# LEGALITY OF INTRUSION-DETECTION SYSTEM TO PROTECT UNCLASSIFIED COMPUTER NETWORKS IN THE EXECUTIVE BRANCH

*Operation of the EINSTEIN 2.0 intrusion-detection system complies with the Fourth Amendment to the Constitution, title III of the Omnibus Crime Control and Safe Streets Act of 1968, the Foreign Intelligence Surveillance Act, the Stored Communications Act, and the pen register and trap and trace provisions of chapter 206 of title 18, United States Code, provided that certain log-on banners or computer-user agreements are consistently adopted, implemented, and enforced by executive departments and agencies using the system. Operation of the EINSTEIN 2.0 system also does not run afoul of state wiretapping or communications privacy laws.*

August 14, 2009

## MEMORANDUM OPINION FOR AN ASSOCIATE DEPUTY ATTORNEY GENERAL

This memorandum briefly summarizes the current views of the Office of Legal Counsel on the legality of the EINSTEIN 2.0 intrusion-detection system. This Office previously considered the legality of the system in an opinion of January 9, 2009. *See* Memorandum for Fred F. Fielding, Counsel to the President, from Steven G. Bradbury, Principal Deputy Assistant Attorney General, Office of Legal Counsel, *Re: Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection System (EINSTEIN 2.0) to Protect Unclassified Computer Networks in the Executive Branch* (Jan. 9, 2009) ("EINSTEIN 2.0 Opinion"). We have reviewed that opinion and agree that the operation of the EINSTEIN 2.0 program complies with the Fourth Amendment to the United States Constitution, title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 211, 18 U.S.C. § 2510 *et seq*. (2006), as amended ("the Wiretap Act"), the Foreign Intelligence Surveillance Act, Pub. L. No. 95-511, 92 Stat. 1783, 50 U.S.C. § 1801 *et seq*. (West Supp. 2009), as amended ("FISA"), the Stored Communications Act, Pub. L. No. 99-508, tit. II, 100 Stat. 1848 (1986), 18 U.S.C. § 2701(a)(1) (2006), as amended, and the pen register and trap and trace provision of title 18, United States Code, 18 U.S.C. § 3121 *et seq*. (2006), as amended. Accordingly, we have drawn upon the analysis in that opinion in preparing this summary, supplementing that material with analysis of an additional legal issue.

We have assumed for purposes of our analysis that computer users generally have a legitimate expectation of privacy in the content of Internet communications (such as an e-mail) while it is in transmission over the Internet.[1] *See, e.g.*, *United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004) (analogizing expectation of email user in privacy of email 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 email generally "enjoys a reasonable expectation that police officials will not intercept the transmission without probable cause and a search warrant"); *see*

[1] Computer users do not have an objectively reasonable expectation of privacy in 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, 510-11 (9th Cir. 2008); *cf. 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).

*also Quon*, 529 F.3d at 905 ("[U]sers do have a reasonable expectation of privacy in the content of their text messages vis-a-vis the service provider."). Even given this assumption, however, we believe the deployment, testing, and use of EINSTEIN 2.0 technology complies with the Fourth Amendment where each agency participating in the program consistently adopts, implements, and enforces the model log-on banner or model computer-user agreements described in this Office's prior opinion, or their substantial equivalents. *See* EINSTEIN 2.0 Opinion at 5-6.

