BUILDING ON EXECUTIVE ORDER 13,636 TO ENCOURAGE INFORMATION SHARING FOR CYBERSECURITY PURPOSES

Over the past several decades, cybersecurity has emerged as an issue of increasing national concern.[1] Both government and private entities rely heavily on computer networks for functions related to defense, routine economic activity, and operation of critical infrastructure such as the electrical grid and the water supply.[2] At the same time, attacks on and exploitations of both commercial and government networks are increasing in number and sophistication.[3] Growing awareness of the threat and of U.S. vulnerability led a recent Secretary of Defense to conclude that the "collective result of these kinds of attacks could be a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life."[4] Perhaps the highest profile recognition of the issue to date is President Obama's warning in last year's State of the Union Address that cyber adversaries pose "real threats to our security and our economy."[5] The President coupled his warning with an announcement of increased executive action to combat these threats and a call for legislation to "give our Government a greater capacity to secure our networks and deter attacks."[6]Though recent disclosures regarding unrelated security programs may have lessened the political appetite for

---

1. *See, e.g.*, COMM. ON IMPROVING CYBERSECURITY RESEARCH IN THE U.S., NAT'L RESEARCH COUNCIL AND NAT'L ACAD. OF ENG'G, TOWARD A SAFER AND MORE SECURE CYBERSPACE 15–17 (Seymour E. Goodman & Herbert S. Lin, eds., 2007).

2. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-13-187, CYBERSECURITY: NATIONAL STRATEGY, ROLES, AND RESPONSIBILITIES NEED TO BE BETTER DEFINED AND MORE EFFECTIVELY IMPLEMENTED 3–12 (2013).

3. *Id.* For a particularly dramatic example, see MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS (2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf, [http://perma.cc/9H8D-2LMJ].

4. Leon E. Panetta, Sec'y, U.S. Dep't of Def., Remarks on Cybersecurity to the Business Executives for National Security (Oct. 11, 2012), *available at* http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136, [http://perma.cc/6LE3-5DGB].

5. Address Before a Joint Session of Congress on the State of the Union, 2013 DAILY COMP. PRES. DOC. NO. 00090, 9 (Feb. 12, 2013).

6. *Id.*

cybersecurity legislation, the threat has not abated.[7] This Note explores the call for legislation in light of Executive Order 13,636, "Improving Critical Infrastructure Cybersecurity."[8]

Part I briefly sets Executive Order 13,636 in the context of the federal government's expanding cybersecurity efforts. Part II turns to the Order itself, focusing on the Enhanced Cybersecurity Services (ECS) information-sharing program, its statutory authority, and its potential for further expansion. Significantly, unlike some programs that have recently been the cause of public concern,[9] ECS does not involve bulk collection of communications or associated metadata by the government. Parts III and IV examine whether the Fourth Amendment, the Wiretap Act, or the Pen Register and Trap and Trace Devices statute impose any constitutional or statutory restrictions on further expansion of ECS. Part V briefly considers two potential legislative approaches that would encourage additional sharing. Part VI concludes that Congress should act to encourage voluntary sharing.

I. THE FEDERAL GOVERNMENT'S EXPANDING CYBERSECURITY PRESENCE

Policymakers for years have recognized the threat to both federal and private networks from malicious cyber actors.[10] Because these networks are interdependent they cannot be effectively defended in isolation. As one defense official put it, "[s]ecure military networks will matter little if the power grid goes down . . . ."[11] Nevertheless, the federal government's

---

7. *See* Ken Dilanian, *NSA leaks halt defense plans; Experts say the U.S. is more vulnerable after the disclosure of spy tactics stalled cyber security initiatives*, L.A. TIMES, Feb. 2, 2014, at A15.

8. Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013) [hereinafter Cyber Order].

9. *See generally* PRESIDENT'S REVIEW GRP. ON INTELLIGENCE AND COMMC'NS TECH., LIBERTY AND SECURITY IN A CHANGING WORLD (2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf, [http://perma.cc/V7VE-HH6Q].

10. *See, e.g.*, COMM. ON IMPROVING CYBERSECURITY RESEARCH IN THE U.S., *supra* note 1, at 15–17.

11. William J. Lynn III, Deputy Sec'y, U.S. Dep't of Def., Remarks at the 2011 DISA Customer and Industry Forum (Aug. 16, 2011), *available at* http://www.defense.gov/transcripts/transcript.aspx?transcriptid=4863, [http://perma.cc/F276-MXGK].

earliest efforts to address cybersecurity focused on protecting national security systems.[12] Over the years Congress expanded that focus by providing various authorities intended to protect military networks,[13] federal networks generally,[14] and to some extent, private commercial networks.[15] Unfortunately, the degree to which these and other authorities are scattered about the executive branch creates difficulty in bringing them to bear on the cyber threat in a comprehensive manner.[16] The Bush Administration began to address this problem with the Comprehensive National Cybersecurity Initiative, which combined various cyber functions with traditional law enforcement, intelligence, counterintelligence, and military capabilities, in order to better protect federal networks.[17] Security experts urged the incoming Obama Administration to continue and expand these efforts, emphasizing the importance of private networks in the overall cybersecurity picture.[18] President Obama responded by declaring the nation's "digital infrastructure," including private commercial networks, to be "a strategic national asset."[19] In the four years following that announcement, Congress introduced numerous bills addressing

12. *See* National Security Directive 42 (July 5, 1990), *available at* http://www.fas.org/irp/offdocs/nsd/nsd42.pdf, [http://perma.cc/R4HY-8KE7].

13. 10 U.S.C. § 2224(a) (2006) (directing the Secretary of Defense "to protect and defend Department of Defense information, information systems, and information networks that are critical to the Department").

14. Federal Information Security Management Act of 2002, 44 U.S.C. §§ 3541–3549 (2006).

15. Homeland Security Act of 2002 § 223, 6 U.S.C. § 143 (2006).

16. EXEC. OFFICE OF THE PRESIDENT, CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE 7 (2009) (noting problem "harmoniz[ing] disparate responsibilities and authorities"), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf, [http://perma.cc/M6RF-v6F2].

17. *Id.* at 4–5.

18. *See, e.g.*, CTR. FOR STRATEGIC AND INT'L STUDIES, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY 15 (2008), *available at* http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf, [http://perma.cc/6A2J-B4NS].

19. Remarks on Securing the Nation's Information and Communications Infrastructure, 1 PUB. PAPERS 731, 733 (May 29, 2009).

cybersecurity, all of which failed to pass.[20] In February 2013, the Administration issued Executive Order 13,636.[21]

II. EXECUTIVE ORDER 13,636

Executive Order 13,636 primarily addresses two issues that relate to the protection of private networks: the expansion of an existing system of near real-time information sharing to privately operated critical infrastructure, and the creation of a "cybersecurity framework" which will recommend security standards for the private sector.[22] Both programs are "voluntary,"[23] though that may change, especially if Congress enacts new legislation on the subject.[24] This Note examines the information sharing program. The "framework" is outside this Note's scope.

