

Cybersecurity: Selected Legal Issues

Edward C. Liu
Legislative Attorney

Gina Stevens
Legislative Attorney

Kathleen Ann Ruane
Legislative Attorney

Alissa M. Dolan
Legislative Attorney

Richard M. Thompson II
Legislative Attorney

Andrew Nolan
Legislative Attorney

April 17, 2013

Congressional Research Service
7-5700
www.crs.gov
R42409

CRS Report for Congress
Prepared for Members and Committees of Congress
c11173008

Summary

The federal government's role in protecting U.S. citizens and critical infrastructure from cyber attacks has been the subject of recent congressional interest. Critical infrastructure commonly refers to those entities that are so vital that their incapacitation or destruction would have a debilitating impact on national security, economic security, or the public health and safety. This report discusses selected legal issues that frequently arise in the context of recent legislation to address vulnerabilities of critical infrastructure to cyber threats, efforts to protect government networks from cyber threats, and proposals to facilitate and encourage sharing of cyber threat information among private sector and government entities. This report also discusses the degree to which federal law may preempt state law.

It has been argued that, in order to ensure the continuity of critical infrastructure and the larger economy, a regulatory framework for selected critical infrastructure should be created to require a minimum level of security from cyber threats. On the other hand, others have argued that such regulatory schemes would not improve cybersecurity while increasing the costs to businesses, expose businesses to additional liability if they fail to meet the imposed cybersecurity standards, and increase the risk that proprietary or confidential business information may be inappropriately disclosed.

In order to protect federal information networks, the Department of Homeland Security (DHS), in conjunction with the National Security Agency (NSA), uses a network intrusion system that monitors all federal agency networks for potential attacks. Known as EINSTEIN, this system raises significant privacy implications—a concern acknowledged by DHS, interest groups, academia, and the general public. DHS has developed a set of procedures to address these concerns, such as minimization of information collection, training and accountability requirements, and retention rules. Notwithstanding these steps, there are concerns that the program may implicate privacy interests protected under the Fourth Amendment.

Although many have argued that there is a need for federal and state governments and owners and operators of the nation's critical infrastructures, to share information on cyber vulnerabilities and threats, obstacles to information sharing may exist in current laws protecting electronic communications or in antitrust law. Private entities that share information may also be concerned that sharing or receiving such information may lead to increased civil liability, or that shared information may contain proprietary or confidential business information that may be used by competitors or government regulators for unauthorized purposes.

Recent legislative proposals, such as H.R. 624, the Cyber Intelligence Sharing and Protection Act (CISPA), would seek to improve the nation's cybersecurity, and may raise some or all of the legal issues mentioned above. This report provides a general discussion of the legal issues raised by these proposals; however, a detailed description and comparison of these legislative proposals is beyond the scope of this report.

Additionally, see CRS Report R42619, *Cybersecurity: CRS Experts*, by Eric A. Fischer.

Contents

Legal Issues Related to Protecting Critical Infrastructure 1
Deference to Agency Decisions 2
Availability of Judicial Review 3
Questions of Fact 4
Interpretations of Law 5
Liability Concerns 6
Freedom of Information 7
Ex Parte Communications 9
Legal Issues Related to the Protection of Federal Networks 10
EINSTEIN Overview 11
EINSTEIN and the Fourth Amendment 12
Monitoring Communications from Federal Employees 14
Monitoring Communications from Private Persons to Federal Employees 16
Alternative to Traditional Warrant Requirement 17
Privacy and Civil Liberties Oversight 18
Legal Issues Related to Cybersecurity Threat Information Sharing 19
Electronic Communications Privacy Act 20
Antitrust Law 22
Liability for Information Sharing 24
Protection of Proprietary or Confidential Business Information 25
Privacy and Civil Liberties 26
Preemption 26

Contacts

Author Contact Information 28

For many, the Internet has become inextricably intertwined with daily life. Many rely on it to perform their jobs, pay their bills, send messages to loved ones, track their medical care, and voice political opinions, among a host of other activities. Likewise, government and business use the Internet to maintain defense systems, protect power plants and water supplies, and keep other types of critical infrastructure running.[1] Consequently, the federal government's role in protecting U.S. citizens and critical infrastructure from cyber attacks has been the subject of recent congressional interest.[2]

This report discusses selected legal issues that frequently arise in the context of legislation to address vulnerabilities of private critical infrastructure to cyber threats, efforts to protect government networks from cyber threats, and proposals to facilitate and encourage sharing of cyber threat information amongst private sector and government entities. This report also provides an overview of the ways in which federal laws of these types may preempt or affect the applicability of state law.

Recent legislative proposals, such as H.R. 624, the Cyber Intelligence Sharing and Protection Act (CISPA),[3] would seek to improve the nation's cybersecurity, and may raise some or all of the legal issues discussed below. This report provides a general discussion of the legal issues raised by these proposals; however, a detailed description and comparison of these legislative proposals is beyond the scope of this report.

Legal Issues Related to Protecting Critical Infrastructure

Although no federal statute currently imposes a generally applicable obligation on businesses in the private sector to take measures to protect themselves from cyber vulnerabilities, Congress has chosen to impose regulatory standards regarding the security, including the cybersecurity, of specific sectors or types of private entities.[4] For example,[5] chemical facilities are subject to chemical facility anti-terrorism standards (CFATS) promulgated by the Department of Homeland

[1] Critical infrastructure commonly refers to those entities that are so vital that their incapacitation or destruction would have a debilitating impact on national security, economic security, or the public health and safety. 42 U.S.C. §5195c(e). For more information, *see* CRS Report RL30153, *Critical Infrastructures: Background, Policy, and Implementation*, by John D. Moteff.

[2] *See*, *e.g.*, Siobhan Gorman, *Cybersecurity Bills Duel Over Rules for Firms*, WALL ST. J., March 9, 2012, at A6.

[3] For more information on legal issues specific to CISPA, *see*:

- CRS Legal Sidebar WSLG478, House Intelligence Committee Marks Up Cybersecurity Bill CISPA, by Richard M. Thompson II and Gina Stevens;
- CRS Legal Sidebar WSLG480, Privacy and Civil Liberties Issues Raised by CISPA, by Andrew Nolan;
- CRS Legal Sidebar WSLG481, CISPA, Private Actors, and the Fourth Amendment, by Richard M. Thompson II; and
- CRS Legal Sidebar WSLG483, Obstacles to Private Sector Cyber Threat Information Sharing, by Edward C. Liu.

[4] *See also* GOVERNMENT ACCOUNTABILITY OFFICE, Information Technology: Federal Laws, Regulations, and Mandatory Standards for Securing Private Sector Information Technology Systems and Data in Critical Infrastructure Sectors, GAO-08-1075R, September 16, 2008, *available at* http://www.gao.gov/assets/100/95747.pdf.

[5] The existing regulatory frameworks discussed here do not constitute an exhaustive list of all regulations applicable to critical infrastructure, but are only intended to provide some context for the following discussions.