First, we conclude that the adoption, implementation, and enforcement of model log-on banners or model computer-user agreements eliminates federal employees' reasonable expectation 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. We therefore do not believe that the operation of intrusion-detection sensors as part of the EINSTEIN 2.0 program constitutes a "search" for Fourth Amendment purposes. *See Minnesota v. Carter*, 525 U.S. 83, 88 (1998). Whether a Government employee has a legitimate expectation of privacy in his use of governmental property at work in particular circumstances 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 v. Ortega*, 480 U.S. 709, 717 (1987) (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."). The existence of an expectation of privacy, moreover, may depend on the nature of the intrusion at issue. *See O'Connor*, 480 U.S. at 717-18 (plurality) (suggesting that a government employee's expectation of privacy might be unreasonable "when an intrusion is by a supervisor" but reasonable when the intrusion is by a law enforcement official). The model banner and model computer-user agreement discussed in our prior opinion are at least as robust as—and we think stronger than—similar materials that courts have held eliminated a legitimate government employee expectation of privacy in the content of Internet communications sent over government systems. *See, e.g.*, *Simons*, 206 F.3d at 398 (finding no legitimate expectation of privacy in light of computer-use policy expressly noting that government agency 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'") (quoting policy); *United States v. Angevine*, 281 F.3d 1130, 1132-33 (10th Cir. 2002) (finding no legitimate expectation of privacy in light of computer-use policy stating that 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'") (quoting policy); *United States v. Thorn*, 375 F.3d 679, 682 (8th Cir. 2004), *vacated on other grounds*, 543 U.S. 1112 (2005) (finding no legitimate expectation of privacy in light of computer-use policy warning that employees "'*do not* have any personal privacy rights regarding their use of [the employing agency's] information systems and technology,'" and that "'[a]n 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'") (quoting policy). We therefore believe that the adoption, implementation, and enforcement of the language in those model materials, or their substantial equivalents, by agencies participating in the EINSTEIN 2.0 program will eliminate federal 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.[2]

We also believe that individuals in the private sector who communicate directly with federal employees of agencies participating in the EINSTEIN 2.0 program through Government-owned information systems do not have a legitimate expectation of privacy in the content of those communications provided that model log-on banners or agreements are adopted and implemented by the agency. The Supreme Court has repeatedly held 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); *see also United States v. Miller*, 425 U.S. 435, 443 (1976) ("[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."); *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984) ("[W]hen a person communicates information 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."). We believe this principle also applies to a person who emails a federal employee at the employee's personal email account when that employee accesses his or her personal email account through a Government-owned information system, when the consent procedures described above are followed. By clicking through the model log-on banner or agreeing to the terms of the model computer-user agreement, a federal 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," including the purpose of protecting federal computer systems against malicious network activity. Therefore, an individual who communicates with a federal 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 Amendment right against the Government activity of protecting federal computer systems against malicious network activity, as the employee has consented to that activity. *See Jerry T. O'Brien, Inc.*, 467 U.S. at 743; *Jacobsen*, 466 U.S. at 117; *Miller*, 425 U.S. at 443.

Under Supreme Court precedent, this principle applies even where, for example, the sender of an email to an employee's personal, Web-based email account (such as Gmail or Hotmail) does not know of the recipient's status as a federal employee or does not anticipate that the employee might read, on a federal Government system, an email sent to a personal email account at work or that the employee has agreed to Government monitoring of his communications on that system. A person communicating with another assumes the risk that the person has agreed to permit the Government to monitor the contents of that communication. *See*,

[2] 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 agency officials contradict these materials. *See Quon*, 529 F.3d at 906-07. Management officials of agencies participating in the EINSTEIN 2.0 program therefore should ensure that agency practices are consistent with the statements in the model materials.

*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); *cf. 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."). Accordingly, when 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 of the relevant agency through a Government-owned information system does not infringe upon any legitimate expectation of privacy of the parties to that communication.

We also think that, under the Court's precedents, an individual who submits information through the Internet to a federal agency participating in the EINSTEIN 2.0 program does not have a legitimate expectation of privacy for Fourth Amendment purposes in the contents of the information that he transmits directly to the participating 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). Further, as just discussed, 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. It follows a fortiori that where an individual is communicating directly with a declared agent of the Government, the individual does not have a legitimate expectation that his communication would not be monitored or acquired by the Government.