A. The Enhanced Cybersecurity Services (ECS) Program

The Order contemplates two types of sharing. First, it directs the Secretary of Homeland Security and the Director of National Intelligence to establish a process for disseminating reports to

---

20 . Benjamin Wittes, *Allan Friedman on Why the Executive Order on Cyber*, LAWFARE (Feb. 14, 2013, 7:48 AM), http://www.lawfareblog.com/2013/02/allan-friedman-on-why-the-executive-order-on-cyber/, [http://perma.cc/LNG2-NAVB].

21. Cyber Order, *supra* note 8.

22. *See* Cyber Order, *supra* note 8; Michael Daniel, Special Ass't to the President and White House Cybersecurity Coordinator, *Improving the Security of the Nation's Critical Infrastructure*, THE WHITE HOUSE BLOG (Feb. 13, 2013, 6:39 PM), http://www.whitehouse.gov/blog/2013/02/13/improving-security-nation-s-critical-infrastructure/, [http://perma.cc/L89T-EGAH]. Daniel cites privacy as a third issue. *See id.*

23. Cyber Order, *supra* note 8, §§ 4, 8.

24. It is unclear whether the framework will remain voluntary even absent new legislation. The Order directs administrative agencies, and requests independent agencies, to assess whether they possess the regulatory authority to mandate the framework. *Id.* § 10. Relying on newly discovered authority, however, may be an overreach. *See, e.g.*, FDA v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 160 (2000) ("[W]e are confident that Congress could not have intended to delegate a decision of such economic and political significance [tobacco regulation] to an agency in so cryptic a fashion."). *But see* Massachusetts v. EPA, 549 U.S. 497, 531 (2007) (finding "nothing counterintuitive" in the exercise of previously undiscovered power to regulate CO2 emissions).

targeted entities.[25] Second, and more significantly, the Order directs the Secretary of Homeland Security, in coordination with the Secretary of Defense, to expand the Enhanced Cybersecurity Services (ECS) program to all critical infrastructure sectors.[26] This program originated as a Department of Defense (DoD) program to protect the Defense Industrial Base (DIB).[27]

Most critical infrastructure entities use cybersecurity providers (CSPs) to protect their networks.[28] ECS interfaces with those commercial providers—typically internet service providers (ISPs)—to augment their services with government cyber threat information.[29] The program "provides classified signatures to [appropriately cleared] firms or their ISPs to help counter known malicious cyber activity"[30] in "near real-time" using an automated process.[31] Signatures are "machine readable patterns of network traffic" deployed to detect and mitigate malicious cyber activity.[32] They are comprised of cyber threat "indicators," which are combinations of "data related to IP addresses, domains, e-mail headers, files, and strings" that identify such activity.[33] DoD has a

---

25. Cyber Order, *supra* note 8, § 4(a) (unclassified reports) & § 4(b) (classified reports); *see also* Exec. Order No. 13,549, 3 C.F.R. 234 (2010) (establishing program easing clearance process for state, local, tribal, and private sector entities).

26. Cyber Order, *supra* note 8, § 4(c).

27. U.S. DEP'T OF HOMELAND SEC., DHS/NPPD/PIA-028, PRIVACY IMPACT ASSESSMENT FOR THE ENHANCED CYBERSECURITY SERVICES 1–2 (2013), http://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_nppd_ecs_jan2013.pdf, [http://perma.cc/8ZUJ-ZXEK]; s*ee also* Lynn, *supra* note 11 (stating intent to bring DIB Pilot to critical infrastructure).

28. *Enhanced Cybersecurity Services*, U.S. DEP'T OF HOMELAND SEC., http://www.dhs.gov/enhanced-cybersecurity-services/, [http://perma.cc/GE56-D76J].

29. *Id.*

30. Michael Daniel, Special Ass't to the President & White House Cybersecurity Coordinator, 007 or DDoS: What is Real World Cyber? (Feb. 28, 2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-02-28_final_rsa_speech.pdf, [http://perma.cc/9P8B-6ZQ9].

31. WHITE HOUSE BLOG, *supra* note 22.

32. U.S. DEP'T OF HOMELAND SEC., *supra* note 27, at 2 & n.6; *see generally* KAREN SCARFONE & PETER MELL, NAT'L INST. OF STANDARDS & TECH., NIST SPECIAL PUBLICATION 800-94; GUIDE TO INTRUSION DETECTION AND PREVENTION SYSTEMS: RECOMMENDATIONS OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY 2-4 (2007), *available at* http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf, [http://perma.cc/T7BC-BT5S] (explaining signature-based detection).

33. U.S. DEP'T OF HOMELAND SEC., *supra* note 27, at 1 n.2. Depending on their source, indicators may be classified. *Id.*

role in providing cyber threat indicators and signatures that it obtains and develops through its foreign intelligence mission.[34]

Providing signatures that counter threats makes ECS much more significant than an increase in reporting. Reports require human action to interpret them and respond. ECS enables privately operated networks to benefit from confidential government information, including classified foreign intelligence, in real time through a system that makes it useable and protects it from disclosure. The difference is the difference between receiving a notice of an attack after the fact and being able to stop an attack before it succeeds.[35]

B. Scope of Statutory Authority for ECS

The Order explicitly grounds its authority for expanding ECS to the private sector in 6 U.S.C. § 143.[36] Section 143 authorizes the Department of Homeland Security (DHS) to provide "as appropriate . . . and upon request . . . analysis and warnings related to threats to, and vulnerabilities of, critical information systems" to private entities that own or operate such systems.[37] This language easily encompasses signature sharing by the government with the private sector. It does not, however, authorize DHS to mandate private sector participation. On the contrary, the phrase "upon request"[38] suggests any such mandate is forbidden.[39] The section is silent regarding government receipt of information.[40] Other provisions of the Homeland Security Act, however, reflect an assumption that, in general, DHS is not

---

34. *See* Cyber Order, *supra* note 8, § 4(c); Lynn, *supra* note 11, ("[C]lassified threat intelligence is shared with defense contractors or their commercial internet service providers along with the know-how to employ it in network defense.").

35. *Cf.* Lynn, *supra* note 11 (explaining—in context of DoD networks—the difference between "passive defenses that employ only after-the-fact detection and notification," and "[a]ctive defenses [that] operate at network speed, using sensors, software, and signatures derived from intelligence to detect and stop malicious code before it succeeds").

36. *See* Cyber Order, *supra* note 8, § 4(c).