Security (DHS), which include provisions requiring chemical facilities to take measures to protect against cyber threats.[6] Electrical utilities are required to comply with reliability standards, including standards to protect against cyber incidents, set by the North American Electrical Reliability Corporation (NERC).[7] Similarly, the Maritime Transportation Security Act (MTSA) gives the Coast Guard the authority to regulate the security of maritime facilities and vessels, including requiring security plans that contain provisions for the security of communications systems used in those facilities.[8]

Proposals that focus on the increased cybersecurity of certain sectors of the economy are frequently justified on the grounds that those private entities, including energy, transportation, or communication providers, comprise the nation's critical infrastructure. If the incapacity or destruction of such systems or assets would have a debilitating impact on national security, economic security, or public health and safety, it would be in the national interest to ensure that such critical infrastructure was adequately protected. Consequently, it has been argued that a regulatory framework governing selected critical infrastructure entities is needed to ensure that these private entities take measures adequate to maintain a minimum level of security from cyber threats, in order to protect the rest of the economy.[9]

On the other hand, others have argued that such regulatory schemes would not improve cybersecurity and would also increase the costs of doing business for these sectors of the economy.[10] There are also concerns that businesses would face additional exposure to civil liability from private suits if they failed to meet the imposed standards. As many of these regulatory schemes provide regulatory agencies with access to information held by the regulated entities, concerns have also been raised about the inappropriate disclosure of proprietary or confidential business information.

The concerns raised by these issues have shaped the existing legal schemes regulating the security of specific categories of critical infrastructure, and may also inform legislative proposals to improve the security of critical infrastructure from cyber threats. A brief overview of each of these issues is provided in the next sections of this report.

Deference to Agency Decisions

Proposals to establish a regulatory scheme for the cybersecurity of critical infrastructure may provide the agency or agencies charged with administering the program with significant discretion. For example, agencies may be responsible for identifying those private entities that would fall within the scope of a particular bill and that will, therefore, be subject to the

[6] P.L. 109-295, §550 (codified at 6 U.S.C. §121 note). For a more detailed discussion of CFATS, *see* CRS Report R41642, *Chemical Facility Security: Issues and Options for the 112th Congress*, by Dana A. Shea.

[7] For a more detailed discussion of cybersecurity and electrical utilities, see CRS Report R41886, *The Smart Grid and Cybersecurity—Regulatory Policy and Issues*, by Richard J. Campbell.

[8] 46 U.S.C. §§70102-70103.

[9] For a more detailed discussion of critical infrastructure policy arguments, see CRS Report RL30153, *Critical Infrastructures: Background, Policy, and Implementation*, by John D. Moteff.

[10] *E.g.*, *Securing America's Future: The Cybersecurity Act of 2012 Before the S. Comm. on Homeland Security and Governmental Affairs*, 112th Cong. (statement of former DHS Secretary Tom Ridge on behalf of U.S. Chamber of Commerce) ("New compliance mandates would drive up costs and misallocate business resources without necessarily increasing security.")

requirements that would be imposed under the bill. Agencies may also be delegated the authority to develop the precise standards or metrics that regulated entities will be measured against. Being subject to the regulations may have significant cost, liability, or other implications for a regulated entity; therefore, such entities may seek to challenge the decisions or rules promulgated by an agency through redress mechanisms created in the statute or through judicial review of agency action under the Administrative Procedure Act (APA).[11] Entities may also seek judicial review of agency actions in the context of enforcement actions taken against them under the various regulatory schemes.

Depending upon the legislative language delegating regulatory authority to the agency, a court will evaluate an agency's decision under varying standards of review. In the context of regulating the security of critical infrastructure, a more deferential standard of review of agency determinations typically means that regulated private entities would have less recourse in the event that they disagreed with an agency's determination. On the other hand, a less deferential standard of review may extend the time to implement particular security standards if the agency encounters delays caused by litigation. Examples of the different types of judicial review that may be involved in such a regulatory scheme are discussed below.

Availability of Judicial Review[12]

Initially, it is necessary to determine whether a particular agency action is judicially reviewable. As a general matter, there is a "'strong presumption that Congress intends judicial review' of administrative action."[13] This presumption is embodied in the Administrative Procedure Act (APA), which provides that "final agency action for which there is no other adequate remedy in a court [is] subject to judicial review."[14] The APA provides two exceptions to the presumption of availability of judicial review of agency action: (1) "to the extent that ... statutes preclude judicial review" and (2) "where agency action is committed to agency discretion by law."[15] However, judicial review of an unreviewable determination may occur if there is a constitutional issue.[16]

Under the APA, judicial review of agency actions may be unavailable if such review is specifically precluded by statute.[17] This exemption requires the existence of an explicit statutory

[11] 5 U.S.C. §701 *et seq.*, *see e.g.*, Nat'l Propane Gas Ass'n v. DHS, 534 F. Supp. 2d 16 (D.D.C. 2008) (denying temporary restraining order in action brought under APA claim for review of agency's designation of propane as chemical of interest for purposes of CFATS).

[12] For more information on judicial review of agency actions, see CRS Report R41546, *A Brief Overview of Rulemaking and Judicial Review*, by Todd Garvey and Daniel T. Shedd.

[13] Gutierrez De Martinez v. Lamagno, 515 U.S. 417, 424 (1995) (quoting Bowen v. Michigan Academy of Family Physicians, 476 U.S. 667, 670 (1986)); *see also* McNary v. Haitian Refugee Center, Inc., 498 U.S. 479, 496 (1991); Abbott Laboratories v. Gardner, 387 U.S. 136 (1967); Citizens to Protect Overton Park v. Volpe, 401 U.S. 402 (1971); 28 U.S.C. §1331; *but see* Block v. Community Nutrition Institute, 467 U.S. 340, 349 (1984) (noting that "[t]he presumption favoring judicial review of administrative action ... may be overcome by specific language or specific legislative history that is a reliable indicator of congressional intent"). "The congressional intent necessary to overcome the presumption may also be inferred from contemporaneous judicial construction barring review and the congressional acquiescence in it ... or from the collective import of legislative and judicial history behind a particular statute," or from "inferences of intent drawn from the statutory scheme as a whole." *Id.*

[14] 5 U.S.C. §§702, 704.

[15] 5 U.S.C. §701.

[16] *See* Webster v. Doe, 486 U.S. 592 (1988); Oestereich v. Selective Service System, 393 U.S. 233 (1968).

[17] 5 U.S.C. §701(a)(1).

provision prohibiting judicial review of agency action. Additionally, even where judicial review has not been explicitly barred, the APA precludes judicial review where the decision has been committed to agency discretion by law.[18] This second exemption has been interpreted by the Supreme Court to be a very narrow exception, and applies only in situations where the statute provides no law for a reviewing court to apply.[19] For example, in *Webster v. Doe*,[20] the Supreme Court held that firing decisions made by the Director of Central Intelligence were unreviewable because the National Security Act provided that the Director "may, in his discretion, terminate the employment of any officer or employee of the [Central Intelligence Agency] whenever he shall deem such termination necessary or advisable in the interests of the United States."[21] The Court held that such a statute "exuded deference" and noted:

> Short of permitting cross-examination of the Director concerning his views of the Nation's security and whether the discharged employee was inimical to those interests, we see no basis on which a reviewing court could properly assess an Agency termination decision.[22]

Since the statute contained no standards a court could apply to evaluate the Director's decision, the Court determined that these decisions had been committed to agency discretion by law, and were consequently unreviewable.

