears that the federal courts agree that, again like the sender of a first-class letter, an individual has a "diminished" expectation of privacy in the content of an e-mail that "ha[s] already arrived at the recipient." *Lifshitz*, 369 F.3d at 190 (internal citations omitted); *see Guest v. Leis*, 225 F.3d 325, 333 (6th Cir. 2001) (individual does not have a reasonable expectation of privacy "in an e-mail that had already reached its recipient; at this moment, the e-mailer would be analogous to a letter-writer, whose expectation of privacy ordinarily terminates upon delivery of the letter"); *Maxwell*, 45 M.J. at 417 (once an e-mail, like a letter, "is received and opened, the destiny of the [e-mail] then lies in the control of the recipient . . . , not the sender"); *United States v. Jones*, No. 03-15131, 149 F. Appx. 954, 959 (11th Cir. Sept. 20, 2005) (unpublished) ("We have not addressed previously the existence of a legitimate expectation of privacy in text messages or e-mails. Those circuits that have addressed the question have compared e-mails with letters sent by postal mail. Although letters are protected by the Fourth Amendment, 'if a letter is sent to another, the sender's expectation of privacy ordinarily terminates upon delivery.'" (quoting *United States v. King*, 55 F.3d 1193, 1195–96 (6th Cir. 1995)).

1.

We first address the expectations of Executive Branch employees. The Supreme Court has rejected the contention that public employees "can never have a reasonable expectation of privacy in their place of work." *O'Connor v. Ortega*, 480 U.S. 709, 717 (1987) (plurality); *id.* at 729–31 (Scalia, J., concurring). "Individuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer." *Id.* at 717 (plurality). Nevertheless, there are reasons to doubt that an Executive Branch employee has a legitimate expectation of privacy in the content of his Internet communications made using government-owned information systems. The text of the Fourth Amendment protects the right of the people to be secure only in "*their* persons, houses, papers, and effects." U.S. Const. amend. IV (emphasis added). Although an individual generally possesses a legitimate expectation of privacy in his own personal computer, *e.g.*, *United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007); *Lifshitz*, 369 F.3d at 190, it is less clear that an Executive Branch employee has a legitimate expectation of privacy in Internet communications he makes using a computer that is the property of the United States government, provided by the taxpayers for his use at work. *Cf. Muick v. Glenayre Elecs.*, 280 F.3d 741, 743 (7th Cir. 2002) (Posner, J.) (employee "had no right of privacy in the computer that [his private employer] had lent him for use in the workplace"); *but cf. United States v. Slanina*, 283 F.3d 670, 677 (5th Cir. 2002) (employee had reasonable expectation of privacy in use of city-owned computer where there was no "city policy placing Slanina on notice that his computer usage would be monitored" and there was no "indication that other employees had routine access to his computer"), *vacated on other grounds*, 537 U.S. 802 (2002). A government employee lacks an ownership or other property interest in the computer he uses at work; and he especially lacks any such interests in the Federal Systems—the network infrastructure that the government provides to enable its employees to access the Internet—that, unlike his personal computer, ordinarily is not within his day to day control.

As a general matter, however, the Supreme Court has held that there may be circumstances in which a government employee has a legitimate expectation of privacy in the contents of governmental property that the employee uses or controls at work, such as an office or a locked desk

drawer. *See O'Connor*, 480 U.S. at 716–19 (1987) (plurality opinion) (public employee has a reasonable expectation of privacy in personal items, papers, and effects in office, desk, and file cabinets provided by public employer); *id*. at 730–31 (Scalia, J., concurring) (government employee has a legitimate expectation of privacy in the contents of his office). And the Court also has made it clear that property interests are not conclusive regarding the legitimacy of an individual's expectation of privacy. *See Oliver v. United States*, 466 U.S. 170, 183 (1984) ("The existence of a property right is but one element in determining whether expectations of privacy are legitimate."); *Warden v. Hayden*, 387 U.S. 294, 304 (1967) ("The premise that property interests control the right of the Government to search and seize has been discredited."); *see also Legality of Television Surveillance in Government Offices*, 3 Op. O.L.C. 64, 66–67 (1979) (government ownership of office insufficient to establish employee's lack of expectation of privacy where "in a practical sense" the employee exercises exclusive use of the office) ("*Television Surveillance*"); *but cf. United States v. Ziegler*, 474 F.3d 1184, 1191 (9th Cir. 2007) (private employee's "workplace computer . . . is quite different from the" property described in *O'Connor*, because the computer was owned by the company, was controlled jointly by the company and the employee, and was monitored to ensure that employees did not visit pornographic or other inappropriate websites).

Instead, whether, in a particular circumstance, a government employee has a legitimate expectation of privacy in his use of governmental property at work is determined by "[t]he operational realities of the workplace" and "by virtue of actual office practices and procedures, or by legitimate regulation." *O'Connor*, 480 U.S. at 717 (plurality); *see United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000) ("[O]ffice practices, procedures, or regulations may reduce legitimate privacy expectations."). Here, we believe that an Executive Branch employee will not have a legitimate expectation of privacy in the content of his Internet communications transmitted over government-owned information systems, provided that EINSTEIN 2.0 Participants consistently adopt, implement, and enforce appropriate consent and notification procedures, such as the model log-on banner or model computer-user agreement.

Although the Supreme Court has not addressed the issue, the federal courts of appeals have held that the use of log-on banners or computer-user agreements, such as the models provided by DHS to EINSTEIN 2.0

Participants, can eliminate any legitimate expectation of privacy in the content of Internet communications made at work using government-owned information systems. For example, in *Simons*, the computer-use policy at the Foreign Bureau of Information Services ("FBIS"), a division of the Central Intelligence Agency, expressly noted that FBIS would "'audit, inspect, and/or monitor'" employees' use of the Internet, "including all file transfers, all websites visited, and all e-mail messages, 'as deemed appropriate.'" 206 F.3d at 398 (quoting policy). The Fourth Circuit held that this policy "placed employees on notice that they could not reasonably expect that their Internet activity would be private" and that, "in light of the Internet policy, Simons lacked a legitimate expectation of privacy" in his use of the Internet at work. *Id*.

Likewise, in *United States v. Angevine*, 281 F.3d 1130 (10th Cir. 2002), the Tenth Circuit held that a professor at a state university had no reasonable expectation of privacy in his Internet use in light of a broadly worded computer-use policy and log-on banner. The computer-use policy stated that the university "'reserves the right to view or scan any file or software stored on the computer or passing through the network, and will do so periodically'" and has "'a right of access to the contents of stored computing information at any time for any purpose which it has a legitimate need to know.'" *Id*. at 1133 (quoting policy). The log-on banner provided that "'all electronic mail messages . . . contain no right of privacy or confidentiality except where Oklahoma or Federal statutes expressly provide for such status,'" and that the university may "'inspect electronic mail usage by any person at any time without prior notice as deemed necessary to protect business-related concerns . . . to the full extent not expressly prohibited by applicable statutes.'" *Id*. (quoting banner). The court held that these notices prevent university employees "from reasonably expecting privacy in data downloaded from the Internet onto [u]niversity computers," because users are warned that data "is not confidential either in transit or in storage" and that "network administrators and others were free to view data downloaded from the Internet." *Id*. at 1134.

The Eighth Circuit came to the same conclusion in *United States v. Thorn*, 375 F.3d 679 (8th Cir. 2004), *vacated on other grounds*, 543 U.S. 1112 (2005). In *Thorn*, a state employee had acknowledged in writing a computer-use policy, which warned that employees "'*do not* have any personal privacy rights regarding their use of [the agency's] information

systems and technology. An employee's use of [the agency's] information systems and technology indicates that the employee understands and consents to [the agency's] right to inspect and audit all such use as described in this policy.'" *Id*. at 682 (quoting policy). As a result of this policy, the court held that the state employee "did not have any legitimate expectation of privacy with respect to the use and contents of his [work] computer," because under the agency's policy, employees have "no personal right of privacy with respect to their use of the agency's computers" and provides the state with a "right to access all of the agency's computers." *Id*. at 683.

The decisions of other federal courts that have addressed the issue support the proposition that actual and consistent use of log-on banners or computer-user agreements can eliminate any legitimate expectation of an employee in the privacy with respect to his Internet communications using government-owned information systems. *See Biby v. Bd. of Regents*, 419 F.3d 845, 850–51 (8th Cir. 2005) (university computer policy warning user "not to expect privacy if the university has a legitimate reason to conduct a search" and that "computer files, including e-mail, can be searched" under certain conditions eliminates any reasonable expectation of privacy the use of the computer network); *Muick*, 280 F.3d at 743 (employer's announced policy of inspecting work computers "destroyed any reasonable expectation of privacy"); *United States v. Monroe*, 52 M.J. 326, 330 (C.A.A.F. 1999) (no reasonable expectation of privacy that network administrators would not review e-mail where banner stated that "users logging on to this system consent to monitoring"); *see also Heckenkamp*, 482 F.3d at 1147 ("[P]rivacy expectations may be reduced if the user is advised that information transmitted through the network is not confidential and that the systems administrators may monitor communications transmitted by the user.") (citing *Angevine*, 281 F.3d at 1134, and *Simons*, 206 F.3d at 398); *cf. Slanina*, 283 F.3d at 677 ("[G]iven the absence of a city policy placing Slanina on notice that his computer usage would be monitored and the lack of any indication that other employees had routine access to his computer, we hold that Slanina's expectation of privacy was reasonable."); *Leventhal v. Knapek*, 266 F.3d 64, 73–74 (2d Cir. 2001) (public employee had reasonable expectation of privacy in the contents of his office computer because his employer neither "had a general practice of routinely conducting searches of office computers" nor

"had placed [him] on notice that he should have no expectation of privacy in the contents of his office computer").