37. Homeland Security Act of 2002 § 223, 6 U.S.C. § 143, (2006) ("Enhancement of non-Federal cybersecurity").

38. *Id.*

39. *See, e.g.*, Corley v. United States, 556 U.S. 303, 314 (2009) ("[A] statute should be construed so that effect is given to all its provisions, so that no part will be inoperative or superfluous, void or insignificant.") (internal citations omitted).

40. *See* 6 U.S.C. § 143.

precluded from receiving information pertaining to critical infrastructure that is "voluntarily shared" by private entities.[41]

C. Potential for Further Expansion of ECS

As currently structured, ECS is primarily a mechanism for the sharing of government cybersecurity information with the private sector on a voluntary basis. Absent from the Executive Order is any mention of sharing of information from the private sector to the government.[42] Yet the government is interested in receiving cybersecurity information from the private sector.[43] In 2012, General Alexander, head of both the National Security Agency and U.S. Cyber Command, explained the kind of information the government would like to receive from private-sector critical infrastructure entities.[44] Discussing a hypothetical where people in various critical infrastructure sectors received e-mails containing malicious code, Alexander emphasized that the government would not want to receive the contents of such e-mails.[45] Rather, the government would want technical information including the signature involved, and the IP addresses and ports transited.[46] According to Alexander, this

---

41. *See* 6 U.S.C. § 133(a) (prescribing rules for handling). "Voluntary" means any sharing not compelled. § 131(7)(A).

42. *See* Cyber Order, *supra* note 8. Some "anonymized information" is shared with the government, however. *See Enhanced Cybersecurity Services*, *supra* note 28.

43. Officials speak of expanding the program. *See* Daniel, *supra* note 30, ("[W]e will continue to support congressional action . . . that . . . increase[es] information sharing. . . ."). An early draft of the Order requested that the private sector share certain information with the government. *See* White House Memorandum, Paper Deputies Committee Meeting on Executive Order on Improving Critical Infrastructure Cybersecurity Practices (Sept. 28, 2012), *available at* http://www.lawfareblog.com/wp-content/uploads/2012/11/White-House-Draft-Executive-Order-Publicly-Circulating-Copy-11-1-12.pdf, [http://perma/cc/8MMV-ZMZD]. Additionally, major legislative proposals have addressed such sharing. *See* THE HERITAGE FOUND., FACTSHEET NO. 110, COMPARISON OF CYBERSECURITY LEGISLATION 1–2 (2012), *available at* http://www.heritage.org/research/factsheets/2012/07/updated-comparison-of-cybersecurity-legislation, [http://perma.cc/X2BL-JTDN] (contrasting sharing provisions).

44. Gen. Keith B. Alexander, Commander, U.S. Cyber Command, Dir., Nat'l Sec. Agency, Remarks on Cybersecurity and American Power, (July 9, 2012), *available at* http://www.aei.org/events/2012/07/09/cybersecurity-and-american-power/, [http://perma.cc/V498-SGEX].

45. *Id*.

46. *Id.*; *see also* Ellen Nakashima, *Cybersecurity chief urges action by Congress*, WASH. POST POLITICS BLOG (July 10, 2012, 8:00 AM), http://www.washingtonpost.com/

type of information would allow the government to figure out if the country were under attack, and how to respond.[47] Because only "hits" would be shared, the government would not collect communications or associated metadata in bulk.[48]

III. FOURTH AMENDMENT CONSTRAINTS ON INFORMATION SHARING

Expansion of ECS to accommodate information sharing from the private sector to the federal government potentially implicates the Fourth Amendment. The Fourth Amendment prohibits the government from conducting "unreasonable searches and seizures."[49] In the context of electronic communications, a "search" occurs when monitoring violates a "reasonable expectation of privacy."[50] The prohibition on unreasonable searches extends to private entities when they act as agents of the government.[51] Courts have implied a number of exceptions to the general prohibition.[52] Subparts A and B consider whether actions pursuant to the ECS program are searches and whether participating providers are agents of the government. Subpart C considers the applicability of three exceptions.

A. Electronic Searches

In *Katz v. United States*, the Supreme Court held there is a reasonable expectation of privacy in the contents of telephone conversations.[53] By contrast, in *Smith v. Maryland*,[54] the Court held there is no such expectation of privacy in phone numbers dialed.[55] The Court justified this distinction between content

---

blogs/2chambers/post/cybersecurity-chief-urges-action-by-congress/2012/07/09/gJQAP4gMZW_blog.html, [http://perma/cc/SYB3-VC5S] (describing remarks).

47. Alexander, *supra* note 44.

48. *Id.*; *cf.* PRESIDENT'S REVIEW GRP. ON INTELLIGENCE AND COMMC'NS TECH., *supra* note 9, at 17 (criticizing government collection and storage of telephony metadata in bulk).

49. U.S. CONST. amend. IV.

50. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

51. *See, e.g.*, Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 614 (1989).

52. *See, e.g.*, Kentucky v. King, 131 S. Ct. 1849, 1856 (2011).

53. *See* 389 U.S. at 360 (Harlan, J., concurring).

54. 442 U.S. 735 (1979).

55. *Id.* at 745–46 (holding police use of pen register does not violate Fourth Amendment).

and addressing information on the basis of the third-party doctrine.[56] It reasoned that "[a]lthough petitioner's conduct may have been calculated to keep the *contents* of his conversation private, [it] could not have been calculated to preserve the privacy of the number he dialed" because he knew the phone company would use it to complete the call.[57] Courts applying *Smith* to e-mail and other online communications have held that addressing information used by ISPs for routing purposes is non-content outside the Fourth Amendment's protection.[58] Non-routing information, such as the subject lines and bodies of e-mails, has generally been held to be content within the protection of the Amendment.[59]

The information the government has expressed interest in receiving through ECS is limited to addressing and routing information.[60] This information does not implicate the Fourth Amendment. According to DHS, however, the scans of network traffic that generate this information may not be as limited.[61] This depends on how signatures are constructed.[62] Recall that signatures are comprised of indicators, and that indicators may

---

56. *Id.* at 743–44. This distinction echoes the Court's longstanding approach to the mail. *See Ex parte* Jackson, 96 U.S. 727, 733 (1877) ("Letters and sealed packages . . . are . . . fully guarded from examination and inspection, except as to their outward form and weight. . . .").

57. *Smith*, 442 U.S. at 743–44.

58. *See, e.g.*, United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (holding computer surveillance collecting e-mail headers and IP addresses "constitutionally indistinguishable from the use of a pen register"). A recent district court opinion held in an analogous context that aggregation and retention of metadata in large volumes likely violates the Fourth Amendment. *See* Klayman v. Obama, No. 13-0851, slip op. at 46–47 (D.D.C. Dec. 16, 2013) (addressing NSA Bulk Telephony Metadata Program). The decision is on appeal.