Questions of Fact

Where a statute does provide judicially administrable standards, agency determinations of factual questions are typically reviewed under the "substantial evidence" or "abuse of discretion standards."[23] In the administrative context, substantial evidence review and abuse of discretion review occur in factually distinct circumstances. Substantial evidence is required when an agency engages in either formal rulemaking or an adjudicatory hearing.[24] In contrast, abuse of discretion applies in cases of informal rulemaking and decisions.[25]

Some courts appear to consider substantial evidence a more demanding standard than abuse of discretion, but the consistent theme of both standards is that the court is not free to substitute its judgment in place of the agency's.[26] In terms of analysis, the substantial evidence and abuse of discretion standards are both less stringent than *de novo* review, which would allow a court to look at the evidence anew and come to its own conclusions. Nevertheless, the Supreme Court has described these standards as requiring "more than a mere scintilla" of support and comparable to the standard a trial judge must meet to sustain a jury's verdict.[27] In the federal courts, a jury

[18] 5 U.S.C. §701(a)(2).

[19] Citizens of Overton Park v. Volpe, 401 U.S. 402 (1971).

[20] Webster v. Doe, 486 U.S. 592 (1988).

[21] 50 U.S.C. §403-4a(e)(1).

[22] *Webster*, 486 U.S. at 600.

[23] 5 U.S.C. §706(2).

[24] *Id.* at §706(2)(E).

[25] *Id.* at §706(2)(A).

[26] *See*, *e.g.*, Frontier Fishing Corp. v. Evans, 429 F. Supp. 2d 316, n.7 (citing Indus. Union Dep't v. API, 448 U.S. 607, 705 (1980) (Marshall, J., dissenting) (asserting that substantial evidence is more stringent, but is ultimately a deferential standard)).

[27] Consolidated Edison Co. v. NLRB, 305 U.S. 197, 229 (1938); NLRB v. Columbian Enameling & Stamping Co., 306 U.S. 292, 300 (1939)

verdict will not be disturbed if "reasonable and fair-minded persons in exercise of impartial judgment" might have come to the same conclusion as the jury.[28]

Examples of a factual question that might be raised in the context of cybersecurity regulation of critical infrastructure may include whether the disruption of a particular asset could lead to sufficient harm to qualify the asset as critical infrastructure that would be subject to increased scrutiny under a new regulatory scheme. Factual questions may also arise in the context of agency determinations regarding whether a regulated entity had met an applicable cybersecurity standard. Unless legislation sets forth a different standard of review, it is likely that, under the APA, a court would apply a "substantial evidence" or "abuse of discretion" standard to these types of factual questions.

Interpretations of Law

Agencies may also exercise discretion in interpreting the terms used in a statute. Proposals to regulate the cybersecurity of critical infrastructure may include ambiguity regarding the precise scope of the term "critical infrastructure." This and other terms used in the regulatory scheme may be susceptible to more than one specific construction, and the different interpretations may have material consequences for those subject to the regulatory scheme. A narrow definition may mean that fewer entities would be subject to regulation, while a broader definition may encompass a more expansive cross-section of businesses.

The validity of an agency's construction of a statute would likely be evaluated using the two-prong test described by the Supreme Court in *Chevron v. Natural Resources Defense Council*.[29] First, if the text and legislative history of the statute demonstrate that Congress has spoken directly on the issue, then that statutory language or history must control. However, under the second prong, if the statute is ambiguous because "Congress has not directly addressed the precise question at issue," the agency's interpretation will stand so long as it is a reasonable one.[30]

Therefore, under *Chevron*, whether a particular statutory provision is ambiguous or not can change the degree of deference afforded an agency. Where no ambiguity exists, the reviewing court's focus is on the intent of Congress, and it may interpret the law *de novo* without any deference toward the agency's interpretation. On the other hand, if the statute is ambiguous, either because the language used is susceptible to more than one meaning or because the law contains internal inconsistencies, the reviewing court is not permitted to supplant its own interpretive preferences for that of the agency, unless the agency's interpretation is unreasonable. Under this deferential standard of review, the discretion available to an agency is inversely proportional to the degree of specificity provided in a particular statute. In other words, the less specific a particular law is regarding the Secretary's regulatory authority, the more flexibility might be available to her to exercise during implementation.

[28] *E.g.*, Kosmynka v. Polaris Industries, Inc., 462 F.3d 74, 79-82 (2d Cir. 2006) (upholding jury's finding that a manufacturer was negligent for failing to warn that its all-terrain vehicle might upend itself despite uncontested evidence that the manufacturer had received no reports of such incidents).

[29] Chevron v. Nat'l Resources Def. Council, 467 U.S. 837, 842-45 (1984).

[30] *Id.*

Liability Concerns

The creation of a regulatory scheme applicable to critical infrastructure may raise issues regarding the effects that the new regulatory scheme would have on the potential civil or criminal liability of the covered entities. Regulators may be given the authority to impose civil or criminal penalties for noncompliance, or may seek to promote compliance by offering financial incentives.[31]

In addition to the forms of liability imposed by regulatory authorities, questions may arise regarding the potential ways in which the regulatory scheme may expose covered entities to additional private civil liability. In this context, a federal regulatory scheme could be viewed as creating a standard of care that might be used to establish tort liability under state law. Entities that fall below that standard of care face the possibility of liability in the event of a security breach, separate and apart from any penalties that might be imposed by government regulators. The most likely form that such a civil action would take is in a tort suit alleging that the private entity had acted negligently; that is, the entity had failed to exercise reasonable care in the face of a foreseeable risk. Under current state law, entities found negligent may be liable for harm that results from their negligence.[32] Similar liability may also arise under statutory or contractual provisions that prescribe reasonable conduct.[33]

The existence of a federal regulatory scheme that imposes compliance standards may affect suits alleging negligence in two ways. First, the entities that are subject to the compliance standards may be found negligent *per se* if they fail to satisfy those standards.[34] Negligence *per se* is a theory of negligence in which the fact that an entity's conduct has violated some applicable statute is *prima facie* evidence that the entity has acted negligently.[35] Unless the defendant could rebut that presumption, the defendant would likely be found to be *per se* negligent, and consequently liable for any harm that results from that negligence.[36] In the context of cyber threats to critical infrastructure, this might mean that a regulated entity that fails to adequately secure its information infrastructure as required under a federal regulatory scheme would be liable for a cyber incident that causes harm to customers or other third parties.