In light of these decisions, we believe that an Executive Branch employee who has clicked through the model log-on banner or signed the model computer-user agreement—or a log-on banner or computer-user agreement containing substantially equivalent terms—would not have a legitimate expectation of privacy in the contents of Internet communications made using government-owned information systems and transmitted over Federal Systems. The model log-on banner is explicit and comprehensive regarding an employee's lack of a legitimate expectation of privacy in his use of government-owned information systems. That banner states that the information system the employee uses is the property of the government and "is provided for U.S. Government-authorized use only." The user "understand[s] and consent[s]" that: he has "no reasonable expectation of privacy regarding communications or data transiting or stored" on that information system; "[a]t any time, and for any lawful government purpose, the Government may monitor, intercept, and search any communication or data transiting or stored" on the information system; and any communications transmitted through or data stored on the information system "may be disclosed or used for any lawful government purpose." *See supra* pp. 69–70. We believe that the current DOJ banner, which deviates from the model log-on banner and the model computer-user agreement language in some respects, is to the same effect. *See supra* note 5. Both the model log-on banner and computer-user agreement and the current DOJ log-on banner are at least as robust as—and we think they are even stronger than—the materials that eliminated an employee's legitimate expectation of privacy in the content of Internet communications in *Simons*, *Angevine*, *Thorn*, *Biby*, and *Monroe*. Therefore, we believe that adoption of the language in those model materials by EINSTEIN 2.0 Participants would eliminate their employees' legitimate expectations of privacy in their uses of government-owned information systems with respect to the lawful government purpose of protecting Federal Systems against network intrusions and exploitations.

It is important to note, however, that the use of log-on banners or computer-user agreements may not be sufficient to eliminate an employee's legitimate expectation of privacy if the statements and actions of Executive Branch officials contradict these materials. Recently, in *Quon v. Arch Wireless Operating Company*, the Ninth Circuit held that a police officer

had a legitimate expectation of privacy in the contents of text messages sent and received on his department-provided pager notwithstanding departmental policies, because informal guidance from the officer's superiors had established, in practice, that the department would not monitor the content of his text messages. 529 F.3d at 906–07. Thus, the "operational reality" at the department established a reasonable expectation of privacy in the text messages sent through a department-provided pager. *Id*. at 907 (quoting *O'Connor*, 480 U.S. at 717). In light of *Quon*, management officials at EINSTEIN 2.0 Participants should be careful not to make statements—either formal or informal—or to adopt practices that contradict the clear position in a log-on banner or a computer-user agreement that an employee has no legitimate expectation of privacy in his use of government-owned information systems.

2.

We next consider whether an individual in the private sector communicating with an Executive Branch employee (such as where an individual sends an e-mail to either the employee's governmental—i.e., work—or personal e-mail account) or with an EINSTEIN 2.0 Participant directly (such as where an individual browses the website of the participating department or agency) has a legitimate expectation of privacy in the content of those communications. We conclude that he does not, provided that EINSTEIN 2.0 Participants consistently adopt, implement, and enforce notice and consent procedures for Executive Branch employees, such as the model log-on banner or model computer-user agreement, or banners or user agreements with terms that are substantially equivalent to those models.

The Supreme Court has held repeatedly that "[t]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *United States v. Miller*, 425 U.S. 435, 443 (1976); *see SEC v. Jerry T. O'Brien, Inc*., 467 U.S. 735, 743 (1984) ("[W]hen a person communicates to a third party even on the understanding that the communication is confidential, he cannot object if the third party conveys that information or records thereof to law enforcement authorities."); *Smith*, 442 U.S. at

743–44 ("[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."). Accordingly, "[i]t is well[ ]settled" that where a person "reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information." *United States v. Jacobsen*, 466 U.S. 109, 117 (1984).

We believe this principle applies to a person e-mailing an Executive Branch employee at the employee's personal e-mail account, where the employee has agreed to permit the government to monitor, intercept, and search all of his Internet communications and data transiting government-owned information systems. By clicking through the model log-on banner or agreeing to the terms of the model computer-user agreement, an Executive Branch employee gives ex ante permission to the government to intercept, monitor, and search "any communications" and "any data" transiting or stored on a government-owned information system for any "lawful purpose." That permission necessarily includes the interception, monitoring, and searching of all personal communications and data sent or received by an employee using that system for the purpose of protecting Federal Systems against malicious network activity.[7] Therefore, an individual who communicates with an employee who has agreed to permit the government to intercept, monitor, and search any personal use of the employee's government-owned information systems has no Fourth

[7] The language of the model log-on banner and model computer-user agreement unambiguously applies to "any" communications and "any" data transiting through or stored on a government-owned information system and clearly eliminates any reasonable expectation of privacy that a user could have with respect to such communications and data. Nevertheless, if a participating department or agency wished to add even more express notice that those terms apply to personal communications and personal data that an employee sends, receives, or stores using a government-owned information system, such as the use of personal web-based e-mail accounts at work, the department or agency could do so in several ways. To be clear, we do not believe that any such efforts are legally required. But should a participating department or agency decide to go even further than the robust protection afforded by the model language, it would have several options at its disposal. For example, the department or agency could include in its log-on banner or computer-user agreement express language regarding personal communications or data. Or it could notify employees through computer training and certification programs that *any* personal use of government-owned information systems by an employee is subject to interception, monitoring, and searching.

Amendment right to prohibit the government from doing what the employee has authorized. *See Jerry T. O'Brien, Inc.*, 467 U.S. at 743; *Jacobsen*, 466 U.S. at 117; *Miller*, 425 U.S. at 443.

This well-settled Fourth Amendment principle applies even where, for example, the sender of an e-mail to an employee's personal, web-based e-mail account (such as G-mail or Hotmail) does not know of the recipient's status as a federal employee or does not anticipate that the employee might read an e-mail sent to a personal e-mail account at work. Indeed, it is well established that a person communicating with another (who turns out to be an agent for the government) assumes the risk that the person has agreed to permit the government to monitor the contents of that communication. *See, e.g.*, *United States v. White*, 401 U.S. 745, 749–51 (1971) (plurality opinion) (no Fourth Amendment protection against government monitoring of communications through transmitter worn by undercover operative); *Hoffa v. United States*, 385 U.S. 293, 300–03 (1966) (information disclosed to individual who turns out to be a government informant is not protected by the Fourth Amendment); *Lopez v. United States*, 373 U.S. 427, 439 (1963) (same); *Rathbun v. United States*, 355 U.S. 107, 111 (1957) ("Each party to a telephone conversation takes the risk that the other party may have an extension telephone and may allow another to overhear the conversation. When such takes place there has been no violation of any privacy of which the parties may complain."); *United States v. Coven*, 662 F.2d 162, 173–74 (2d Cir. 1981) (individual has no expectation of privacy in documents given to or accessible by undercover informant). Therefore, where an employee agrees to let the government intercept, monitor, and search any communication or data sent, received, or stored by a government-owned information system, the government's interception of the employee's Internet communications with individuals outside the Executive Branch does not infringe upon those individuals' legitimate expectations of privacy. *See also infra* pp. 83–89 (consent of employee).

We also think it clear that an individual submitting information directly to an EINSTEIN 2.0 Participant through the Internet—such as where an individual submits an application online or browses the public website of the Participant—has no legitimate expectation of privacy in the contents of any information that he transmits to the department or agency. An individual has no expectation of privacy in communications he makes to a known representative of the government. *See United States v. Caceres*,

440 U.S. 741, 750–51 (1979) (individual has no reasonable expectation of privacy in communications with IRS agent made in the course of an audit); *cf. Transmission by a Wireless Carrier of Information Regarding a Cellular Phone User's Physical Location to Public Safety Organizations*, 20 Op. O.L.C. 315, 321 (1996) (individual calling 911 lacks a reasonable expectation that information regarding his location will not be transmitted to public safety organizations) ("*Caller ID*"). Furthermore, an individual who communicates information to another individual who turns out to be an undercover agent of the government has no legitimate expectation of privacy in the content of that information. *See supra* p. 81. *A fortiori*, where an individual is communicating with a *declared* agent of the government—here, an executive department or agency—the individual does not have a legitimate expectation that his communication would not be monitored or acquired by the government. It also is well established that an individual does not have any legitimate expectation of privacy in information that he reveals to a third party. *See supra* p. 79; *see also United States v. Ganoe*, 538 F.3d 1117, 1127 (9th Cir. 2008) (individual has no legitimate expectation of privacy in computer files he made accessible to others); *United States v. King*, 509 F.3d 1338, 1342 (11th Cir. 2007) (individual has no legitimate expectation of privacy in computer files shared with others over network on military base). Hence, an individual could not possibly have a legitimate expectation of privacy in communications he shares directly with a department or agency of the government. Indeed, the entire purpose of his online communication is for the government to receive the content of his message. *Cf. Caller ID*, 20 Op. O.L.C. at 321 (purpose of calling 911 is to request governmental aid in an emergency). Therefore, we also do not believe that EINSTEIN 2.0 operations implicate a legitimate expectation of privacy in the content of Internet communications made between private individuals and an EINSTEIN 2.0 Participant.

B.

Even if EINSTEIN 2.0 operations were to constitute a "search" under the Fourth Amendment, we believe that those operations nonetheless would be consistent with that Amendment's "central requirement" that all searches be reasonable. *Illinois v. McArthur*, 531 U.S. 326, 330 (2001) (internal quotation marks omitted). Where, as here, the statutes and com-

mon law of the founding era do not provide a specific analogue, we analyze the reasonableness of a search in light of traditional judicial standards, balancing the degree of intrusion upon an individual's privacy in light of the search's promotion of legitimate governmental interests. *Virginia v. Moore*, 553 U.S. 164, 168–71 (2008). In many circumstances, a search is unreasonable unless law enforcement officials first obtain a warrant "issued by a neutral magistrate after finding probable cause." *McArthur*, 531 U.S. at 330. Yet the Supreme Court also has "made it clear that there are exceptions to the warrant requirement," *id.*, and that "neither a warrant nor probable cause, nor, indeed, any measure of individualized suspicion, is an indispensable component of reasonableness in every circumstance," *Nat'l Treasury Emps. Union v. Von Raab*, 489 U.S. 656, 665 (1989).

One well-known exception to the need to obtain a warrant based upon probable cause is where a person consents to the search. *See Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973) (consent is "one of the specifically established exceptions to the requirements of both a warrant and probable cause"). An Executive Branch employee who clicks "I agree" in response to the model log-on banner, enabling him to use government-owned information systems to access the Internet, or an employee who signs the model computer-user agreement, thereby acknowledging his "consent[]" to monitoring of his use of those systems, certainly appears to have consented expressly to the scanning of his incoming and outgoing Internet communications.

In the context of public employment, however, merely obtaining the consent of an employee to search is not necessarily coextensive with the requirements of the Fourth Amendment. Such consent must be voluntary and cannot be obtained through duress or coercion. *See generally Schneckloth*, 412 U.S. at 223–35. Where an employee is confronted with the choice of either consenting to a search or facing adverse employment consequences, it is debatable whether consent is in fact voluntary. An Executive Branch employee who refuses to accept a log-on banner or to sign a computer-user agreement likely will not be able to access his computer and, hence, may be unable to perform his duties. *See, e.g.*, *Anobile v. Pelligrino*, 303 F.3d 107, 124 (2d Cir. 2002) ("[C]oercion may be found where one is given a choice between one's employment and one's constitutional rights.").