59. *See, e.g.*, United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (holding "a subscriber enjoys a reasonable expectation of privacy in the *contents* of e-mails" (emphasis added)).

60. Alexander, *supra* note 44, (expressing desire for IP addresses and port numbers); *cf.* EXEC. OFFICE OF THE PRESIDENT, THE COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE 3 (2009), http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf, [http://perma.cc/L8YY-HD4N] (explaining EINSTEIN system for federal networks "send[s] alerts that do not contain the content of communications to the National Security Agency").

61. *See* U.S. DEP'T OF HOMELAND SEC., *supra* note 27, at 8.

62. *See* SCARFONE & MELL, *supra* note 32, at 2-4 (providing examples of signature construction).

include text strings.[63] If these strings are located in the body or subject line of an e-mail,[64] courts will consider them contents. This creates at least two problems for ECS. First, as part of identifying relevant non-content information, the private-sector ISP may scan the contents of the communication. If the ISP is acting as an agent of the government[65] the scan itself is potentially problematic. Second, apart from the scan itself, sharing the fact of a positive hit on a particular signature could result in disclosure of communications content by implication. Suppose, for example, that "signature A" triggers on the combined presence of three indicators: a sender's e-mail address, a port number, and a content string in the body of the e-mail.[66] If an ISP were to report to the government that "signature A" triggered on a particular message, the government could infer the presence of the content string from the design of the signature.

A potential solution is not to use content-based indicators in signatures. This, however, may not be practical. Presumably, the ability to include content indicators in a signature is useful. Sometimes malicious code is embedded in the body of an e-mail.[67] Other times it may be that the best indicator is a particular content string.[68] Moreover, if treated as a necessary rather than sufficient condition, adding an additional indicator to a signature lowers the risk of a false positive. As a result, it is unlikely DHS would consider a blanket policy of not using content-based indicators in signatures a plausible option. Accordingly, it is likely that some signatures will be constructed in this manner. Thus, a court very likely would consider scanning in the context of the ECS program to be a search under the Fourth Amendment.

---

63. U.S. DEP'T OF HOMELAND SEC., *supra* note 27, at 2–3.

64. *Id.* at 8 (noting indicators for e-mail subject lines).

65. *See infra* Part III. B.

66. U.S. DEP'T OF HOMELAND SEC., *supra* note 27, at 4 (describing similar indicator combinations).

67. U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR EINSTEIN 2 15 (2008) http://www.dhs.gov /xlibrary/assets/privacy/privacy_pia_einstein2.pdf, [http://perma.cc/PX7P-C4VP] (explaining that "sometimes the malicious payload is hidden and delivered via the content (or body) of the e-mail").

68. For example, the infamous "I love you" worm contained an eponymous text string in the e-mail message. *Return to Sender*, ECONOMIST, May 11, 2000, http://www.economist.com/node/308454, [http://perma.cc/5FXL-H4DQ].

B. Agents of the Government

The Fourth Amendment does not restrict private searches unless the party carrying out the search is an agent of the government. [69] Compelling a search destroys its private character.[70] However, "[t]he fact that the Government has not compelled a private party to perform a search does not, by itself, establish that the search is a private one."[71] Rather, the question turns on the degree of government involvement "in light of all the circumstances."[72] Federal appellate courts have held private parties to be agents of the government when "the government knew of and acquiesced in the intrusive conduct" and "the party performing the search intended to assist law enforcement efforts [rather than] further his own ends."[73]

For example, in *United States v. Souza*, the Tenth Circuit held that an employee of a private shipping company acted as an agent of the government when a DEA agent present at the shipper's facility selected and removed a package from a moving conveyor belt, alerted a company employee to its location, and helped the employee open the package. [74] The court acknowledged the company's "legitimate reasons to search packages independent of any motivation to assist police," but found no evidence of an independent motivation on the record before it.[75] By contrast, in *United States v. Momoh*, the First Circuit held that the existence of an FAA regulation that subjected packages from unregistered senders to opening and inspection did not by itself support the conclusion that an employee of a private shipping company who opened a package pursuant to the regulation was acting as an agent of the government.[76] The court reasoned, "[I]t may well have been a concern with 'safeguarding life and property,' or a concern about 'carrying contraband,' rather than its desire to

69. *See, e.g.*, United States v. Jacobsen, 466 U.S. 109, 113 (1984).

70. *See* Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 614 (1989).

71. *Id.* at 615.

72. *Id.* at 614 (quoting Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971)).

73. United States v. Souza, 223 F.3d 1197, 1201 (10th Cir. 2000); *see also* United States v. Momoh, 427 F.3d 137, 141 (1st Cir. 2005) (applying same standard as factors rather than two-part test).

74. *Souza*, 223 F.3d at 1202 (finding "no evidence [of] a legitimate, independent motivation to open the package").

75. *Id.*

76. *Momoh*, 427 F.3d at 142.

conform to FAA regulations, that led [the carrier] to inspect [the] package."[77] Taken together, these examples suggest that when a private party maintains a strong enough independent interest in a search, it will not be deemed an agent of the government, even where the search may also serve a government interest.

As currently implemented through the Executive Order, the ECS program very likely does not make service providers agents of the government. The government "knows" and "acquiesces" to activities that likely constitute private searches. As in *Momoh*, however, the service providers possess an independent motivation for engaging in the conduct. ECS provides ISPs with classified foreign intelligence that supplements a service for which they charge their clients. Arguably this makes the service more valuable. Additionally, as the *Momoh* court acknowledged, carriers have an independent interest in ensuring their services are not used illegally.[78] ISPs routinely act on this interest apart from government intervention by scanning their networks for the presence of child pornography and illegal file sharing.[79] Thus, because the providers are acting to further their own ends, they very likely are not agents of the government.

The question would become closer if the ECS program were modified to accommodate voluntary ISP sharing of information with the government. There, the government's knowledge of and acquiescence in the private-party action would be greater: In addition to providing signatures, the government would be signaling its willingness to receive any results from those signatures. Courts are often suspicious when a purportedly private search follows government encouragement.[80] Thus, a court could look at the information sharing mechanism, conclude that the search is intended primarily to benefit the government, and hold that it is no longer private. Such a holding would likely be incorrect, however. First, the government's creation of an

---

77. *Id.*; *see also* United States v. Richardson, 607 F.3d 357, 367 (4th Cir. 2010) (holding ISP not an agent of the government when it scanned user's e-mail for child pornography and subsequently reported it as required by reporting law).

78. 427 F.3d at 142; *see also* Illinois v. Andreas, 463 U.S. 765, 769 n.1 (1983) ("Common carriers have a common-law right to inspect packages they accept for shipment, based on their duty to refrain from carrying contraband.").