---

[31] A second issue with respect to enforcement is whether penalties would be limited to fines and other monetary penalties or whether injunctive relief may also be sought to compel compliance or to stop a noncompliant facility from operating. For example, violations of CFATS can be punished by civil monetary penalties or an injunction to cease operations. 6 C.F.R. §27.300. Similarly, under MTSA, covered vessels and facilities without an approved security plan may be prohibited from operating. 46 U.S.C. §70103(c)(5). Questions may also arise regarding the types of investigative authorities that would be provided to the agency tasked with administering the regulatory scheme.

[32] Reese v. Philadelphia & R. R. Co., 239 U.S. 463, 465 (1915) ("The rule is well settled that a railroad company is not to be held as guaranteeing or warranting absolute safety to its employees under all circumstances, but is bound to exercise the care which the exigency reasonably demands in furnishing proper roadbed, tracks, and other structures. A failure to exercise such care constitutes negligence.").

[33] *See*, Patco Constr. Co. v. People's United Bank, 2012 U.S. App. LEXIS 13617 (1st Cir. 2012) (holding that bank may be liable for fraudulent electronic transfers if its security systems were not commercially reasonable under Uniform Commercial Code art. 4A).

[34] *See* RESTATEMENT (SECOND) OF TORTS §285 ("The standard of conduct of a reasonable man may be ... adopted by the court from a legislative enactment or an administrative regulation which does not so provide ...").

[35] *See*, *e.g.*, Makas v. Hillhaven, Inc., 589 F. Supp. 736, 741 (M.D.N.C. 1984) ("Negligence *per se* in effect is a presumption that one who has violated a safety statute has violated its legal duty to exercise due care.").

[36] *See*, *e.g.*, Resser v. Boise-Cascade Corp., 587 P.2d 80, 84 (Or. 1978) (violation of state law establishing speed limits at railroad crossing raises a rebuttable presumption of negligence).

Second, entities that are not subject to regulation under a federal scheme may not be subject to negligence *per se*. However, the performance standards or other requirements imposed under that scheme may still affect their liability for negligence if such requirements establish an applicable standard of care that the nonregulated entity would be judged against in a private civil suit.[37]

Because of the effect that a regulatory scheme can have on civil liability, proposals to regulate the cybersecurity of critical infrastructure may also propose limits on liability for regulated entities. The scope of such limits may range from complete immunity from private suits, to lesser restrictions such as prohibitions against the awarding of punitive damages. Such limits on liability may also be made dependent upon an entity's satisfaction of its regulatory obligations, in order to create a further incentive for compliance.

Freedom of Information

Access to the confidential business information of owners and operators of the nation's critical infrastructure and of private sector entities continues to be an important component of efforts to protect against cybersecurity threats. However, some critical infrastructure owners and operators and private sector entities may be hesitant to share cybersecurity-related information with the government because of the possible disclosure of this information to the public under the Freedom of Information Act (FOIA)[38] and state open records laws.[39] In addition, concerns also exist that sharing of cybersecurity information may facilitate access to proprietary and confidential business information by competitors. Furthermore, some have expressed concerns that the government may use information obtained for cybersecurity purposes for non-cybersecurity purposes, such as regulatory actions. Concerns also exist that reliance on FOIA's exemptions to shield shared cybersecurity threat information is misplaced because court interpretations of the scope of FOIA's exemptions can change.[40] Proponents of open records and government transparency argue that new exemptions from FOIA jeopardize the public's ability to obtain information about government and industry practices, cast a shroud of secrecy over government's functions, and are unnecessary because FOIA's exemptions adequately protect private information from disclosure.[41] Some observers believe that it is not certain that some cybersecurity threat information, such as routing information or website access logs, would fit within FOIA's exemptions.

---

[37] *See*, *e.g.*, Burmaster v. Gravity Drainage Dist. No. 2, 448 So. 2d 162, 164 (La. Ct. App. 1984) (Occupational Safety and Health Act regulations and standards published by industry groups warrant consideration as evidence of standard of care, even if they are not controlling).

[38] 5 U.S.C. §552.

[39] National Freedom of Information Coalition, State Freedom of Information Laws (2012), at http://www.nfoic.org/state-freedom-of-information-laws.

[40] As an example, in Milner v. Dept. of the Navy, 131 S. Ct. 1259 (2011), the Supreme Court limited the scope of FOIA Exemption 2 (the Court held that "Exemption 2, consistent with the plain meaning of the term "personnel rules and practices," encompasses only records relating to issues of employee relations and human resources."). *Id.* at 1271. *See* U.S. Dep't of Justice, Exemption 2 After the Supreme Court's Ruling in *Milner v. Department of the Navy*, at http://www.justice.gov/oip/foiapost/2011foiapost15.html.

[41] Testimony of David Sobel, Electronic Privacy Information Clearinghouse before the U.S. Congress, House Committee on Energy and Commerce, Subcommittee on Oversight and Investigations, *Creating The Department of Homeland Security: Consideration of the Administration's Proposal*, 107th Cong., 2nd sess., June 25 and July 9, 2002, Serial No. 107-113 (Washington: GPO, 2002), p. 258.

The Freedom of Information Act of 1974 (FOIA) regulates the disclosure of federal agency records.[42] FOIA requires that certain types of records be published in the *Federal Register*;[43] that certain types of records be made available for public inspection and copying;[44] and that all other records be subject to request in writing. All records not available via publication or inspection, not exempt from disclosure, or excluded from coverage are subject to disclosure.[45] FOIA has nine exemptions from disclosure which permit, rather than require, the withholding of the requested information.[46]

Subsection (b)(3) of FOIA, commonly referred to as exemption 3, permits agencies to withhold information under FOIA that is specifically prohibited from disclosure by other federal statutes.[47] For a nondisclosure provision in a separate federal statute to qualify for exemption 3 status, the nondisclosure provision must meet the following criteria: either the statute must require that matters be withheld from the public in such a manner as to leave no discretion on the issue; or the statute must establish particular criteria for withholding or refer to particular types of matters to be withheld; and it must specifically cite FOIA exemption 3.[48] If the statute meets the criteria of exemption 3 and the information to be withheld falls within the scope and coverage of FOIA, the information is exempt from disclosure under exemption 3.[49] Statutes that meet these criteria are referred to as "FOIA exemption 3 statutes."[50]

To encourage private and public sector entities and persons to voluntarily share their critical infrastructure information with the Department of Homeland Security (DHS), the Critical Infrastructure Information Act of 2002 (CIIA) includes several measures to ensure against disclosure of protected critical infrastructure information by DHS. According to the Department of Justice, the agency responsible for administering FOIA, the CIIA will operate as an exemption 3 statute under FOIA for critical infrastructure information that is obtained by the Department of Homeland Security.[51] Relevant to this discussion, the CIIA provides protections against the disclosure of information that is voluntarily submitted by a critical infrastructure entity to DHS. If the information submitted satisfies the requirements of the CIIA, the information is designated as

[42] 5 U.S.C. §552.

[43] 5 U.S.C.§552(a)(1).

[44] 5 U.S.C. §552(a)(2).

[45] Excluded from the act's coverage are special categories of law enforcement records related to criminal law investigations or proceedings, informant records, and records maintained by the FBI pertaining to foreign intelligence, counterintelligence or international terrorism. 5 U.S.C. §552(c)(1), (c)(2), (c)(3).