Indeed, putting a public employee to the choice of either consenting to an *unreasonable* search or facing potential adverse employment consequences may impose an invalid condition on public employment. Into the first part of the 20th Century, the government "enjoyed plenary authority to condition public employment on the employee's acceptance of almost any term of employment including terms that restricted constitutional rights." Memorandum for the Attorney General, from Charles J. Cooper, Assistant Attorney General, Office of Legal Counsel, *Re: The Legality of Drug Testing Programs for Federal Employees* at 4 (Aug. 25, 1986) ("*Drug Testing*"). That view has since given way to the doctrine of unconstitutional conditions, which, as applied to public employment, prohibits the government from conditioning employment on the relinquishment of a constitutional right, such as the First Amendment right to freedom of speech. *See, e.g.*, *Pickering v. Bd. of Educ.*, 391 U.S. 563, 568 (1968) ("'The theory that public employment, which may be denied altogether may be subjected to any conditions, regardless of how unreasonable, has been uniformly rejected.'") (quoting *Keyishian v. Bd. of Regents*, 385 U.S. 589, 605–06 (1967)). More than 20 years ago, we noted that the federal courts of appeals "have generally applied the doctrine of unconstitutional conditions" to conditions of employment that would require government employees to forgo their Fourth Amendment rights against unreasonable searches. *Drug Testing* at 7 ("[T]here appears to be a consensus that the doctrine of unconstitutional conditions applies in the Fourth Amendment context."). That statement is just as true today. *See, e.g.*, *Anobile*, 303 F.3d at 123–25 (search of dormitories of horse-racing industry employees' pursuant to their written consent unreasonable under the Fourth Amendment); *McGann v. Ne. Ill. Reg'l Commuter R.R. Corp.*, 8 F.3d 1174, 1180 (7th Cir. 1993) ("[T]he conditioning of access on the surrender of one's Fourth Amendment rights raises the specter of an unconstitutional condition."); *McDonell v. Hunter*, 807 F.2d 1302, 1310 (8th Cir. 1987) ("If a search is unreasonable, a government employer cannot require that its employees consent to that search as a condition of employment."); *Doyon v. Home Depot U.S.A., Inc.*, 850 F. Supp. 125, 129 (D. Conn. 1994) (Cabranes, J.) ("[C]onsent to an unreasonable search is not voluntary when required as a condition of employment.").

We do not believe, however, that the unconstitutional conditions doctrine applies here, because obtaining the consent of employees for EINSTEIN 2.0 operations does not require Executive Branch employees

to consent to an *unreasonable* search. Notwithstanding that the terms of both the model log-on banner and the model computer-user agreement would permit monitoring of an employee's computer use for purposes other than network defense, we believe that the specific EINSTEIN 2.0 operations to which Executive Branch employees would be asked to consent would be reasonable.[8] Where, as here, an Executive Branch employee is being asked to consent only to a reasonable search, there is no invalid conditioning of public employment on the employee's relinquishment of his Fourth Amendment rights against unreasonable searches and no coercion that renders a search involuntary. *See, e.g.*, *United States v. Sihler*, 562 F.2d 349 (5th Cir. 1977) (prison employee's consent to routine search of his lunch bag valid); *cf. Drug Testing* at 7 ("[C]onsent to an *unreasonable* search is invalid.") (emphasis added); *Anobile*, 303 F.3d at 124 (similar); *McDonnell*, 807 F.2d at 1310 (similar). Thus, the inquiry regarding the voluntariness of an Executive Branch employee's consent merges with the underlying inquiry regarding the overall reasonableness of EINSTEIN 2.0 operations.[9] *See Drug Testing* at 7 ("[I]t appears that the government could not insist upon a complete waiver of Fourth Amendment rights as a condition of public employment and that the courts will scrutinize the search under the Fourth Amendment to determine whether it is reasonable.").

Therefore, we turn to the reasonableness of EINSTEIN 2.0 operations. A work-related administrative search by a public employer conducted for a non-law enforcement purpose is not per se unreasonable under the

---

[8] Because the question presented to us is whether an employee's consent to conduct the particular scanning activities performed by EINSTEIN 2.0 technology would be valid under the Fourth Amendment, we do not address whether there would be valid consent to conduct any other search that could be conducted pursuant to the terms of the model log-on banner or the model computer-user agreement. *See Warshak v. United States*, 532 F.3d 521, 529–31 (6th Cir. 2008) (en banc) (rejecting premature Fourth Amendment challenge to facial constitutionality of provisions of the Stored Communications Act).

[9] Indeed, the consent of an employee is one factor the courts consider in determining whether a search by a public employer is reasonable. *See, e.g.*, *Nat'l Treasury Emps. Union*, 489 U.S. at 672 & n.2 (considering consent to drug testing by customs officers as one factor in concluding that such testing was reasonable); *United States v. Scott*, 450 F.3d 863, 868 (9th Cir. 2006) ("[S]earches of government employees still must be reasonable. . . . The employee's assent is merely a relevant factor in determining how strong his expectation of privacy is, and thus may contribute to a finding of reasonableness.") (internal citations omitted).

Fourth Amendment simply because the government has not obtained a warrant based upon probable cause. The Supreme Court has said that "special needs, beyond the normal need for law enforcement," may render the warrant and probable cause provisions of the Fourth Amendment "impracticable for legitimate work-related, non-investigatory intrusions as well as investigations of work-related misconduct." *O'Connor*, 480 U.S. at 725 (plurality opinion) (internal quotation marks and citations omitted); *id*. at 732 (Scalia, J., concurring) (searches in the government-employment context present "special needs"); *see also Nat'l Treasury Emps*. *Union*, 489 U.S. at 665–66 (warrant and probable cause provisions of the Fourth Amendment are inapplicable to a search that "serves special governmental needs, beyond the normal need for law enforcement"); *Griffin v*. *Wisconsin*, 483 U.S. 868, 872 (1987) (special needs doctrine applies in circumstances that make the "warrant and probable cause requirement impracticable"). Rather, "public employer intrusions on the constitutionally protected privacy interests of government employees for noninvestigatory, work-related purposes . . . should be judged by the standard of reasonableness under all the circumstances." *O'Connor*, 480 U.S. at 726 (plurality); *see id*. at 732 (Scalia, J., concurring).

Here, the government plainly has a lawful, work-related, noninvestigatory purpose for the use of EINSTEIN 2.0's intrusion-detection system, namely the protection of Federal Systems against unauthorized network intrusions and exploitations. *See Heckenkamp*, 482 F.3d at 1148 (preventing misuse of and damage to university computer network is a lawful purpose); *see also Nat'l Treasury Emps*. *Union*, 489 U.S. at 668 (special needs include government's need to "discover . . . latent or hidden" hazards); Federal Information Security Management Act of 2002, Pub. L. No. 107-347, tit. III, 116 Stat. 2899, 2946 (2006) (codifying 44 U.S.C. §§ 3541–3549) ("FISMA") (establishing purposes and authorities for the protection of federal information systems). As we have already noted, *see supra* p. 64, there is a substantial history of intrusions and exploitations against Federal Systems. The deployment of EINSTEIN 2.0 technology is designed to provide greater awareness regarding intrusions and exploitations against those Systems in order to facilitate improved network defenses against malicious network activity. Those goals are unrelated to the needs of ordinary criminal law enforcement. *See Heckenkamp*, 482 F.3d at 1147–48 (state university has "separate security interests" in maintaining integrity and security of its network that are unrelated to

interest in law enforcement); *see also Illinois v. Lidster*, 540 U.S. 419, 424 (2004) (although ordinary law enforcement objectives do not qualify as "special needs," certain distinct "special law enforcement concerns" do); *Mich. Dep't of State Police v. Sitz*, 496 U.S. 444 (1990) (upholding highway checkpoint stops designed to detect and prevent drunk driving). It is true that DHS may share alerts of detected signatures associated with malicious computer code with other executive departments and agencies, including law enforcement agencies, as permitted by applicable law and DHS procedures. The disclosure of alert information to law enforcement agencies, however, is at most an ancillary, rather than a central, feature of EINSTEIN 2.0 operations. *Cf. Ferguson v. City of Charleston*, 532 U.S. 67, 79–80 (2001) ("central and indispensable feature" of hospital policy to screen obstetrics patients for cocaine was to facilitate "the use of law enforcement" tools—arrest and prosecution—"to coerce the patients into substance abuse treatment"); *City of Indianapolis v. Edmond*, 531 U.S. 32, 44 (2001) ("primary purpose" of narcotics checkpoints is to advance the "general interest" in "ordinary crime control"). We understand that EINSTEIN 2.0 operations are for the purpose of protecting Federal Systems, *see supra* p. 66, and are not conducted in order to advance ordinary law enforcement goals. Therefore, we conclude that EINSTEIN 2.0 operations would advance special governmental needs distinct from the ordinary interest in criminal law enforcement.

Furthermore, it would be impracticable to require the government to obtain a warrant based upon probable cause before deploying EINSTEIN 2.0 technology to detect malicious cyber activity against Federal Systems. The need for coordinated situational awareness regarding all intrusions and exploitations against Federal Systems is inconsistent with the requirement to obtain a warrant based upon probable cause. *See Bd. of Educ. v. Earls*, 536 U.S. 822, 828 (2002) (warrant and probable cause requirements are "peculiarly related to criminal investigations and may be unsuited to determining the reasonableness of administrative searches where the government seeks to prevent the development of hazardous conditions"). Indeed, the goal of near-real-time awareness of malicious network activity is incompatible with a requirement to obtain a warrant. Given the constant stream of intrusions and exploitations against Federal Systems and the time it would take to seek and obtain a warrant, it would be entirely impracticable—if not impossible—to identify data packets containing malicious code in near real-time if the government was re-

quired first to obtain a warrant before each such action. *See Skinner*, 489 U.S. at 623 (interest in dispensing with warrant requirement is at its strongest where "the burden of obtaining a warrant is likely to frustrate the governmental purpose behind the search") (internal quotation marks omitted). Requiring a particularized warrant based upon probable cause before a scan for each signature would introduce an element of delay, thus frustrating the government's ability to collect information regarding intrusions and exploitations in a timely manner. *See Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995) (obtaining a warrant based upon probable cause is not a necessary element of reasonableness where such a requirement "would unduly interfere with the swift and informal" procedures needed to facilitate the government's special needs) (internal quotation marks omitted). Moreover, in light of the speed and frequency with which intrusion and exploitation techniques change, requiring the government to obtain a warrant to use EINSTEIN 2.0 sensors to protect Federal Systems would require nearly continuous, ongoing, daily supervision by the courts of the details of the government's network-defense activities. Such supervision would frustrate efforts to protect Federal Systems and to obtain new information regarding advanced intrusion and exploitation techniques. *See Heckenkamp*, 482 F.3d at 1148 ("[R]equiring a warrant to investigate potential misuse of the university's computer network would disrupt the operation of the university and the network that it relies upon in order to function."). For these reasons, we do not believe that EINSTEIN 2.0 operations would be presumptively unreasonable absent a warrant justified by probable cause.