79. *See Richardson*, 607 F.3d at 363.

80. *See, e.g.*, *Souza*, 223 F.3d at 1202.

additional sharing mechanism would not diminish an ISP's independent interest in providing government signatures to their customers. The presence of a feedback loop might even increase the value of the government signatures to the ISP if it led to an improvement in quality. Second, an ISP's independent interest in ensuring its services are not used illegally would not be reduced. Thus, a court should hold that the search is a private one.

C. Exceptions

Even if activities conducted pursuant to the ECS program constitute a search, and even if participation in these activities made private ISPs government agents, it would not necessarily follow that the program violates the Fourth Amendment. As noted above, the Fourth Amendment's prohibition "is subject to certain reasonable exceptions."[81] One such exception is a search conducted with consent.[82] Federal courts have held computer-use policies implemented with click-through banners sufficient to eliminate any expectation of privacy.[83] Under the ECS program, ISPs only provide the supplemental protection from government signatures to critical infrastructure customers who purchase that service.[84] In theory at least, the program could require that those customers implement click-through banners notifying users that the systems are subject to search.[85] Assuming the language of the

81. Kentucky v. King, 131 S. Ct. 1849, 1856 (2011).

82. *See, e.g.*, Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973).

83. *See, e.g.*, United States v. Angevine, 281 F.3d 1130, 1135 (10th Cir. 2002) (holding log-in banner eliminated professor's expectation of privacy in use of state university computers). *But see* City of Ontario v. Quon, 130 S. Ct. 2619, 2629 (2010) (leaving unresolved whether "operational realities" contradicting computer-use policy could render it ineffective); *cf.* United States v. Nosal, 676 F.3d 854, 861–63 (9th Cir. 2012) (questioning efficacy of "terms of service" agreements to support prosecution under Computer Fraud and Abuse Act for exceeding authorized access). A click-through banner is typically implemented as a pop-up window that a user must acknowledge ("click") before gaining access to the system.

84. *Enhanced Cybersecurity Services*, *supra* note 28.

85. This is the mechanism the government relies on to conduct searches on its own networks. *See* Legality of Intrusion-Detection Sys. to Protect Unclassified Computer Networks in the Exec. Branch, 2009 WL 3029764 at *1–3 (Op. O.L.C. Aug. 14, 2009). Whether it would pose implementation or other challenges in the private sector is beyond the scope of this Note.

banner was sufficient to obtain the proper scope of consent, a search very likely would be permissible.[86]

Alternatively, it is arguable that signatures that detect only unlawful activity would not constitute a search at all.[87] For example, in *Illinois v. Caballes*,[88] the Supreme Court reaffirmed its earlier holding that the use of a well-trained narcotics dog does not implicate a legitimate privacy interest because it "'does not expose noncontraband items that otherwise would remain hidden from public view.'"[89] This is true even though the dog may sometimes generate false positives.[90] Whether the Court would extend that rationale by analogizing a packet sniff that reveals the presence of malicious code to a dog sniff that reveals the presence of drugs or explosives is uncertain. They are at least similar in that in both instances no information is revealed to a human until an alert is generated. In the context of e-mail and other internet communication, this may in fact be the touchstone concern.[91] Thus, while the issue would be one of first impression, a court could conclude that automated scanning through the use of signatures designed to detect only unlawful activity is not a search.[92]

---

86. *See* United States v. Dichiarinte, 445 F.2d 126, 129 (7th Cir. 1971) ("A consent search is reasonable only if kept within the bounds of the actual consent.").

87. *See* United States v. Jacobsen, 466 U.S. 109, 123 (1984) (holding government chemical test "reveal[ing] whether a substance is cocaine, and no other arguably 'private' fact, compromises no legitimate privacy interest").

88. 543 U.S. 405 (2005).

89. 543 U.S. 405, 409 (2005) (quoting United States v. Place, 462 U.S. 696, 707 (1983)). The Court's recent decision in *Florida v. Jardines* does not impact this analysis as that case turned on the fact that the dog sniff took place in the home. *See* 133 S. Ct. 1409, 1417 (2013); *id.* at 1419 n. 1 (Kagan, J., concurring). Network scanning does not take place in the home.

90. *Caballes*, 543 U.S. at 409.

91. *Compare* Richard Perez Pena, *Harvard Search of E-Mail Stuns Its Faculty Members*, N.Y. TIMES, Mar. 10, 2013, at A3 (reporting faculty outrage at manual e-mail searches by system administrators), *with* Abby Ellin, *Lawsuit: Gmail, Yahoo E-mail Invade Privacy, Even Non-Users*, ABC NEWS, July 2, 2012, http://abcnews.go.com/Business/lawsuit-gmail-yahoo-invade-privacy-email-account/story?id=16680463, [http://perma.cc/L9BV-K8TC] (noting "most of us" have accepted automated scanning of personal e-mail to generate advertising).

92. *Cf.* CHRISTOPHER SLOBOGIN, BROOKINGS INST., IS THE FOURTH AMENDMENT RELEVANT IN A TECHNOLOGICAL AGE? 6 (2010), http://www.brookings.edu/~/media/research/files/papers/2010/12/08%204th%20amendment%20slobogin/1208_4th_amendment_slobogin.pdf, [http://perma.cc/AZU4-6DLT] (noting the

Finally, government monitoring of internet communications for cybersecurity purposes may be permissible under the "special needs" doctrine.[93] Under the doctrine, "[a] judicial warrant and probable cause are not needed where the search or seizure is justified by 'special needs, beyond the normal need for law enforcement'"[94] and obtaining the warrant is "impracticable."[95] Courts have applied this doctrine in national security and terrorism cases. For example, in *Cassidy v. Chertoff*,[96] then-Judge Sotomayor upheld searches of ferry passengers' baggage, reasoning that "[p]reventing or deterring large-scale terrorist attacks present[s] problems that are distinct from standard law enforcement needs and indeed go well beyond them."[97] Here, the limitation of the ECS program to critical infrastructure entities who obtain services through an ISP may be analogous to the performance of searches in narrow contexts such as boarding a ferry. Even if ECS were implemented more broadly, that would not necessarily pose a problem. As one scholar has noted, "the logic of [the special needs] cases applies pretty straightforwardly to the cybersecurity situation."[98]

In sum, even if the ECS program constitutes a search, and even if it made private ISPs government agents, the program likely would not run afoul of the Fourth Amendment so long as the search is consented to, does not reveal activity beyond wrongdoing, or is justified by special needs. Thus, the Fourth Amendment is unlikely to bar expansion of the ECS program

---

acceptance of "mechanical dogs" in the form of airport sniffers that identify weapons and contraband).