[46] *See* Dep't of the Air Force v. Rose, 425 U.S. 352, 361 (1976) (holding that "limited exemptions do not obscure the basic policy that disclosure, not secrecy, is the dominant objective of the Act").

[47] 5 U.S.C. §552(b)(3).

[48] 5 U.S.C. §552(b)(3).

[49] U.S. Department of Justice, Statutes Found to Qualify under Exemption 3 of the FOIA, (August 2011), *available at* http://www.justice.gov/oip/exemption3.pdf.

[50] Examples of FOIA exemption 3 statutes are the Aviation and Transportation Security Act of 2001 (ATSA) which designates 16 categories of sensitive security information and includes information submitted pursuant to a requirement and information voluntarily submitted, P.L. 107-71, codified at 49 U.S.C. §40119; the Critical Infrastructure Information Act of 2002 (CIIA) which provides confidentiality protections for critical infrastructure information voluntarily submitted to DHS, P.L. 107-296, codified at 6 U.S.C. §133 *et seq.*; the Maritime Transportation Security Act of 2002 (MTSA) which requires covered entities to submit information to the federal government, P.L. 107-295; and the Safe Drinking Water Act (SDWA), as amended, which requires community water systems to perform vulnerability analyses of their facilities and includes protections for vulnerability assessments. P.L. 107-188, 42 U.S.C. §300i-2.

[51] Department of Justice, "Homeland Security Law Contains New Exemption 3 Statute," FOIA Post (2003).

critical infrastructure information (CII), and for purposes of FOIA, the CIIA expressly prohibits the disclosure of critical infrastructure information. Critical infrastructure information "means information not customarily in the public domain and related to the security of critical infrastructure or protected systems."[52] Therefore, the classification of information as CII would protect that information from disclosure under FOIA, state and local disclosure laws, and use in civil litigation. In addition, protected critical infrastructure information cannot be used for regulatory purposes.[53] Federal, state, and local government officials and contractors approved by DHS can access the information for critical infrastructure protection or criminal law enforcement purposes.

With respect to concerns about litigation, CIIA limits the use of CII in civil litigation and provides that sharing CII with the agency does not count as the "waiver of any applicable privilege or protection provided under law," such as trade secret protection or the attorney-client privilege.[54] CIIA authorizes the use or disclosure of such information by officers and employees in furtherance of the investigation or the prosecution of a criminal act, or for disclosure to Congress or the Government Accountability Office.

Another exemption 3 statute under FOIA for critical infrastructure information was recently enacted in the National Defense Authorization Act for Fiscal Year 2012. Section 1091 authorizes the Secretary of Department of Defense (DOD), or his designee, to exempt DOD critical infrastructure security information from disclosure pursuant to Section 552(b)(3) of Title 5 (FOIA Exemption 3) upon a written determination that the information is DOD critical infrastructure security information, and the public interest consideration in the disclosure of such information does not outweigh preventing the disclosure of such information.[55] Department of Defense critical infrastructure security information means sensitive but unclassified information that, if disclosed, would reveal vulnerabilities of DOD critical infrastructure that could result in the disruption, degradation, or destruction of Department of Defense (DOD) operations, property, or facilities.

In addition to protections of proprietary information that exist in current law, proposals to regulate the cybersecurity of critical infrastructure may provide additional protections for information submitted to federal agencies under the new regulatory scheme. Such proposals may simply expand existing categories of protected information, or may create new categories of protected information that would be subject to different prohibitions on disclosure or sharing.

Ex Parte Communications

Providing information to a regulatory agency may also be subject to further disclosure if the communication would implicate agency rules or judicial doctrine regarding ex parte communications. Under the APA, formal agency adjudications are to be decided solely on the basis of record evidence. The APA provides that "[t]he transcript of testimony and exhibits, together with all papers and requests filed in the proceeding, constitutes the exclusive record for

[52] 6 C.F.R. §29.2(b).

[53] *See* U.S. Dept. of Homeland Security, Protected Critical Infrastructure Information (PCII) Program, at http://www.dhs.gov/files/programs/editorial_0404.shtm; PCII Program and Procedures Guidance Manual (April 2009) at http://www.dhs.gov/xlibrary/assets/pcii_program_procedures_manual.pdf.

[54] *See* Fed. R. Evid. 501.

[55] P.L. 112-8, §1091, 125 Stat. 1604.

decision."[56] The reason for this "exclusiveness of record" principle is to provide fairness to the parties in order to ensure meaningful participation. Challenges to the "exclusiveness of record" occur when there are ex parte contacts—communications from an interested party to a decision-making official that take place outside the hearing and off the record.[57] The APA prohibits any "interested person outside the agency" from making, or knowingly causing, "any ex parte communication relevant to the merits of the proceeding" to any decision making official.[58] Similar restraints are imposed on the agency decision makers.[59] Additionally, ex parte communications received in violation of these rules are generally required to be disclosed to all other interested parties and made part of the public record for the proceeding.[60] The CIIA provides that CII will not be subject to agency rules or judicial doctrine regarding ex parte communications. However, if an entity is involved in a proceeding where ex parte communications are prohibited, there may be concerns that providing cybersecurity information that would not qualify as CII might implicate the rules against ex parte communications, and could be subject to disclosure on the public record or to other interested parties. Consequently, proposals to regulate the cybersecurity of critical infrastructure may exempt certain types of information that is shared with federal agencies for regulatory purposes from the definition of an ex parte communication, so that such information would not be subject to further disclosure.

Legal Issues Related to the Protection of Federal Networks

Prompted by a perceived threat to governmental information technology (IT) systems, DHS, in conjunction with the National Security Agency (NSA), has incrementally ramped up monitoring of federal government networks over the past decade to identify and prevent cyber attacks. A focal point of these efforts is EINSTEIN, a network intrusion system that monitors all federal agency networks for potential attacks. As part of this monitoring, all communications by federal executive agency employees made on federal networks, and incidentally, all communications they have with private citizens, are monitored for malicious activity. This monitoring may trigger Fourth Amendment guarantees to the right to be free from unreasonable searches and excessive government intrusion. Additionally, Congress has enacted statutory rules that place a higher restriction than the Constitution on government access to electronic communications.[61]

Some cybersecurity proposals may seek to codify current executive agency practices embodied in the EINSTEIN program, to provide agencies with explicit statutory authority to engage in such monitoring. This section surveys EINSTEIN's background and discusses the Fourth Amendment concerns it raises for both federal employees and private citizen's communicating with them, and

[56] 5 U.S.C. §556(e).

[57] *Id*.

[58] 5 U.S.C. §557(d)(1). For example, under CFATS, during an adjudication ex-parte communications between the department and the chemical facility is not permitted. 6 C.F.R. §27.320.

[59] 5 U.S.C. §557(d)(1)(E).

[60] 5 U.S.C. §557(d)(1)(C).