Therefore, the reasonableness of EINSTEIN 2.0 operations is measured in light of the "totality of the circumstances," *United States v. Knights*, 534 U.S. 112, 118 (2001), in "the context within which a search takes place," *New Jersey v. T.L.O.*, 469 U.S. 325, 337 (1985). In the context of a workplace search by a public employer, the reasonableness analysis requires balancing the "invasion of the employees' legitimate expectation of privacy against the government's need for supervision, control, and the efficient operation of the workplace." *O'Connor*, 480 U.S. at 719–20 (plurality); *see Knights*, 534 U.S. at 118–19 (reasonableness inquiry balances, "on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which a search is needed for the promotion of legitimate governmental interests") (internal quotation marks omitted). A reasonable workplace search must be "justified at

its inception" and "reasonably related in scope to the circumstances which justified the interference in the first place." *O'Connor*, 480 U.S. at 726 (plurality) (internal quotation marks omitted).

Based upon the information available to us, we believe that EINSTEIN 2.0 operations are reasonable under the totality of the circumstances. In light of the substantial history of intrusions and exploitations against Federal Systems, *see supra* p. 64, the deployment and use of EINSTEIN 2.0 technology to scan Federal Systems Internet Traffic of EINSTEIN 2.0 Participants for malicious computer code certainly is "justified at its inception." *O'Connor*, 480 U.S. at 726 (plurality) (internal quotation marks omitted).

We also conclude that any search conducted under EINSTEIN 2.0 operations would have a minimal impact upon the legitimate privacy expectations of computer users. The Supreme Court has said that "[w]hen faced with . . . diminished expectations of privacy, minimal intrusions, or the like, certain general, or individual, circumstances may render a warrantless search or seizure reasonable." *McArthur*, 531 U.S. at 330. We already have noted that individuals have no legitimate expectation of privacy whatsoever in certain categories of information collected by EINSTEIN 2.0—e.g., to/from addresses for e-mails, the IP addresses of websites visited, and the total traffic volume of a user—generated in connection with the routing of Internet communications. *See supra* pp. 71–72. And in light of the notice and consent procedures that EINSTEIN 2.0 Participants must adopt under the MOA, we believe that an individual's expectation of privacy in the content of Internet communications transiting Federal Systems would, at a minimum, be significantly diminished. *See supra* pp. 75–78. Furthermore, we think it is reasonably likely that most Executive Branch employees and United States persons interacting with EINSTEIN 2.0 Participants and their employees neither intend to include nor want to receive malicious computer code in their e-mails and other Internet communications. And those who do intentionally unleash malicious computer code upon the Internet in order to conduct an unauthorized exploitation against Federal Systems have "no reasonable expectation of privacy" in the contents of those unauthorized Internet communications. 18 U.S.C. § 2510(21)(A).

We also conclude that the use of EINSTEIN 2.0 technology to detect malicious computer code in Federal Systems Internet Traffic imposes, at

worst, a minimal burden upon legitimate privacy rights. Indeed, we understand that the actual scope of content monitoring by EINSTEIN 2.0 technology will be quite narrow. EINSTEIN 2.0 technology scans a mirror copy of the Federal Systems Internet Traffic of EINSTEIN 2.0 Participants. Of course, the EINSTEIN 2.0 technology will scan a copy of every single data packet of the Federal Systems Internet Traffic of those Participants. But we understand that the technology will scan that traffic—and only that traffic—only for particular malicious computer code associated with specific signatures. There is no authorization to acquire the content of any communication unrelated to detecting malicious computer code present in the packet. Therefore, we believe the intrusion upon any expectation of privacy in the privacy of the content of Internet communications that computer users may have vis-à-vis EINSTEIN 2.0 operations would be minimal, encompassing only the intrusion of searching for specified malicious computer code.

Our conclusion finds some support in the Supreme Court's cases holding that a search technique that reveals only unlawful activity is not subject to the Fourth Amendment at all. *See Jacobsen*, 466 U.S. at 123–24 (chemical field test that could disclose only whether white powder was cocaine does not infringe upon a legitimate expectation of privacy); *see also United States v. Place*, 462 U.S. 696, 706–07 (1983) (canine sniff by a well-trained narcotics detection dog that discloses only the presence or absence of narcotics is "*sui generis*" because it "is so limited both in the manner in which the information is obtained and in the content of the information revealed by the procedure" and, therefore, does not intrude upon a legitimate expectation of privacy). The inclusion of malicious computer code in an e-mail or other Internet-based communication may or may not be analogous to the possession of contraband, such as narcotics, at issue in *Jacobsen* and *Place*. But the use of malicious computer code to gain access to Federal Systems is a federal offense, *see, e.g.*, 18 U.S.C. § 1030(a)(2)(B), (3), & (5)(A) (2006), and the inclusion of that code in, for example, an e-mail is far from "perfectly lawful activity," *Illinois v. Caballes*, 543 U.S. 405, 409–10 (2005) (emphasizing that a canine sniff detects only unlawful activity and does not implicate legitimate privacy interests).

We also find support in the decisions of federal appellate courts concluding that the use of a magnetometer (a metal detector) to scan for weapons at airports, courthouses, and other special locations is a reasona-

ble search. *See, e.g.*, *United States v. Albardo*, 495 F.2d 799, 803–06 (2d Cir. 1974) (airport); *United States v. Epperson*, 454 F.2d 769, 771–72 (4th Cir. 1972) (airport); *Klarfield v. United States*, 944 F.2d 583, 586 (9th Cir. 1991) (courthouse). In those contexts, the government's interests are compelling, and the magnetometer's ability to detect not only weapons, but also keys, belt buckles, jewelry, and other harmless items does not otherwise render its use an unreasonable search. *See United States v. Bell*, 464 F.2d 667, 675 (2d Cir. 1972) (Friendly, J.); *Epperson*, 454 F.2d at 771–72. Regardless whether the government's interests here are on par with preventing hijacking or airport and courthouse violence, EINSTEIN 2.0 technology promotes the government's network-defense interests through a more limited and precise intrusion. The information provided to us indicates that EINSTEIN 2.0 technology is more precisely calibrated than a magnetometer to detect the materials (here, malicious computer codes) that pose a threat. *See supra* pp. 66–68. Hence, we believe that, like the use of the magnetometer in certain contexts, the use of EINSTEIN 2.0 technology to detect malicious computer code in Federal Systems Internet Traffic is a reasonable activity.

Furthermore, we understand that any information acquired or shared by DHS in the course of EINSTEIN 2.0 operations shall be subject to minimization procedures that are designed to minimize the acquisition, retention, and dissemination of non-publicly available information concerning United States persons. So, for example, even to the extent EINSTEIN 2.0 operations would acquire the content of malicious computer code that overlaps with human-readable text—e.g., the "I love you" virus from several years ago, or social engineering techniques that rely upon regular e-mail text to encourage the recipient to submit sensitive information, including personally identifiable information—we understand that these minimization procedures are intended to reduce further the impact of EINSTEIN 2.0 operations upon the privacy interests of United States persons in the content of their Internet communications. *Cf. In re Sealed Case*, 310 F.3d 717, 740 (FISA Ct. Rev. 2002) (noting importance of minimization procedures in holding that electronic surveillance pursuant to FISA was reasonable under the Fourth Amendment). In addition, we understand that DHS is required to develop auditing, oversight, and training procedures to ensure that its employees follow the procedures developed with respect to minimizing and protecting United States person information. We further understand that DHS is required to develop

procedures for the development of signatures to be programmed into the EINSTEIN 2.0 sensors, to ensure that the sensors are limited only to the detection of malicious computer code. In light of these safeguards, we believe that EINSTEIN 2.0 operations will have a minimal impact upon the legitimate privacy rights of computer users.

We conclude that the important governmental interest in protecting Federal Systems from intrusion and exploitation at the hands of foreign intelligence services, transnational criminal enterprises, and rogue computer hackers, *see supra* p. 64, outweighs the limited impact on the privacy rights, if any, of computer users communicating through Federal Systems. *See Heckenkamp*, 482 F.3d at 1148 (there is a "compelling government interest" in maintaining "the security of its network" and in determining the source of "unauthorized intrusion into sensitive files"); *Vernonia Sch. Dist.*, 515 U.S. at 661 (government must identify "an interest that appears *important enough* to justify the particular search at hand"). Based upon the information provided to us, we believe that EINSTEIN 2.0 operations would constitute a "reasonably effective means" of promoting those interests. *Earls*, 536 U.S. at 837 (activity must be "a reasonably effective means of addressing" government's interest); *see Vernonia Sch. Dist.*, 515 U.S. at 663 (considering "the efficacy of [the] means for addressing the problem"). As explained, *see supra* pp. 66–68, EINSTEIN 2.0 operations are expected to improve the government's situational awareness regarding computer network intrusions and exploitations against Federal Systems and to strengthen the ability to defend Federal Systems across the entire Executive Branch. Because EINSTEIN 2.0 technology is designed to detect and to store only malicious computer code associated with previously signatures, they also "are reasonably related in scope" to the problem EINSTEIN 2.0 is intended to address—the use of known malicious computer code to conduct intrusions and exploitations against Federal Systems. *O'Connor*, 480 U.S. at 726 (plurality) (internal quotation marks omitted).

Therefore, even if EINSTEIN 2.0 operations did involve a "search" within the meaning of the Fourth Amendment, we conclude that those operations nonetheless would satisfy the reasonableness requirement of the Fourth Amendment. For that same reason, we also conclude that an Executive Branch employee's agreement to the terms of the model log-on banner or the model computer-user agreement, or those of a banner or user agreement that are substantially equivalent to those models, consti-

tutes valid, voluntary consent to the reasonable scope of EINSTEIN 2.0 operations, and, thus, does not impose any coercive unconstitutional condition upon federal employment.

III.