Second, even if EINSTEIN 2.0 operations were to constitute a "search" under the Fourth Amendment, we believe that those operations would be consistent with the Amendment's "central requirement" that all searches be reasonable. *Illinois v. McArthur*, 531 U.S. 326, 330 (2001) (internal quotation marks omitted). As discussed in the prior opinion of this Office, the Government has a lawful, work-related purpose for the use of EINSTEIN 2.0's intrusion-detection system that brings the EINSTEIN 2.0 program within the "special needs" exception to the Fourth Amendment's warrant and probable cause requirements. *See O'Connor*, 480 U.S. at 720 (plurality); *see also Nat'l Treasury Employees Union v. Von Raab*, 489 U.S. 656, 665-66 (1989) (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, 872-73 (1987) (special needs doctrine applies in circumstances that make the "warrant and probable cause requirement impracticable"); *United States v. Heckenkamp*, 482 F.3d 1142, 1148 (9th Cir. 2007) (preventing misuse of and damage to university computer network is a lawful purpose). And, based upon the information available to us, and as discussed in the prior opinion of this Office, we believe that the operation of the EINSTEIN 2.0 program falls under that exception and is reasonable under the totality of the circumstances. *See United States v. Knights*, 534 U.S. 112, 118-19 (2001) (reasonableness of a

search under the Fourth Amendment is measured in light of the "totality of the circumstances," balancing "on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests") (internal quotation marks omitted; *New Jersey v. T.L.O.*, 469 U.S. 325, 337 (1985) ("what is reasonable depends on the context within which a search takes place"); *O'Connor*, 480 U.S. at 726 (plurality) (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") (internal quotation marks omitted). In light of that conclusion, we also think that a federal employee's agreement to the terms of the model log-on banner or the model computer-user agreement, or those of a banner of user agreement that are substantially equivalent to those models, constitutes valid, voluntary consent to the reasonable scope of EINSTEIN 2.0 operations. *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"); *United States v. Sihler*, 562 F.2d 349 (5th Cir. 1977) (prison employee's consent to routine search of his lunch bag valid); *cf. 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.").

With respect to statutory issues, we have also concluded that, for the reasons set forth in our prior opinion—and so long as participating federal agencies consistently adopt, implement, and enforce model computer log-on banners or model computer-user agreements—the deployment of the EINSTEIN 2.0 program on federal information systems complies with the Wiretap Act, the Foreign Intelligence Surveillance Act, the Stored Communications Act, and the pen register and trap and trace provisions of title 18 of the United States Code. We agree with the analysis of these issues set forth in our prior opinion, and will not repeat it here.

Finally, we do not believe the EINSTEIN 2.0 program runs afoul of state wiretapping or communication privacy laws. *See, e.g.*,. Fla. Stat. Ann. § 934.03 (West Supp. 2009); 18 Pa. Cons. Stat. Ann. § 5704(4) (West Supp. 2009); Md. Code Ann., Cts. & Jud. Proc. § 10-402(c)(3) (LexisNexis 2006); Cal. Penal Code 631(a) (West 1999). To the extent that such laws purported to apply to the conduct of federal agencies and agents conducting EINSTEIN 2.0 operations and imposed requirements that exceeded those imposed by the federal statutes discussed above, they would "stand[] as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress," and be unenforceable under the Supremacy Clause. *Hines v. Davidowitz*, 312 U.S. 52, 67 (1941); *see also Geier v. American Honda Motor Co.*, 529 U.S. 861, 873 (2000) (same); *Old Dominion Branch v. Austin*, 418 U.S. 264, 273 n.5 (1974) (Executive Order "may create rights protected against inconsistent state laws through the Supremacy Clause"); *Bansal v. Russ*, 513 F. Supp. 2d 264, 283 (E.D. Pa. 2007) (concluding that "federal officers participating in a federal investigation are not required to follow" state wiretapping law containing additional requirements not present in the federal Wiretap Act, because in such circumstances, "the state law would stand as an obstacle to federal law enforcement"); *Johnson v. Maryland*, 254 U.S. 51 (1920); *cf. United States v. Adams*, 694 F.2d 200, 201 (9th Cir. 1980)

("evidence obtained from a consensual wiretap conforming to 18 U.S.C. § 2511(2)(c) is admissible in federal court proceedings without regard to state law").

/s/

DAVID J. BARRON
Acting Assistant Attorney General