[61] This section focuses on the constitutional concerns with EINSTEIN under the Fourth Amendment. Although statutes such as the Electronic Communications Privacy Act of 1986, P.L. 99-508, 100 Stat. 1848, and the Privacy Act of 1974, 5 U.S.C. §522a, may be implicated, they will not be discussed here.

alternative privacy and civil liberties protections that may be instituted to complement Fourth Amendment protections.

EINSTEIN Overview

Before EINSTEIN was introduced, federal agencies reported cyber threats to DHS manually and on an ad hoc basis.[62] It was usually done after the agency systems were affected by the attack. To remedy this, DHS, in collaboration with NSA, created EINSTEIN—a system to detect and report network intrusions. EINSTEIN's mandate derived from a combination of statutes, presidential directives, and agency memoranda. The first mandates for EINSTEIN came in 2002 with the Homeland Security Act and Homeland Security Presidential Directive 7.[63] In 2007, the Office of Management and Budget required all federal executive agencies to develop a comprehensive plan of action to defend against cyber threats.[64] Coinciding with these statutory and administrative directives, DHS and NSA launched EINSTEIN in three phases, each increasingly more sophisticated than the last.

DHS rolled out EINSTEIN 1 in 2004 to automate the process by which federal agencies reported cyber threats to the United States Computer Emergency Readiness Team (US-CERT), the operational arm of DHS's cybersecurity division.[65] Under EINSTEIN 1, federal agencies voluntarily sent "flow records" of Internet network activity to DHS so it could monitor the Internet traffic across the federal .gov domain. These flow records included basic routing information such as the IP addresses of the connecting computer and the federal computer connected to.[66] US-CERT used this information to detect and mitigate malicious activity that threatened federal networks. This information was shared with both public and private actors on the DHS website.[67]

In an effort to upgrade EINSTEIN's capabilities, DHS launched EINSTEIN 2, which is capable of alerting US-CERT of malicious network intrusions in near-real time.[68] Sensors installed at all federal agency Internet access points make a copy of all network activity coming to and from federal networks, including addressing information and the content of the communication.[69] These data are later scanned for the presence of "signatures," patterns that correspond to a known threat, such as denial of service attacks, network backdoors, malware, worms, Trojan horses, and

---

[62] DEP'T OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT: EINSTEIN PROGRAM, at 3 (2004) (hereinafter EINSTEIN 1 PRIVACY IMPACT ASSESSMENT), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_eisntein.pdf.

[63] *Id.* at 1.

[64] Office of Management and Budget, Memorandum for the Heads of Executive Departments and Agencies: Implementation of Trusted Internet Connections (TIC) (November 20, 2007), available at http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-05.pdf.

[65] EINSTEIN 1 PRIVACY IMPACT ASSESSMENT, *supra* note 94 at 4.

[66] *Id.* at 6-7. An IP address is a unique identifier used by most computers when sending data over the Internet. It is akin to a personal telephone number or street address. *See* Stephanie Crawford, *What is an IP address?*, HOW STUFF WORKS, http://computer.howstuffworks.com/internet/basics/question549.htm.

[67] See http://www.us-cert.gov/cas/techalerts/ for an example of cybersecurity alerts provided to the public.

[68] DEP'T OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT: EINSTEIN 2, at 1 (2008) (hereinafter EINSTEIN 2 PRIVACY IMPACT ASSESSMENT), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf.

[69] *Id.* at 9. For more information on intrusion detection systems, see NAT'L INSTITUTE OF STANDARDS AND TECH., GUIDE TO INTRUSION DETECTION AND PREVENTION SYSTEMS (IDPS) (2007) (Pub. No. 800-94), available at http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf (hereinafter "NIST REPORT").

routing anomalies.[70] The system triggers an alert when it senses malicious activity. All the data corresponding with the trigger, including the content of the communication, are saved.[71] Personnel at US-CERT then analyze the stored messages and act accordingly.

In 2010, DHS began testing EINSTEIN 3 on one federal agency.[72] In addition to *detecting* cyber threats, this newest iteration also is designed to *block* and *respond* to these threats before any harm is done.[73] US-CERT is also testing the ability of EINSTEIN 3 to provide real-time information sharing with other federal agencies and the NSA.[74]

EINSTEIN and the Fourth Amendment

There is no doubt that EINSTEIN's monitoring of all communications coming to and from federal agency computers poses significant privacy implications—a concern acknowledged by DHS, interest groups, academia, and the general public.[75] This program affects not only federal employees, but also any private citizen who communicates with them. DHS has developed a set of procedures to address these concerns, such as minimization of information collection, training and accountability requirements, and retention rules. Notwithstanding these steps, growth of this Internet monitoring program may trigger privacy interests protected under the Fourth Amendment.

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."[76] The principal purpose of the Fourth Amendment is to protect the privacy of individuals against invasion from government officials.[77] Not all government acts, however, trigger Fourth Amendment protections. For the Fourth Amendment to apply, a court must first inquire whether the governmental act constitutes a *search* or *seizure* in the constitutional sense.[78] To determine if a *search* has occurred, a court will ask whether the individual had an actual expectation of privacy that society would deem reasonable.[79] If yes, the court will then ask if the search was reasonable—the core Fourth Amendment requirement.[80] Except in well-defined

[70] NIST REPORT, *supra* note 101, at 9-5.

[71] EINSTEIN 2 PRIVACY IMPACT ASSESSMENT, *supra* note 100, at 10.

[72] According to DHS, the name of the agency is classified. DEP'T OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT: INITIATIVE THREE EXERCISE, at 3 (2010) (hereinafter EINSTEIN 3 PRIVACY IMPACT ASSESSMENT) available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_initiative3.pdf.

[73] *Id.* at 3.

[74] *Id.* at 4.

[75] *See*, *e.g.*, DEP'T OF HOMELAND SECURITY, PRIVACY COMPLIANCE REVIEW OF THE EINSTEIN PROGRAM (2012) (hereinafter EINSTEIN PRIVACY COMPLIANCE REVIEW), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_privcomrev_nppd_ein.pdf; THE CONSTITUTION PROJECT, RECOMMENDATIONS FOR THE IMPLEMENTATION OF A COMPREHENSIVE AND CONSTITUTIONAL CYBERSECURITY POLICY (2012) (hereinafter THE CONSTITUTION PROJECT), available at http://www.constitutionproject.org/pdf/TCPCybersecurityReport.pdf; Jack Goldsmith, *The Cyberthreat, Government Network Operations, and the Fourth Amendment* (2010), available at http://www.brookings.edu/papers/2010/1208_4th_amendment_goldsmith.aspx.

[76] U.S. CONST. amend. IV.

[77] Camara v. Mun. Ct., 387 U.S. 523, 528 (1967).

[78] Kyllo v. United States, 533 U.S. 27, 32-33 (2001).

[79] This formulation for determining whether a search of seizure occurred derives from Justice Harlan's concurrence in *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[80] Texas v. Brown, 460 U.S. 730, 739 (1983).

instances, a search is not reasonable unless the government obtains a warrant based upon probable cause.[81] There are, however, exceptions to this rule such as special needs and consent that will be explored below.