We now turn to the statutory issues. DOJ has advised that the deployment, testing, and use of EINSTEIN 2.0 technology would comply with the requirements of the Wiretap Act, FISA, the SCA, and the Pen/Trap Act where EINSTEIN 2.0 Participants obtain the consent of their employees through appropriate log-on banners or computer-user agreements. As we concluded with respect to the Fourth Amendment, we also conclude that EINSTEIN 2.0 operations would be consistent with the requirements of these statutes, provided that each EINSTEIN 2.0 Participant consistently adopts, implements, and enforces the model log-on banner or model computer-user agreement—or a log-on banner or computer-user agreement containing substantially equivalent terms establishing that the consent of its employees is "clearly given" and "clearly obtained."

A.

We begin with the Wiretap Act. The Wiretap Act, as amended by title I of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) ("ECPA"), and other subsequent statutes, prohibits the intentional "intercept[]" of any "electronic communication" unless authorized by law. 18 U.S.C. § 2511(1)(a) (2006); *see also id.* § 2511(1)(c) & (d) (prohibiting the intentional disclosure or use of the contents of electronic communications acquired in violation of section 2511(1)(a)). As relevant here, the Act defines "intercept" as the "acquisition of the contents of any . . . electronic . . . communication through the use of any electronic, mechanical, or other device." *Id.* § 2510(4). EINSTEIN 2.0 technology would constitute a covered "device." *See id.* § 2510(5) (defining "electronic, mechanical, or other devices" as any device "which can be used to intercept a[n] . . . electronic communication other than" certain specified devices not applicable here).

Because use of the EINSTEIN 2.0 sensors requires the creation of a full mirror copy of the Federal Systems Internet Traffic of EINSTEIN 2.0 Participants, we conclude that the operation of those sensors "acqui[res] the contents" of an electronic communication within the meaning of the

Act. The Wiretap Act defines "contents" to mean "any information concerning the substance, purport, or meaning" of a communication. 18 U.S.C. § 2510(8). And "electronic communication" is defined to mean "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, . . . electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce," with certain exceptions not applicable here. *Id.* § 2510(12). The courts have held that communications that have not been recorded (to a medium such as a computer disk), viewed, or listened to have not been "acquired" within the meaning of the Wiretap Act. *See, e.g.*, *United States v. Lewis*, 406 F.3d 11, 17–18 (1st Cir. 2004). Although the full mirror copy of Federal Systems Internet Traffic is only temporary, we believe the creation of the copy is sufficient to constitute an acquisition of the contents of communication under the Wiretap Act. Furthermore, even if creation of the temporary mirror copy were not sufficient to implicate the provisions of that Act, EINSTEIN 2.0 technology also acquires and stores, for later review by analysts, data packets from Federal Systems Internet Traffic containing malicious computer code associated with a signature. The acquisition and storage of these data packets, which are part of the "contents" of electronic communications, certainly constitutes an "intercept" within the meaning of the Wiretap Act. *See* 18 U.S.C. § 2510(4), (5), (8), & (12). Therefore, absent an exception, section 2511(1)(a) applies to at least some aspects of EINSTEIN 2.0 operations.

The Wiretap Act also prohibits a person or entity providing "electronic communication service" to "the public" from intentionally "divulg[ing] the contents of any communication (other than one to such person or entity, or an agent thereof) 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." 18 U.S.C. § 2511(3)(a). It is unclear whether the federal Government provides "electronic communication service" to "the public." It reasonably could be argued that an EINSTEIN 2.0 Participant does offer websites and other Internet-related services that enable the transmission of electronic communications to and from the public, qualifies as a provider of electronic communication service to the public. *See id.* § 2510(15) (defining "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communication service"); *Black's Law Dictionary* 1227 (6th ed. 1990) (defining

public as "aggregate of the citizens"; "everybody"; "the community at large"). We need not decide the issue today, for even if the government is a provider of electronic communication service to the public, we do not believe that EINSTEIN 2.0 operations run afoul of the prohibitions in the Wiretap Act on the divulging of the contents of wire and electronic communications.

We conclude that EINSTEIN 2.0 operations do not constitute an unlawful interception or divulging of the contents of Internet communications under the Wiretap Act for two reasons. First, where EINSTEIN 2.0 Participants obtain the consent of their employees through appropriate log-on banners or computer-user agreements, there would be no violation of the Wiretap Act. Second, there is a strong argument that the government's EINSTEIN 2.0 operations are subject to the "rights or property" exception to the Wiretap Act. We also discuss, but do not decide, whether EINSTEIN 2.0 operations fall within the new "computer trespasser" exception to the prohibitions of the Wiretap Act.

1.

Under the Act, "[i]t shall not be unlawful . . . for a person acting under color of law to intercept a[n] . . . electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception." 18 U.S.C. § 2511(2)(c). Likewise, a person providing electronic communication service to the public "may divulge the contents of any such communication" either "to a person . . . authorized, or whose facilities are used, to forward such communications to its destination," *id*. § 2511(3)(b)(iii), or "with the lawful consent of the originator or any addressee or intended recipient of such communication," *id*. § 2511(3)(b)(ii). These exceptions take EINSTEIN 2.0 operations, if conducted consistent with the terms of the EINSTEIN 2.0 MOA, outside the scope of the prohibitions in the Wiretap Act.

The exception in section 2511(2)(c) applies to the interception of the contents of an Internet communication where an executive department or agency is a direct party to the communication, such as where an individual files a form with an agency through a website or responds online to a government survey. There is no violation of the Wiretap Act where "a person acting under color of law" intercepts an electronic communication

provided that "one of the parties to the communication has given prior consent to such interception." 18 U.S.C. § 2511(2)(c). For purposes of section 2511(2)(c), DHS is "a person acting under color of law" in the course of conducting EINSTEIN 2.0 operations. *Id.* § 2510(6) (defining person to include any "agent" of the United States Government). *See Nardone v. United States*, 302 U.S. 379, 384 (1937) (government bound by wiretap laws because "the sovereign is embraced by general words of a statute intended to prevent injury"); *cf.* 18 U.S.C. § 2520(a) (2006) (plaintiff may recover civil damages from "a person or entity, other than the United States," which engaged in that violation). By entering into an MOA with DHS, an EINSTEIN 2.0 Participant has signaled its consent to the interception by EINSTEIN 2.0 sensors and DHS of the content of Internet communications to which it is a party. Therefore, DHS lawfully may intercept the contents of an EINSTEIN 2.0 Participant's Internet communications with individuals under the Wiretap Act. *Id.* § 2511(2)(c). For the same reason, it also is lawful for an EINSTEIN 2.0 Participant to divulge the contents of an Internet communication to DHS for the purposes of EINSTEIN 2.0 operations where an EINSTEIN 2.0 Participant is one of the addressees or recipients of the communication. *Id.* § 2511(3)(b)(ii) (person may divulge contents of communication "with the lawful consent of the originator or any addressee or intended recipient of such communication").

With respect to intercepting and divulging the contents of Internet communications involving Executive Branch employees and individuals outside the Executive Branch, we do not believe that such actions would violate the prohibitions in the Wiretap Act. To begin with, EINSTEIN 2.0 operations do not unlawfully "divulge" the contents of Internet communications with Executive Branch employees, because the federal government is "authorized," and its "facilities are used, to forward such communications to [their] destination." 18 U.S.C. § 2511(3)(b)(iii). Internet communications cannot get to or from Executive Branch employees at work without routing through the facilities of Federal Systems.

There also is no violation of either the interception or the divulging prohibitions of the Wiretap Act where one of the parties to a communication has given consent. *See* 18 U.S.C. § 2511(2)(c) ("prior consent" required for intercept); *id.* § 2511(3)(b)(ii) ("lawful consent" required for divulging). An EINSTEIN 2.0 Participant cannot consent to the interception of the contents of the communications of its employees on their

behalf; rather, the consent of the employee who is the sender or the recipient of the communication is required. *See Television Surveillance*, 3 Op. O.L.C. at 67 (consent to surveillance is "not predicated on the consent of the owner of the pertinent property, but rather on the consent of the person to whom the targeted individual reveals his communications or activities"); *see also Caceres*, 440 U.S. at 750 ("[F]ederal statutes impose no restrictions on recording a conversation with the consent of one of the conversants."); *United States v. Barone*, 913 F.2d 46, 49 (2d Cir. 1990) (one-party consent obviates the need to obtain a court order under the Wiretap Act). As with any other person, an employee's consent under the Wiretap Act also must be provided voluntarily. *See United States v. Hernandez*, 93 F.3d 1493, 1500 (10th Cir. 1996). Here, an employee's valid, voluntary consent is expressly apparent from his clicking through the log-on banner or signing the computer-user agreement in order to access a government-owned information system. *See supra* pp. 83–89; Memorandum for Ronald D. Lee, Associate Deputy Attorney General, from William Treanor, Deputy Assistant Attorney General, Office of Legal Counsel, *Re: Report of the Working Group on Access to Government Property (Second Draft)* at 5 (June 1, 2000) (consent exception in Wiretap Act satisfied where employee clicks through log-on banner acknowledging monitoring of electronic communications in order to access DOJ's computer network).

An Executive Branch employee's consent to interception or divulging of the contents of his Internet communications also may be implied where the "'circumstances indicat[e] that the [individual] knowingly agreed to the surveillance.'" *United States v. Van Poyck*, 77 F.3d 285, 292 (9th Cir. 1996) (quoting *United States v. Amen*, 831 F.2d 373, 378 (2d Cir. 1987) (federal inmate consented to interception of phone calls where notice that inmate calls were monitored was ubiquitous)). Under the Wiretap Act, "as in other settings, consent inheres where a person's behavior manifests acquiescence or a comparable voluntary diminution of his or her otherwise protected rights." *Griggs-Ryan v. Smith*, 904 F.2d 112, 116 (1st Cir. 1990) (tenant consented to landlord's recording of phone calls where tenant knew that all calls were being recorded); *accord United States v. Staves*, 383 F.3d 977, 981 (9th Cir. 2004) (party to communication impliedly consents to monitoring where circumstances "indicate that [he] knew that interception was likely and agreed to the monitoring"). Where "language or acts . . . tend to prove (or disprove) that a party knows of, or

assents to, encroachments" on a routine expectation of privacy, that party has manifested his consent for purposes of the Wiretap Act. *Griggs-Ryan*, 904 F.2d at 117; *see Van Poyck*, 77 F.3d at 292 (similar).