93. *Id.* at 8–9; s*ee also* JACK GOLDSMITH, BROOKINGS INST., THE CYBERTHREAT, GOVERNMENT NETWORK OPERATIONS, AND THE FOURTH AMENDMENT 12 (2010), http://www.brookings.edu/~/media/research/files/papers/2010/12/08%204th%20amendment%20goldsmith/1208_4th_amendment_goldsmith, [http://perma.cc/CCC3-URVM].

94. Ashcroft v. al-Kidd, 131 S. Ct. 2074, 2081 (2011) (quoting Veronica Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995)).

95. *See* New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring).

96. 471 F.3d 67 (2d Cir. 2006).

97. 471 F.3d at 82; *see also* MacWade v. Kelly, 460 F.3d 260–63 (2d Cir. 2006) (special need in preventing subway bombing justifies suspicionless baggage searches); Nicholas v. Goord, 430 F.3d 652, 668 (2d Cir. 2005) (special need justifies assembling DNA database); *In re* Directives Pursuant to Section 105B of FISA, 551 F.3d 1004–06 (FISA Ct. Rev. 2008) (special need in foreign intelligence justifies warrantless collection subject to certain safeguards).

98. GOLDSMITH, *supra* note 93, at 13.

to accommodate information sharing from the private sector to the federal government.

IV. STATUTORY CONSTRAINTS ON INFORMATION SHARING

Statutory restrictions on information sharing track the constitutional distinction between content and addressing information discussed in the previous section.[99] The Wiretap Act covers interception of communications content,[100] and the Pen Register and Trap and Trace Devices (Pen-Trap) statute covers collection of non-content addressing information.[101] Violation of the Wiretap Act creates a private right of action,[102] and violation of either statute can result in criminal liability.[103] Because signatures can be constructed to include or avoid contents, both statutes are relevant.

A. The Wiretap Act

The Wiretap Act prohibits the intentional interception, use, or disclosure of electronic communications.[104] "Electronic communications" includes internet communications.[105] An "intercept" is the acquisition of the contents of such communications,[106] contemporaneous with transmission.[107] As discussed previously, ISPs scan data as it transits the network.

---

99. *See* United States Telecom Ass'n v. FCC, 227 F.3d 450, 453–54 (D.C. Cir. 2000) (explaining statutory structure).

100. 18 U.S.C. §§ 2510–2522 (2006).

101. 18 U.S.C. §§ 3121–3127.

102. 18 U.S.C. § 2520.

103. 18 U.S.C. §§ 2511(4), 3121(d).

104. 18 U.S.C. § 2511(1). The prohibition also covers "oral" and "wire" communications. *See id*.

105. *See* 18 U.S.C. § 2510(12) (defining term broadly); Kirch v. Embarq Mgmt. Co., 702 F.3d 1245, 1246 (10th Cir. 2012) ("Traffic on the Internet is electronic communication.").

106. 18 U.S.C. § 2510(4). "Contents" is defined as "any information concerning the substance, purport, or meaning" of the communication. 18 U.S.C. § 2510(8).

107. *See, e.g.*, United States v. Steiger, 318 F.3d 1039, 1048–49 (11th Cir. 2003) (inferring contemporaneous requirement from statutory structure and noting agreement of Fifth and Ninth Circuits). *But see* United States v. Councilman, 418 F.3d 67, 80 (1st. Cir. 2005) (en banc) (suggesting, but not deciding, there may not be a "contemporaneity or real-time requirement").

Thus, if contents-based signatures are used, then contents are intercepted within the meaning of the statute.

1. Exceptions to the Prohibition of the Wiretap Act

The Wiretap Act's prohibition is subject to a number of exceptions. Potentially relevant are the consent and provider exceptions, as well as the ordinary business exclusion. The consent exception applies where a "part[y] to the communication . . . has given prior consent to such interception."[108] As in the Fourth Amendment context,[109] a properly worded click-through banner would likely be sufficient.[110] Thus, in theory at least, consent could be obtained sufficient to remove any prohibition of the Wiretap Act.

The provider exception allows a provider to "intercept, disclose, or use" the contents of communications "in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service."[111] Cases applying the exception have generally involved a provider's protection of itself—as opposed to third parties such as customers—from the misuse.[112] As a result, the emphasis in these cases is on the "rights or property" clause of the exception.[113] The Office of Legal Counsel concludes from this that the exception "must protect the provider's own rights or property, and not those of any third party, such as a customer."[114] This interpretation would permit ISPs to

---

108. 18 U.S.C. § 2511(2)(c)–(d).

109. *See supra* Part III. C.

110. *See, e.g.*, United States v. Caceres, 440 U.S. 741, 750 (1979) (noting the Wiretap Act "impose[s] no restrictions on recording a conversation with the consent of one of the conversants").

111. 18 U.S.C. § 2511(2)(a)(i).

112. *See, e.g.*, United States v. Mullins, 992 F.2d 1472, 1478 (9th Cir. 1993) (holding airline within rights or property exception when monitoring users engaged in theft of frequent flier miles over proprietary network).

113. *See, e.g.*, Campiti v. Walonis, 611 F.2d 387, 393 (1st Cir. 1979) (holding exception not applicable when the person is "not an agent of the telephone company and the monitoring had nothing to do with telephone company equipment or rights").

114. Legal Issues Relating to the Testing, Use, & Deployment of an Intrusion-Detection Sys. (Einstein 2.0) to Protect Unclassified Computer Networks in the Exec. Branch, 2009 WL 3029765, at *24 (Op. O.L.C. Jan. 9, 2009) (dictum).

"intercept" or "disclose" information using signatures that identify and mitigate malicious network activity potentially targeting the ISP itself. But it would not permit use of signatures concerned solely with threats to other critical infrastructure.

There are valid reasons, however, to question whether the OLC's reading of the provider exception is broad enough. In the appellate cases OLC cites, a provider's right to protect only its customers was not at issue.[115] Nor was it at issue on the facts for which OLC rendered its opinion.[116] Moreover, textually, the disjunctive article "or" separates the "rights and property" clause from the preceding clause, which states an exception for "any activity which is a necessary incident to the rendition of [the] service."[117] This suggests that the two clauses set forth independent instances of the exception. Finally, the Supreme Court appears to have endorsed, in dictum, a reading of the exception that would permit any normal business practice.[118] Nevertheless, as no court appears to have directly considered whether a provider may act to protect only its customers, relying on a broad reading is not without some legal risk.

2. *An Exclusion from the Prohibition of the Wiretap Act*

In addition to the consent and provider exceptions, the Wiretap Act contains an exclusion that removes from the definition of "intercept" acquisition by the provider during "the ordinary course of its business."[119] Courts have held that ISPs' access to e-mails and other internet traffic for legitimate business reasons falls within the ordinary business exclusion.[120] Scanning network

---

115. *See Campiti*, 611 F.2d at 393; United States v. Auler, 539 F.2d 642, 644–45 (7th Cir. 1976).