There seems to be a consensus in federal courts that Internet users are not entitled to privacy in the non-content, routing information of their Internet communications.[82] In *United States v. Forrester*, the government obtained court permission to install a device similar to a pen register to record the to/from addresses of the defendant's emails, the IP addresses of the sites he visited, and the total volume of data sent to and from his account.[83] The Ninth Circuit Court of Appeals held that these surveillance techniques were indistinguishable from the pen register upheld by the Supreme Court in *Smith v. Maryland*.[84] Internet users should be aware, the panel reasoned, that this routing information is provided to the Internet service provider for the purpose of directing the information.[85]

On the other hand, the cases generally demonstrate that an individual has a legitimate expectation of privacy in the *content* of a communication. In *United States v. Warshak*, the Ninth Circuit ruled that a "subscriber enjoys a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a commercial ISP."[86] In an earlier case, the Second Circuit opined that Internet users have an expectation of privacy in the content of the e-mail while in transmission.[87] Although the Supreme Court declined to resolve this issue in *City of Ontario v. Quon*, deciding the case on other grounds, it opined in dicta that "cell phones and text message communications are so pervasive that some persons may consider them to be an essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy."[88]

This content/non-content distinction is as old as Fourth Amendment case law.[89] In the late 19th century, the Court explained in *Ex parte Jackson* that the outside of a mailed letter—its "outward form and weight"—was not entitled constitutional protection.[90] However, the government must

[81] Mincey v. United States, 437 U.S. 385, 390 (1978). Probable cause has been defined as "the facts and circumstances within the officers' knowledge and of which they had reasonably trustworthy information are sufficient in themselves to warrant a man of reasonable caution in the belief that an offense has been or is being committed." Brinegar v. United States, 338 U.S. 160, 175 (1948).

[82] United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2007) (holding no reasonable expectation of privacy in the to/from line addresses of e-mails and IP address of websites visited); United States v. Christie, 624 F.3d 558, 574 (3rd Cir.) (holding no reasonable expectation of privacy in IP address); United States v. Perrine, 518 F.3d 1196, 1205 (10th Cir.) (holding no reasonable expectation of privacy in Internet subscriber information given to Internet service provider).

[83] United States v. Forrester, 512 F.3d at 511. A pen register is a device that records the numbers dialed from a telephone. 18 U.S.C. §3127(3).

[84] *Id.* at 510. In *Smith v. Maryland*, the Court held that the use of a pen register—a device that obtains the telephone numbers dialed from a certain phone—was not a search under the Fourth Amendment. 442 U.S. 735, 745-46 (1979).

[85] *Forrester*, 512 F.3d at 510.

[86] United States v. Warshak, 631 F.3d 266, 287 (6th Cir. 2010) (internal quotation marks omitted).

[87] United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004).

[88] City of Ontario v. Quon, 130 S. Ct. 2619, 2630 (2010).

[89] *See* Orin Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1022-29) (2010) (analogizing the content/non-content distinction developed in the Fourth Amendment letter and telephone cases with Internet communications).

[90] *Ex parte* Jackson, 96 U.S. 727, 733 (1878); *Forrester*, 512 F.3d at 511 (citing *Ex parte* Jackson, 96 U.S. at 733).

obtain a warrant before examining the contents of a letter or sealed package.[91] The Court protected the inside contents of the letter, but held that the outside, non-content material was not entitled to (in modern parlance) a reasonable expectation of privacy. This same rule was carried over to the telephone context.[92] In *Katz v. United States*, the Court held that the contents of Katz's conversation—the actual words spoken—were protected under the Fourth Amendment.[93] A decade later the Court completed the other side of the doctrine in *Smith v. Maryland*, and held that a person has no expectation of privacy in the non-content, routing information of the telephone call—the numbers dialed.[94]

EINSTEIN 2 not only collects the routing, non-content portions of communications, such as e-mail header information, but also scans and collects the content of the communications, such as the body of e-mails.[95] Based on the reasoning of the Internet content cases, individuals most likely have a reasonable expectation of privacy in those electronic communications.[96] The EINSTEIN program requires a Fourth Amendment inquiry into two discrete classes of individuals: (1) federal agency employees who access federal networks while at work; and (2) private persons who either contact a federal agency directly or who communicate via the Internet with a federal employee.[97] The Fourth Amendment rights of the former primarily rest on cases dealing with privacy in the workplace and consent, while the latter requires a broader look at privacy and electronic communications.

Monitoring Communications from Federal Employees

As work and personal lives can become enmeshed, many employees are accessing not only work e-mail while on the clock, but also personal e-mails. EINSTEIN monitors not only federal executive agency employees' work e-mails or other official Internet activity, but also any information accessed on a federal agency computer including personal e-mails accessed from sites such as Gmail or Hotmail, or other Internet communications such as Facebook and Twitter. This poses several Fourth Amendment issues.

---

[91] *Ex parte* Jackson, 96 U.S. at 733.

> The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be. Whilst in the mail, they can only be opened and examined under like warrant, issued upon similar oath or affirmation, particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household. No law of Congress can place in the hands of officials connected with the postal service any authority to invade the secrecy of letters and such sealed packages in the mail; and all regulations adopted as to mail matter of this kind must be in subordination to the great principle embodied in the fourth amendment of the Constitution.

Id.

[92] Kerr, *supra* note 121, at 1023-24.

[93] Katz v. United States, 389 U.S. 347, 359 (1967)

[94] Smith v. Maryland, 442 U.S. 735, 745-46 (1979).

[95] EINSTEIN PRIVACY COMPLIANCE REVIEW, *supra* note 107, at 5.

[96] *See* 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, 33 Op. O.L.C. 1, *11 (2009) (hereinafter Legal Issues Relating to EINSTEIN 2.0), available at http://www.justice.gov/olc/2009/e2-issues.pdf.

[97] There is also a third category of cases: where a federal employee sends a communication while on the federal network to a private person. Because the principles that apply to communications from a private person to a federal employee are the same as the principles that apply to communications from a federal employee to a private person, these two categories will be discussed jointly.