Here, no Executive Branch employee who has read the model log-on banner or computer-user agreement (or a log-on banner or computer-user agreement with substantially equivalent terms) and who nonetheless has logged on to a government-owned information system could reasonably claim not to have knowledge that monitoring, interception, and searches of his Internet communications would occur. The employee's use of government-owned information systems despite that knowledge would establish voluntary consent to any such monitoring, interception, or search. *See supra* pp. 81, 84–93.[10] Therefore, we believe that EINSTEIN 2.0 operations would comply with the Wiretap Act as long as EINSTEIN 2.0 Participants consistently adopt, implement, and enforce the terms of appropriate log-on banners or computer-user agreements, as discussed in this memorandum.

2.

Even absent the consent of Executive Branch employees, there is a reasonable basis to conclude that the use of EINSTEIN 2.0 technology to protect Federal Systems comes within the express terms of the "rights or property" exception to the prohibitions in the Wiretap Act, 18 U.S.C. § 2511(2)(a)(i). The "rights or property" exception provides in relevant part that the prohibitions in the Act shall not apply to the "intercept, disclosure, or use" of an "electronic communication" by a "provider of a wire or electronic communication service . . . engaged in any activity which is a necessary incident to . . . the protection of the rights or property of the provider of that service." *Id.*

We believe that this provision may be applied to the government here as a "provider" of "electronic communication service[s]" for its employ-

[10] Similarly, no reasonable person communicating directly with an agency of the federal government through the Internet, such as by filing a form on an agency website, could claim not to know that his communication would be acquired by the government. Indeed, that is the entire purpose of communicating with the government. *See supra* pp. 81–82. Hence, the individual impliedly would consent to the government's interception of the contents of his communication. *See Caller ID*, 20 Op. O.L.C. at 320 & n.13 (dialing 911 constitutes implicit consent to government's direct monitoring of an emergency call).

ees. Executive Branch departments and agencies provide the necessary computers, network infrastructure, facilities, and connectivity to the Internet that enable Executive Branch employees "to send or receive" electronic communications. 18 U.S.C. § 2510(15) (defining "electronic communication service"). The courts have held that to benefit from the rights or property exception, the electronic communication service provider's activities must protect the provider's own rights or property, and not those of any third party, such as a customer. *See, e.g.*, *Campiti v. Walonis*, 611 F.2d 387, 393 (1st Cir. 1979) (rights or property exception does not apply to a person who is not an agent of the telephone company for monitoring that "had nothing to do with telephone company equipment or rights"); *United States v. Auler*, 539 F.2d 642, 645–46 (7th Cir. 1976) (telephone companies intercepting communications under section 2511(2)(a)(i) may share those communications with the government only to the extent necessary to protect telephone company's rights or property). EINSTEIN 2.0 technology is owned, operated, and controlled by DHS, and we understand that it is to be used solely for the protection of the government's rights and property in Federal Systems. *See supra* p. 66.

The legislative history of the rights or property exception in the Wiretap Act arguably speaks only to the efforts of telephone companies to monitor calls in order to prevent callers from using "blue boxes" to avoid paying for long-distance telephone calls. *See* S. Rep. No. 90-1097, at 67 (1967), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2182. Nevertheless, we believe that "the plain meaning of Congress'[s] language" in the "rights or property" exception includes EINSTEIN 2.0 operations "within its ambit." *United States v. Savage*, 564 F.2d 728, 731 (5th Cir. 1977). The courts have construed the "necessary" language in the Wiretap Act provision "to impose a standard of reasonableness upon" the provider's activities to protect his rights or property. *United States v. Harvey*, 540 F.2d 1345, 1351 (8th Cir. 1976); *see, e.g.*, *United States v. McLaren*, 957 F. Supp. 215, 220 (M.D. Fla. 1997) (similar). As in the Fourth Amendment context, reasonableness is "assessed under the facts of each case." *Harvey*, 540 F.2d at 1352 n.9. The "rights or property" exception does not strictly *require* "minimization" of the acquisition of communication contents by a provider, *McLaren*, 957 F. Supp. at 220, but a provider's activities are reasonable under the exception where they involve only "minimal interception" of communications. *Harvey*, 540 F.2d at 1351.

We believe that the government's use of EINSTEIN 2.0 technology to detect intrusions and exploitations against Federal Systems is reasonably necessary to protect the federal government's rights with respect to its exclusive use of Federal Systems and its property interests in the integrity and security of its networks and data. For the reasons we have noted already, *see supra* pp. 89–92, we believe that EINSTEIN 2.0 operations would involve the minimal acquisition and storage of communications necessary to detect malicious network activity directed against Federal Systems. EINSTEIN 2.0 operations are limited to the detection and storing of data packets containing only malicious computer code associated with computer intrusions and exploitations, and are reasonably designed to protect Federal Systems without acquiring any additional content of Internet communications that is unrelated to that goal. Thus, EINSTEIN 2.0 operations are appropriately limited in scope to what is reasonably necessary to protect governmental rights and property against computer intrusions and exploitations. *See Harvey*, 540 F.2d at 1351 (recording of limited portion of phone calls to identify use of technology to evade paying for long-distance calls is "reasonable"); *United States v. Freemen*, 524 F.2d 337, 341 (7th Cir. 1975) (taping of conversations for no more than two minutes and only when blue box was in use was "necessary and in line with the minimal invasion of privacy contemplated by the statute"); *cf. Auler*, 539 F.2d at 646 (monitoring and recording of all calls, regardless whether made using a blue box, acquired "far more information" than the telephone company "needed to protect its interests"); *McLaren*, 957 F. Supp. at 220 (interception, recording, and disclosure of complete phone calls "having nothing whatever to do" with abuse of telephone company's service is unreasonable because those actions "could not possibly be 'necessary'" to protecting the company's rights).

Therefore, even absent employee consent, there is a strong basis in the text of the "rights or property" exception to the Wiretap Act to believe that the government's activities under EINSTEIN 2.0 would not violate the prohibitions in the Wiretap Act. That being said, however, there are very few cases applying the rights or property exception since the mid-1970s, and almost none involving computer networks, the Internet, or defenses against cyber intrusions and exploitations, and none involving the government in protecting its own rights or property, as opposed to a private communications provider protecting its private property. Accordingly, we believe there is some uncertainty regarding how the courts

would view a defense of EINSTEIN 2.0 operations based upon the "rights or property" exception to the Wiretap Act.

3.

Finally, we discuss briefly the "computer trespasser" exception in the Wiretap Act, 18 U.S.C. § 2511(2)(i), which was added to the Wiretap Act by section 217 of the USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272, 291 (2001). Section 2511(2)(i) permits "a person acting under color of law" to "intercept" the contents of "wire or electronic communications of a computer trespasser transmitted to, through, or from [a] protected computer" on four conditions: First, "the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer." Second, "the person acting under color of law is lawfully engaged in an investigation." Third, "the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation." And fourth, "such interception does not acquire communications other than those transmitted to or from the computer trespasser." 18 U.S.C. § 2511(2)(i)(I)–(IV). The phrase "protected computer" has the same definition as in 18 U.S.C. § 1030(e)(2), *see id.* § 2510(20) (defining "protected computer"), which includes the government-issued computers of EINSTEIN 2.0 Participants at issue here. "Computer trespasser" is defined to mean "a person who accesses a protected computer without authorization" and "does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer." *Id.* § 2510(21)(A) & (B).

We need not discuss the first three requirements of the computer trespasser exception. Even assuming that EINSTEIN 2.0 operations satisfy these requirements, it is questionable that EINSTEIN 2.0 operations satisfy the final requirement. The computer trespasser exception is applicable only if interception of the contents of communications "does not acquire communications other than those transmitted to or from the computer trespasser." 18 U.S.C. § 2511(2)(i)(IV). We understand that EINSTEIN 2.0 technology is designed to detect and to store only packets containing malicious computer code associated with a signature. Accord-

ingly, it could be argued that it would not acquire communications other than the malicious code sent over the Internet by computer trespassers, as defined in section 2510(21). However, EINSTEIN 2.0 technology also can acquire the contents of communications to or from persons who do not satisfy the definition of "computer trespasser." To take just one example, an Executive Branch employee—even one who intentionally includes malicious computer code in his Internet communications at work—does not appear to be a "computer trespasser" within the scope of the definition. *See id.* § 2510(21)(B) (defining "computer trespasser" to exclude a "person known by the owner or operator of the protected computer to have an existing contractual relationship . . . for access to all or part of the protected computer").[11] EINSTEIN 2.0 operations, however, nonetheless would acquire the contents of their communications.

We do not decide, however, whether the computer trespasser exception would or would not apply to EINSTEIN 2.0 operations. In light of the other legal justifications for EINSTEIN 2.0 operations under the Wiretap Act, we need not rely upon this provision.

B.

We next consider whether the provisions in title I of FISA, which govern the conduct of "electronic surveillance" within the United States, and in revised title VII of FISA, which govern, among other things, the acquisition of foreign intelligence information from United States persons outside the United States, apply to the deployment, testing, and use of EINSTEIN 2.0 technology. We conclude that they do not, provided that EINSTEIN 2.0 Participants obtain the consent of their employees through the terms of log-on banners or computer-user agreements, as discussed throughout this memorandum.

1.

Under 50 U.S.C. § 1809(a)(1) (Supp. II 2008), it is a felony for a person acting "under color of law" to engage intentionally in "electronic

[11] That does not mean that the government would be prohibited from acquiring the communications of an employee or contractor who intentionally incorporates malicious code in their Internet communications. Rather, some other statutory exception—such as consent or the rights or property exception—may authorize that result.

surveillance" as defined in title I of FISA, *see* 50 U.S.C. § 1801(f) (2006), "except as authorized" by FISA, the Wiretap Act, the SCA, the Pen/Trap Act, or any other "express statutory authorization that is an additional exclusive means for conducting electronic surveillance" under 50 U.S.C. § 1812(b) (Supp. II 2008). *See also id*. § 1810 (2006) (establishing civil penalties for violations of section 1809(a)(1)). As we have established in Part III.A, EINSTEIN 2.0 operations would not be prohibited by the Wiretap Act. Thus, it could be argued that they are "authorized" under the Wiretap Act. On this view, FISA does not govern activity that is expressly permitted under provisions in the Wiretap Act, such as activity falling within the terms of the consent or the rights or property exception. *Cf. Freemen*, 524 F.2d at 340 & n.5 (phrase "[e]xcept as authorized by [the Wiretap Act]" in 47 U.S.C. § 605(a) (1970) "permits" telephone companies to protect their rights or property under section 2511(2)(a)(i) notwithstanding any otherwise applicable terms of section 605(a)). Accordingly, EINSTEIN 2.0 operations permitted under the rights or property exception of the Wiretap Act would be authorized notwithstanding the electronic surveillance provisions of FISA (and notwithstanding the absence of a rights or property exception in FISA).