116. 2009 WL 3029765, s*upra* note 114, at *24.

117. 18 U.S.C. § 2511(2)(a)(i) (2006).

118. United States v. New York Tel. Co., 434 U.S. 159, 168 n.13 (1977) (stating the provider exception "specifically excludes all normal telephone company business practices from the prohibitions of the Act").

119. *See* 18 U.S.C. § 2510(4) (defining intercept as the "acquisition of the contents of any . . . communication" through use of an "electronic, mechanical or other device"); 18 U.S.C. § 2510(5)(a)(ii) (excluding from the definition of "electronic, mechanical or other device" any equipment "used by a provider of wire or electronic communication service in the ordinary course of its business").

120. *See* Kirch v. Embarq Mgmt. Co., 702 F.3d 1245, 1247–50 (10th Cir. 2012) (holding no interception occurred where ISP monitored user behavior to generate advertising). *Compare* Hall v. EarthLink Network, Inc., 396 F.3d 500, 505 (2d Cir. 2005) (no

traffic for malicious indicators would seem to be very much within the "ordinary course of business" of an ISP providing cybersecurity services. Thus, the exclusion permits ISPs to use government signatures to scan communications content. Unlike the provider exception discussed above, here there is no concern regarding signatures intended to protect customers.

Relevant in the context of the exclusion, another provision of the statute says that a service provider "shall not intentionally divulge the contents of any communication . . . while in transmission on that service."[121] The prohibition on divulging contents includes two relevant exceptions: first, a cross-reference to the provider exception discussed above;[122] second, another consent exception.[123] In the case of the consent exception, the language is similar to that discussed above, and the same analysis applies.[124] In the case of the provider exception, there is a twist on the previous analysis resulting from the separation of the exclusion and the prohibition on divulging.[125] Whereas in the context of the general prohibition any ambiguity regarding the scope of the provider exception calls into question the permissibility of both interception and disclosure, in the context of the exclusion only the prohibition on divulging is affected by this ambiguity.

To sum up, the Wiretap Act permits ISPs to scan their networks using government signatures obtained through ECS. Absent consent, however, under either the exceptions or the exclusion there is legal ambiguity regarding the scope of permissible disclosure to the government for purposes other than self-protection by the provider. Thus, even though the Wiretap Act permits ISP use of ECS signatures, ambiguity

---

interception when ISP "continue[d] to receive and store e-mails on the server[]" after an account was cancelled), *with* United States v. Councilman, 418 F.3d 67, 70–71 (1st Cir. 2005) (en banc) (interception occurred when ISP employee diverted e-mails to personal inbox "in the hope of gaining a commercial advantage").

121. 18 U.S.C. § 2511(3)(a).

122. 18 U.S.C. § 2511(3)(b)(i) (permitting disclosure "as otherwise authorized in section 2511(2)(a) or 2517").

123. 18 U.S.C. § 2511(3)(b)(ii).

124. *See id.* (provider may divulge "with the lawful consent of the originator or any addressee or intended recipient of such communication").

125. *Compare* 18 U.S.C. § 2510(5)(a)(ii) (exclusion), *with* 18 U.S.C. § 2511(3)(a) (prohibition on divulging).

regarding the scope of permissible disclosure means there is some legal risk to ISPs if they were to share results with DHS.

B. The Pen-Trap Statute

Following the Court's decision in *Smith* that non-content information was unprotected by the Fourth Amendment, Congress enacted, and President Reagan signed, a prohibition on the use of pen registers or trap and trace (pen-trap) devices without a court order.[126] The definition of such devices has since been amended expressly to embrace all forms of electronic communication (as opposed to telephone communication only).[127] The Pen-Trap statute includes several broad exceptions that permit service providers to use pen-trap devices on their networks.[128] Unlike the Wiretap Act however, the statute is silent regarding voluntary disclosure of information obtained under these exceptions.

1. Exceptions to the Prohibition on Pen-Trap Devices

The Pen-Trap statute's exceptions permit service providers to use pen-trap devices to, among other things, protect their own "rights or property,"[129] or to protect "user[s] of [the] service from . . . unlawful or abusive use of service."[130] The purpose of using signatures to scan network traffic is to protect the network and its users from malicious activity. Thus, ISPs participating in ECS fit comfortably into these exceptions, and may use government signatures to scan addressing information on their networks.

---

126 . *See* Electronic Communications Privacy Act of 1986 § 301, 18 U.S.C. §§ 3121–3127 (2006).

127. *See* 18 U.S.C. § 3127(3)–(4). A pen register records outgoing addressing information. 18 U.S.C. § 3127(3). A trap and trace device records incoming addressing information. 18 U.S.C. § 3127(4).

128. *See* 18 U.S.C. § 3121(b)(1)–(3).

129. 18 U.S.C. § 3121(b)(1).

130. 18 U.S.C. § 3121 (b)(2) (internal punctuation omitted). Additionally, just as with the Fourth Amendment and the Wiretap Act, consent removes the prohibition. *See* § 3121(b)(3).

2. Disclosure of Pen-Trap Information

Whether the Pen-Trap statute would permit ISPs to voluntarily share pen-trap information with the government is somewhat less clear. As noted above, the statute is silent regarding voluntary disclosure of information collected under its exceptions. This stands in contrast to the Wiretap Act,[131] as well as to the Stored Communications Act (SCA),[132] the latter of which protects content and non-content information in electronic storage.[133] One commentator has suggested that the non-content disclosure prohibitions and exceptions of the SCA should be read to apply to the Pen-Trap statute, arguing that to do otherwise "would effectively gut the non-content provisions of the SCA."[134] Because the SCA's exceptions are similar to those of the Wiretap Act,[135] this would introduce a similar ambiguity regarding the protection of customers.

It is doubtful that reading the disclosure provisions of the SCA into the Pen-Trap statute is a sound construction. There is, however, a structural argument in its favor: If in-transit communications content receives more protection than stored communications content, and if stored non-content information receives some protection, then it would appear anomalous for in-transit non-content information to receive zero protection from voluntary disclosure.

However attractive this argument may appear initially, closer examination reveals its flaws. First, the argument selectively ignores the sections of the SCA dealing with voluntary disclosure of stored communications content.[136] Obviously these provisions cannot be read into the Wiretap Act. In light of this, it would appear inconsistent to suggest that the provisions

---

131. *See supra* Part IV. A.

132. 18 U.S.C. §§ 2701–2712 (2006). The SCA, like the Wiretap Act, generally prohibits disclosure, but provides a list of exceptions. *See id.*

133. *See, e.g.*, Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1231 (2004).