There is much to recommend that view, although the better reading of "authorized" may be that the term refers to orders obtained under the procedures of the Wiretap Act, the SCA, the Pen/Trap Act, or another covered statute, rather than to activities that merely are not prohibited by those statutes. *Cf. United States v. Keen*, 508 F.2d 986, 988 (9th Cir. 1974) ("Section 2511(2)(c) is worded as an exception to [the] general prohibition of judicially non-authorized wire taps, not as a positive authorization of such taps."). We need not and do not resolve this issue today. Rather, we assume for the purposes of this memorandum that title I of FISA applies to the deployment, testing, and use of EINSTEIN 2.0 technology if those actions constitute "electronic surveillance" within the meaning of 50 U.S.C. § 1801(f).

Section 1801(f) sets forth four separate definitions of "electronic surveillance." They are as follows:

> (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communications sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired

> by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
>
> (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18;
>
> (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or
>
> (4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

50 U.S.C. § 1801(f)(1)–(4). EINSTEIN 2.0 operations that scan, acquire, and store copies of data packets containing malicious computer code from Federal Systems Internet Traffic constitute an "acquisition" of the "contents" of a communication. *Id.* § 1801(n) (defining "contents" to include "any information concerning the identity of the parties to . . . communications or the existence, substance, purport, or meaning of that communication").

Nevertheless, paragraphs (1) and (3) of section 1801(f) do not apply to EINSTEIN 2.0 operations. Those operations do not constitute electronic surveillance under section 1801(f)(1), because EINSTEIN 2.0 sensors generally would not target any "particular, known United States person" in the United States. Nor do EINSTEIN 2.0 operations constitute electronic surveillance within the meaning of section 1801(f)(3), because the EINSTEIN 2.0 sensors do not acquire the contents of any "radio communication." As explained in Part I, EINSTEIN 2.0 sensors are to scan only a mirror copy of Federal Systems Internet Traffic created as that traffic passes through the facilities located at the government's TICs. Further-

more, even if section 1801(f)(1) and section 1801(f)(3) did apply to EINSTEIN 2.0 operations, the use of EINSTEIN 2.0 technology still does not constitute "electronic surveillance" under those definitions, because the use of those sensors does not implicate "a person's reasonable expectation of privacy." *See supra* pp. 71–82 and *infra* p. 106.

That leaves section 1801(f)(2) and (4). Section 1801(f)(2) applies to EINSTEIN 2.0 operations only if EINSTEIN 2.0 technology acquires the contents of "wire communication[s]," which FISA defines as "any communication while it is being carried by a wire, cable, or other like connection furnished or operated by . . . a common carrier . . . providing or operating such facilities for the transmission of interstate or foreign communications." 50 U.S.C. § 1801(*l*); *see* H.R. Rep. No. 95-1283, at 66–67 (1978) (communications are wire communications "only when they are carried by a wire furnished or operated by a common carrier"). FISA does not define the term "common carrier." We need not decide whether EINSTEIN 2.0 operations acquire the contents of communications while being carried by the wire facilities of a common carrier. Even if they do, the use of EINSTEIN 2.0 technology does constitute electronic surveillance under section 1801(f)(2) as long as the government obtains "the consent of any party" to a communication to acquire the contents of that communication. 50 U.S.C. § 1801(f)(2).

Because the consent exception in section 1801(f)(2) concerns the same subject matter—consent of a party to a communication—as section 2511(2)(c), we construe the two provisions *in pari materia*. *See Wachovia Bank, N.A. v. Schmidt*, 546 U.S. 303, 316 (2006) (statutes addressing a similar subject matter should be read "as if they were one law") (internal quotation marks omitted); *Authority of USDA to Award Monetary Relief for Discrimination*, 18 Op. O.L.C. 52, 69 (1994) ("Statutes addressing the same subject matter—that is, statutes '*in pari materia*'—should be construed together."). That construction is consistent with the stated views of the Senate Select Committee on Intelligence and the Senate Committee on the Judiciary in their respective committee reports on the legislation that ultimately would become FISA. *See* S. Rep. No. 95-604, pt. I, at 35 (1978) (definition of electronic surveillance "has an explicit exception where any party has consented to the interception. This is intended to perpetuate the existing law regarding consensual interceptions found in 18 U.S.C. § 2511(2)(c)."), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3936–37; S. Rep. No. 95-701, at 37 (1978) (same), *reprinted in* 1978 U.S.C.C.A.N.

3973, 4006. Accordingly, for the same reasons already noted above with respect to the Wiretap Act, we believe that the government could obtain valid consent under section 1801(f)(2) through consistent and actual use of log-on banners or computer-user agreements. *See United States v. Missick*, 875 F.2d 1294, 1299 (7th Cir. 1989) (section 1801(f)(2) does not apply to acquisition of content of telephone calls where one of the parties consented).

For that same reason, we do not believe that EINSTEIN 2.0 operations constitute "electronic surveillance" under section 1801(f)(4). It is plain that the use of EINSTEIN 2.0 technology constitutes "the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information." 50 U.S.C. § 1801(f)(4). But regardless whether that technology would acquire the contents of communications "other than from" the wire facilities of a common carrier, EINSTEIN 2.0 operations would not fall within the scope of section 1801(f)(4). As long as EINSTEIN 2.0 Participants consistently adopt, implement, and enforce the use of appropriate log-on banners or computer-user agreements as discussed in this memorandum, EINSTEIN 2.0 technology would not acquire the contents of Internet communications under circumstances where there is a "reasonable expectation of privacy" and a warrant "would be required for law enforcement purposes." *See supra* Parts II.A.2, III.A.1; *see also Interception of Radio Communication*, 3 Op. O.L.C. 240, 241 (1979) (phrase "reasonable expectation of privacy" in FISA incorporates "the standard of constitutionally protected privacy interests"); H.R. Rep. No. 95-1283, pt. 1, at 53 (1978) (under section 1801(f)(4) "the acquisition of information [must] be under circumstances in which a person has a constitutionally protected right of privacy. There may be no such right in those situations where the acquisition is consented to by at least one party to the communication"); S. Rep. No. 95-701, at 37 (1978) (same).

Therefore, EINSTEIN 2.0 operations would not constitute "electronic surveillance" under title I of FISA as long as EINSTEIN 2.0 Participants consistently adopt, implement, and enforce the terms of appropriate log-on banners or computer-user agreements, as discussed in this memorandum.

2.

For the same reasons, we do not believe that the use of EINSTEIN 2.0 technology with respect to the Federal Systems Internet Traffic of Executive Branch employees outside the United States, such as (hypothetically) employees of the Department of State or the Central Intelligence Agency, implicates revised title VII of FISA. As applicable here, section 703(a)(1) of FISA provides that the Foreign Intelligence Surveillance Court ("FISC") shall have jurisdiction over the "the targeting of a United States person reasonably believed to be located outside the United States to acquire foreign intelligence information, if the acquisition constitutes electronic surveillance" under FISA. 50 U.S.C. § 1881b(a)(1) (Supp. II 2008). And section 704(a)(2) of FISA generally prohibits elements of the Intelligence Community from "intentionally target[ing], for the purpose of acquiring foreign intelligence information, a United States person reasonably believed to be located outside the United States under circumstances in which [the] person has a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted inside the United States for law enforcement purposes." *Id*. § 1881c(a)(2) (Supp. II 2008).

We have no reason to believe that EINSTEIN 2.0 operations generally would involve the intentional targeting of any United States person employed by an EINSTEIN 2.0 Participant outside the United States in order to acquire "foreign intelligence information" as defined in 50 U.S.C. § 1801(e). Even assuming for the sake of argument that EINSTEIN 2.0 operations would satisfy those requirements, we do not believe those operations would satisfy the other jurisdictional requirements in sections 1881b(a)(1) or 1881c(a)(2), provided that EINSTEIN 2.0 Participants employing United States persons outside the United States consistently adopt, implement, and enforce appropriate notice and consent procedures, as discussed in this memorandum. In that circumstance, there would be no "electronic surveillance" as defined in section 1801(f)(1)–(4), and, thus, section 1881b(a)(1) would be inapplicable. *See supra* Part III.B.1. Likewise, there would be no reasonable expectation of privacy and a warrant would not be required for law enforcement purposes for either of two reasons: there would be no search under the Fourth Amendment, *see supra* Part II.A, or there would be proper consent, thus obviating the need for a warrant and probable cause, *see supra* pp. 81, 84–93. Under either rationale (or both), the prohibition in section 1881c(a)(2) would not apply.

Therefore, we do not believe that EINSTEIN 2.0 operations would be subject to revised title VII of FISA.

C.

We also conclude that the relevant provisions of the Stored Communications Act would not apply to EINSTEIN 2.0 operations, provided that EINSTEIN 2.0 Participants consistently adopt, implement, and enforce the terms of appropriate log-on banners or computer-user agreements, as discussed in this memorandum. As relevant here, the SCA prohibits a person or entity "providing an electronic communication service to the public" from knowingly "divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1) (2006). As already noted with respect to the Wiretap Act, it is unclear that the federal government—which does offer websites and other Internet-related services that enable the transmission of electronic communications to and from the public—qualifies as a provider of electronic communication service to the public under the SCA. *See supra* p. 94. The matter is far from settled. *Compare Andersen Consulting LLP v. UOP*, 991 F. Supp. 1041, 1042–43 (N.D. Ill. 1998) (computer system of partnership used to communicate with third parties does not provide electronic communication service to the public within the meaning of the SCA), *with Bohach v. City of Reno*, 932 F. Supp. 1232, 1236 (D. Nev. 1996) (City of Reno is an "electronic communication service provider" under the SCA because it provides the terminals, computers, pages, and software that enables its own personnel to send and to receive electronic communications). We need not decide the issue, for even if the government is a provider of electronic communication service to the public, we do not believe that EINSTEIN 2.0 operations would run afoul of the SCA.

EINSTEIN 2.0 operations would implicate the prohibition in section 2702(a)(1) if the temporary mirroring of all Federal Systems Internet Traffic of EINSTEIN 2.0 Participants divulges the content of an electronic communication "while in electronic storage." The SCA defines "electronic storage" to mean:

> (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

> (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

Id. § 2510(17)(A) & (B). The courts have interpreted section 2510(17)(A) to apply only to an electronic communication stored temporarily on a provider's server pending delivery of the communication to the recipient. *See, e.g*., *In re DoubleClick, Inc*. *Privacy Litig*., 154 F. Supp. 2d 497, 511–12 (S.D.N.Y. 2001). As noted in Part I, *see supra* p. 67, EINSTEIN 2.0 technology does not have any effect upon the transmission of wire or electronic communications to their intended recipients. Rather, EINSTEIN 2.0 operations will make a mirror copy of every packet in Federal Systems Internet Traffic and will scan that copy to detect known signatures. This copy is "temporary" storage of communications "incidental" to their transmission, in the sense that the storage is related to the transmission of those communications. But arguably it is not "intermediate" in the process of that transmission, because the temporary copy is not created as part of a step in the chain of transmitting the communication to its intended recipient. Rather, the copy is made for the separate purpose of enabling EINSTEIN 2.0 sensors to detect malicious computer code embedded in Federal Systems Internet Traffic. Indeed, the EINSTEIN 2.0 scanning process occurs out-of-line from the transmission process, even if it is related to the in-line transmission of Federal Systems Internet Traffic.

Nor do we understand that EINSTEIN 2.0 operations would divulge the content of any communication while in storage "for purposes of backup protection" within the meaning of section 2510(17)(B), even under a broader reading of "backup protection" than DOJ has embraced in litigating the scope of that provision. *See Theofel v*. *Farey Jones*, 341 F.3d 978, 985 (9th Cir. 2003) (backup protection means "storing a message on a service provider's server after delivery to provide a second copy of the message in the event that the user needs to download it again"). Because the EINSTEIN 2.0 sensors scan a mirror copy of Federal Systems Internet Traffic for the purpose of detecting malicious computer code, there is no routing of the contents of any communication stored by an ISP for purposes of backup protection. It is true that EINSTEIN 2.0 technology would store data packets containing malicious computer code for later review by DHS analysts. But the "purpose" of any storage and subsequent review by analysts of blocked data packets would be to prevent

intrusions and exploitations against Federal Systems, and not "to provide a second copy of the message in the event that the user needs to download it again." *Id.* at 985. Therefore, we have no reason to believe that EINSTEIN 2.0 operations would divulge the contents of communications stored for backup protection.

Even if section 2702(a)(1) would apply to EINSTEIN 2.0 operations, scanning Federal Systems Internet Traffic for malicious computer code would fall within the SCA's consent exception in 18 U.S.C. § 2702(b)(3) as long as EINSTEIN 2.0 Participants consistently adopt, implement, and enforce the terms of appropriate log-on banners or computer-user agreements, as discussed in this memorandum. Section 2702(b)(3) states in relevant part that an electronic communication service provider "may divulge the contents of a communication . . . with the lawful consent of the originator or an addressee or intended recipient of such communication." *Id.*; *see also id.* § 2702(c)(2) (provider may divulge information pertaining to subscriber or customer of electronic communication service, but not the contents of that communication, "with the lawful consent of the customer or subscriber"). We have interpreted a similar consent exception in 18 U.S.C. § 2703(c)(1)(B)(iii) (2006), which states that a provider shall divulge a record pertaining to the identity of a subscriber or customer—but not the contents of a communication—to a governmental entity that "has the consent" of the customer or subscriber, *in pari materia* with the consent exception in the Wiretap Act. *See Caller ID*, 20 Op. O.L.C. at 319 & n.12 (interpreting consent exception in section 2703(c)(1)(B)(iii) in accord with the consent exception in the Wiretap Act). We also construe the consent exception in section 2702(b)(3)—which is even more closely analogous to the consent exception in section 2511(2)(c) than is section 2703(c)(1)(B)(iii)—*in pari materia* with section 2511(2)(c). *See supra* p. 105. For the reasons already noted with respect to the consent exception in the Wiretap Act, *see supra* Part III.A.1, to the extent the SCA applies to EINSTEIN 2.0 operations, we believe that the government could obtain proper consent under section 2702(b)(3) and (c)(2) through the consistent and actual use of log-on banners or computer-user agreements.[12]

[12] EINSTEIN 2.0 operations also may fall within the "rights or property" exceptions to the SCA, *see* 18 U.S.C. § 2702(b)(5), (c)(3). The SCA's "rights or property" exceptions are substantively similar to the parallel exception in the Wiretap Act. The SCA's first

D.

Finally, we conclude that the Pen/Trap Act would not apply to EINSTEIN 2.0 operations where EINSTEIN 2.0 Participants consistently adopt, implement, and enforce the terms of appropriate log-on banners or computer-user agreements, as discussed in this memorandum. Section 3121(a) of title 18, United States Code, provides that "[e]xcept as provided in this section, no person may install or use a pen register or a trap-and-trace device without first obtaining a court order under section 3123 of this title or" FISA. 18 U.S.C. § 3121(a) (2006). As relevant here, the statute defines a "pen register" as a "device . . . which records or decodes . . . routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication." *Id*. § 3127(3) (2006). And a "trap-and-trace device" means "a device . . . which captures the incoming electronic or other impulses which identify . . . routing, addressing, and signaling information reasonably likely to identify the source of a wire or

---

rights or property provision states that a provider of electronic communication service to the public may divulge the contents of a stored communication "as may be necessarily incident . . . to the protection of the rights or property of the provider of that service." 18 U.S.C. § 2702(b)(5). Another provision in the SCA permits a provider of electronic communication service to the public to disclose non-content information regarding a subscriber or a customer "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." *Id*. § 2702(c)(3). In light of the similarities in wording and subject matter between the SCA's rights or property exceptions and the Wiretap Act's parallel provision, we construe them *in pari materia*. *See supra* pp. 105, 110.

A crucial difference, however, between the "rights or property" exceptions in the SCA and the one in the Wiretap Act is that the SCA provisions apply only to a provider of electronic communication service *to the public*, whereas the Wiretap Act provision applies to *any* provider of such service, whether to the public or otherwise. As we noted, it is debatable whether the government is a "provider" of electronic communication service to the public under the SCA. *See supra* pp. 94, 108. Assuming that the government is a public provider of electronic communication service, the SCA's rights or property exceptions apply to any action under EINSTEIN 2.0 divulging the contents of stored electronic communications or non-content information concerning a subscriber or a customer that is reasonably necessary to protect Federal Systems. *See supra* Part III.A.2. Of course, if the government is not a public provider, then the provisions of the SCA do not apply to it in any event.

electronic communication, provided, however, that such information shall not include the contents of any communication." *Id.* § 3127(4).[13]

We assume for the purposes of this memorandum that the use of EINSTEIN 2.0 technology would fall within the definitions of both a pen register and a trap-and-trace device, because they can both "record" and "capture," 18 U.S.C. § 3127(3) & (4), information that identifies routing, addressing, and signaling information for data packets that are part of Federal Systems Internet Traffic. *See supra* pp. 66–68, 71. Hence, absent an exception, we assume that the government would be required to obtain a court order before the deployment, testing, and use of EINSTEIN 2.0 technology. *See* 18 U.S.C. § 3123 (2006).

As with the Wiretap Act, FISA, and the SCA, obtaining the valid consent of Executive Branch employees also exempts EINSTEIN 2.0 operations from any applicable requirement of the Pen/Trap Act. Section 3121(a) "does not apply with respect to the use of a pen register or a trap-and-trace device by a provider of electronic or wire communication service . . . where the consent of the user of that service has been obtained." 18 U.S.C. § 3121(b)(3).[14] We believe that an EINSTEIN 2.0 Participant providing Internet service to its employees through government-owned information systems and its Federal Systems would qualify as a "provider of electronic . . . communication service" within the meaning of the Pen/Trap Act. *See supra* p. 98; 18 U.S.C. § 2510(15). Accordingly, the government would be exempt from the prohibitions of the Pen/Trap Act with respect to EINSTEIN 2.0 operations where the "consent" of the "user[s]" of their electronic communication service "has been obtained." With respect to both entities, we believe that the "user" whose consent needs to be obtained is the Executive Branch employee using a government-owned computer at an IP address that is subject to EINSTEIN 2.0 operations. For the same reasons discussed above we believe that EINSTEIN 2.0 Participants could obtain proper consent from their em-

[13] Title III of FISA also establishes a statutory basis for the government to obtain an authorization from the FISC to install a pen register or a trap-and-trace device in order to acquire certain foreign intelligence information. *See* 50 U.S.C. §§ 1841–1846 (2006 & Supp. II 2008). Under FISA, the terms "pen register" and "trap and trace device" have the same meanings as used in 18 U.S.C. § 3127(3) and (4). *See* 50 U.S.C. § 1841(2).

[14] The consent exception in section 3121(b)(3) also applies to the provisions in FISA authorizing the installation or use of such devices to acquire foreign intelligence information.

ployees under section 3121(b)(3) through the consistent adoption, implementation, and enforcement of appropriate log-on banners or computer-user agreements, as discussed in this memorandum. Therefore, we conclude that the deployment, testing, and use of EINSTEIN 2.0 technology would not constitute the unauthorized installation or use of a pen register or a trap-and-trace device under 18 U.S.C. § 3121(a).[15]

STEVEN G. BRADBURY
Principal Deputy Assistant Attorney General
Office of Legal Counsel

---

[15] EINSTEIN 2.0 operations also may fall within the "rights or property" exception to the Pen/Trap Act. Section 3121(b)(1) provides that the prohibitions of that Act do not apply with respect to the use of such technology "by a provider of electronic or wire communication service . . . relating to . . . the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service." 18 U.S.C. § 3121(b)(1).

We believe there is a strong argument that EINSTEIN 2.0 operations are subject to this "rights or property" exception. The rights or property exception in the Pen/Trap Act is more expansive than the parallel provisions in the Wiretap Act and the SCA. There is no requirement under the Pen/Trap Act provision that the action of a provider be "necessary" to protecting its rights or property. Furthermore, the Pen/Trap Act provision also permits a provider to protect not only its own rights or property, but also its users against "abuse of service or unlawful use of service." 18 U.S.C. § 3121(b)(1). Accordingly, under EINSTEIN 2.0 operations the government is protecting the Executive Branch "users" of the Internet service and the government's own rights and property. For these reasons and the reasons noted with respect to the narrower exception in the Wiretap Act, *see supra* Part III.A.2, we believe the rights or property exception to the Pen/Trap Act provides an additional basis to believe that EINSTEIN 2.0 operations are consistent with the Pen/Trap Act.