134. Aaron J. Burstein, *Amending the ECPA to Enable a Culture of Cybersecurity Research*, 22 HARV. J.L. & TECH. 167, 193 (2008).

135. *See* 18 U.S.C. § 2702(c)(2) (permitting disclosure with consent); § 2702(c)(3) (permitting disclosure when "necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service").

136. The SCA contains separate lists of exceptions permitting disclosure of stored content and non-content "records." *See* 18 U.S.C. § 2702(b)–(c).

regarding stored non-content information should be read into the Pen-Trap statute. Second, under the logic of the overall statutory scheme, it is not anomalous for in-transit addressing information to receive less protection from voluntary disclosure than other kinds of information receive. This is exactly how the scheme structures compelled disclosure.[137] Third, in some circumstances at least, courts have been inclined to construe the SCA's disclosure prohibitions narrowly.[138] Thus, the best interpretation of silence in the Pen-Trap statute regarding voluntary disclosure is that such disclosure is permitted. Nevertheless, regardless of the correct reading, ambiguity creates some degree of legal risk that discourages sharing.

To sum up, the Pen-Trap statute, like the Wiretap Act, permits ISPs to scan their networks using government signatures. Absent consent, however, under both statutes there is some ambiguity as to the scope of permissible voluntary disclosure of the results of those scans to the government. The Wiretap Act may limit disclosures to information necessary to protect the rights or property of the ISP itself. Similarly, there is a colorable—though probably incorrect—argument that an analogous limit applies to the Pen-Trap statute. Because ISPs are unlikely to be willing to incur legal risk in exchange for a benefit that is diffused to society at large, this ambiguity is likely sufficient to derail any attempt by the executive to expand the ECS program without Congressional action.

V. LEGISLATIVE APPROACHES TO INCREASING INFORMATION SHARING

There are two potential legislative approaches to remedying the disincentives created by ambiguities in the Wiretap Act and the Pen-Trap statute. First, Congress could mandate that the private sector share certain cybersecurity information with the

---

137. The Wiretap Act requires a warrant on a heightened probable-cause standard. *See* 18 U.S.C. § 2518. The SCA requires a showing of "specific and articulable facts." § 2703(d). The pen/trap statute requires only that the applicant certify belief that the information to be obtained is "relevant to an ongoing criminal investigation." § 3122(b)(2).

138. *See, e.g.*, Andersen Consulting LLP v. UOP, 991 F. Supp. 1041, 1043 (N.D. Ill. 1998) (holding provider of corporate e-mail service not subject to the limits on providers to the public).

government. Second, Congress could remove the hurdles to voluntary sharing. As stated in Part III, a mandate would render scanning pursuant to the ECS program a government search within the meaning of the Fourth Amendment. As discussed there, however, that is not necessarily fatal given that a court could sanction action that identifies only illegal activity, or that satisfies a special need. Thus, the choice between mandating or facilitating sharing is driven primarily by policy rather than constitutional concerns.

A mandate has the advantage of obviating any incentive problem,[139] and would ensure sharing occurs. Yet, if legal uncertainty is the primary inhibitor to voluntary sharing, then removing that uncertainty may be just as effective. In addition, keeping sharing voluntary may have other advantages. First, voluntary participation in ECS has the potential to improve the program because the government is likely to respond to the possibility that participants will leave an ineffective or overly burdensome program. This was reportedly the experience of the DIB Pilot.[140] Second, voluntary sharing has the potential to be more protective of privacy. Voluntary participation will permit companies with data they feel is especially sensitive to avoid sharing it without Congress having to anticipate this reaction and enumerate an exception.[141] Additionally, because a variety of consumer groups monitor internet companies' sharing of

---

139. *Cf. The Cybersecurity Act of 2012: Hearing Before the S. Comm. on Homeland Sec. and Gov't Affairs*, 112th Cong. 3 (2012) (statement of Michael Chertoff, Managing Principal, The Chertoff Group), http://www.hsgac.senate.gov/issues/cybersecurity/, [http://perma.cc/525A-FU7J] (noting insufficiency of market incentives in analogous context of security standards).

140. *See* Ellen Nakashima, *Cyber defense effort is mixed, study finds*, WASH. POST, Jan. 12 2012, http://www.washingtonpost.com/world/national-security/cyber-defense-effort-is-mixed-study-finds/2012/01/11/gIQAAu0YtP_story.html, [http://perma.cc/DU2F-7CUK]; John Reed, *Rogers was right, DoD-DHS cyber info sharing program has shrunk*, FOREIGN POL'Y FP 'KILLER APPS' BLOG, (Oct. 24, 2012, 3:29 PM), http://killerapps.foreignpolicy.com/posts/2012/10/24/rogers_was_right_dod_dhs_cyber_info_sharing_program_has_shrunk/, [http://perma.cc/W2NM-Y9YN].

141. *See* STEVEN P. BUCCI ET AL., HERITAGE FOUND., A CONGRESSIONAL GUIDE: SEVEN STEPS TO U.S. SECURITY, PROSPERITY, AND FREEDOM IN CYBERSPACE 5 (2013), http://www.heritage.org/research/reports/2013/a-congressional-guide-seven-steps-to-US-security-prosperity-and-freedom-in-cyberspace, [http://perma.cc/7P27-73X8].

information with the government,[142] a voluntary program creates an incentive against forms of sharing that the public believes are especially intrusive. This incentive may require an offset, such as a statutory or executive proscription on the government's use of the information for non-cybersecurity purposes. Thus, there are sound policy reasons for preferring the voluntary approach.

VI. CONCLUSION

The information sharing program formalized in Executive Order 13,636 is an important step toward protecting critical infrastructure from cyber threats. ECS enables privately operated networks to benefit from foreign intelligence through a system that makes the intelligence useable and protects it from disclosure. Expanding ECS to accommodate voluntary information sharing from the private sector to the government is likely to further improve the security of critical infrastructure and does not involve the government in the bulk collection of communications or associated metadata. The President's call for congressional action is well founded. Even though DHS may legally accept information voluntarily shared by private entities without new authority, and even though such sharing is unlikely to offend the Fourth Amendment, ambiguity regarding its permissibility under the Wiretap Act and the Pen-Trap statute likely is sufficient to discourage providers from sharing. Congress should correct this problem by clearly enabling private entities to voluntarily share information with the federal government for cybersecurity purposes.

Jeremy J. Broggi

142. *See, e.g.*, NATE CARDOZO ET AL., ELEC. FRONTIER FOUND., WHO HAS YOUR BACK: WHICH COMPANIES HELP PROTECT YOUR DATA FROM THE GOVERNMENT? (2013), https://www.eff.org/files/who-has-your-back-2013-report-20130513.pdf, [http://perma.cc/QV7A-V6KR].