In *City of Ontario v. Quon*, the Supreme Court upheld under the Fourth Amendment the city's search of text messages sent on a city-issued pager by a police officer employed by that city.[98] Before issuing the pagers, the city had announced a usage policy that informed the officers that the city reserved the right to monitor the use of the pager including e-mail and Internet use, with or without notice to the employee.[99] The Court assumed without deciding that the employee had a reasonable expectation of privacy in the sent text messages, that the review of text messages constituted a search, and that the same rules that apply to a search of an employee's office apply equally to an intrusion into his electronic communications.[100] Further, the Court declined to decide which Fourth Amendment employment-based test from *O'Connor v. Ortega* applied—the plurality's "operational realities" test that looked at the specific facts of the employment situation on a case-by-case basis, or Justice Scalia's private employment equivalence test—because the Court decided the case on narrower grounds.[101]

The Court instead relied on the special needs exception to the warrant requirement, which holds that in certain limited instances a government employer need not get a warrant to conduct a search. When a government employer conducts a warrantless search for a "non-investigatory, work-related purpose," it does not violate the warrant requirement if it is "justified at its inception and if the measures are reasonably related to the objective of the search and not excessively intrusive in light of the circumstances giving rise to the search."[102] In the Court's judgment, the city had a "legitimate work-related rationale," and the scope of the search was reasonable and not "excessively intrusive."[103]

Like the city communication policy in *Quon*, as a condition of enrolling in EINSTEIN 2, each federal agency is required to enter into an agreement with DHS that certifies that certain log-on banners or computer user agreements are used to ensure employees are aware of and consent to the monitoring, interception, and search of their communications on federal systems.[104] Applying the "operational realities" test from *O'Connor*, the Department of Justice's Office of Legal Counsel posits that use of the log-on banners on all federal computers will eliminate any expectation of privacy in communications transmitted over those systems.[105] Professor Orin Kerr takes a different approach, treating the terms of service of an Internet service contract—the equivalent to a log-on banner—as consent rather than an outright elimination of a reasonable expectation of privacy.[106] Under either approach, the conclusion reached is likely the same—the monitoring is in all likelihood reasonable.[107] However, *Quon* was limited to searches for a

[98] City of Ontario v. Quon, 130 S. Ct. 2619, 2624 (2010). For an in-depth treatment of *Quon*, see CRS Report R41344, *Public Employees' Right to Privacy in Their Electronic Communications: City of Ontario v. Quon in the Supreme Court*, by Charles Doyle.

[99] *Quon*, 130 S. Ct. at 2625.

[100] *Id.* at 2630.

[101] *Id.* at 2630.

[102] *Id.* at 2631.

[103] *Id.* (internal citations omitted).

[104] Legal Issues Relating to EINSTEIN 2.0, *supra* note 128, at *11.

[105] *Id.* at 32-33.

[106] Kerr, *supra* note 121, at 1031.

[107] *See also* THE CONSTITUTION PROJECT, *supra* at note 107, at 14 ("For federal employees, the analysis that employees consent to having Einstein monitor communications is likely reasonable given the overwhelming importance of protecting key federal agency networks.").

"noninvestigatory work-related purpose."[108] If EINSTEIN could be construed as overreaching this permissible purpose, say, by scanning e-mails for unlawful activity instead of simply malicious computer activity, a court may find its scope beyond *Quon*'s holding. Further, *Quon* insisted that these work-related investigations not be "excessively intrusive."[109] A reasonable argument could be made that monitoring the content of every employee communication is excessively intrusive. Additional questions remain. For instance, what is the scope of a non-investigatory, work-related purpose? Does scanning for malicious activity qualify as a work-related purpose? Does *United States v. Jones*'s physical intrusion test apply here where the employee's electronic *papers* and *effects* are being scanned?[110] Because no court has confronted a program like EINSTEIN, answers to these questions are unclear.

Monitoring Communications from Private Persons to Federal Employees

EINSTEIN not only monitors the computer activity of federal agency employees, but also any communications sent by a private person to a federal employee on his governmental e-mail or personal e-mail. One may argue that these concerns are more serious than in the employment context, on the theory that there is neither a presumption that an individual's privacy rights are diminished nor has the private actor consented to monitoring by clicking on a log-on banner or user agreement that would inform him of the privacy implications of his communication.

Some would argue that the third-party doctrine permits EINSTEIN's monitoring of private parties.[111] Traditionally, there has been no Fourth Amendment protection for information voluntarily conveyed to a third-party.[112] This doctrine dates back to the "secret agent" cases, in which any words uttered to another person, including a government agent or informant, were not covered by the Fourth Amendment.[113] Because federal employees have agreed to permit governmental monitoring of their communications, the Office of Legal Counsel (OLC) argues they are permitting *ex ante* surveillance of all their communications, including those from private persons to the federal employee's personal e-mail.[114]

---

[108] *Quon*, 130 S. Ct. at 2631.

[109] *Id.*

[110] Another possible approach is that taken in *United States v. Jones*, 565 U.S. ___ (2012) (slip op.), in which the Court held that a physical intrusion into a constitutionally protected area—there, the defendant's car (an effect)—coupled with an attempt to obtain information, was a Fourth Amendment search. If a court concluded that an e-mail is a paper (or packet of data, an effect), protected under the Fourth Amendment's catalog of protected areas (persons, houses, papers, and effects), the *Jones* physical intrusion analysis may call into question whether EINSTEIN's surveillance is constitutionally permissible.

[111] Legal Issues Relating to EINSTEIN 2.0, *supra* note 128, at 35-36 (citing Smith v. Maryland, 442 U.S. 735, 743-44) (1979).

[112] *United States v. Miller*, 425 U.S. 435 (1976) holding that financial statements and deposit slips transmitted to bank were not protected from police inquiry because they had been turned over to a third party); *Smith*, 442 U.S. 735. It should be noted that in *United States v. Jones*, Justice Sotomayor opined that it "may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." United States v. Jones, 565 U.S. ___, 5 (Sotomayor, J., concurring in the judgment and the opinion).

[113] United States v. White, 401 U.S. 745, 750 (1971) (holding that the Fourth Amendment "affords no protection to a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.") (internal quotation marks omitted).

[114] Legal Issues Relating to EINSTEIN 2.0, *supra* note 128, at 36-37.

However, the third-party cases have traditionally applied only to non-content information. In *Smith v. Maryland*, the Court noted that pen registers only disclose the telephone numbers dialed: "[n]either the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers."[115] The case rested on the devices "limited capabilities."[116] The Ninth Circuit borrowed this reasoning in *Forrester*, where the panel distinguished "mere addressing" in an e-mail such as the to/from line, from "more content-rich information" such as the text in the body of an e-mail.[117] And as noted in *United States v. Warshak*, people still should expect privacy in the content of their telephone calls despite the ability of an operator to listen.[118] Further, the Supreme Court has noted that "the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards."[119] These cases severely diminish the argument that the third-doctrine permits absolute access to private communications. Instead, it could be reasonable to conclude from these cases that the third-party doctrine would permit access to the routing information of Internet communications, but might not go so far as to allow monitoring of the content of those communications.

Additionally, the OLC contends that under the "secret agent" cases the government can monitor private communications even if the sender is unaware that the recipient is a federal employee or did not anticipate that the communication would be opened on a federal computer.[120] The "secret agent" cases generally hold that "when a person communicates to 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."[121] Because these cases do not limit the instances this rule can be applied, it seems reasonable that they can be applied to EINSTEIN.

Alternative to Traditional Warrant Requirement

Assuming both federal employees and those communicating with them have a reasonable expectation of privacy in the contents of their communications, EINSTEIN must be tested under the general reasonableness requirement of the Fourth Amendment. A search is generally unreasonable without a warrant or some individualized suspicion.[122] However, under the "special needs exception" cases, the Court has held that when there are special governmental needs, beyond normal law enforcement, the government may need neither a warrant nor any level of individualized suspicion.[123] To determine whether the special needs exception applies, the Court balances the individual's privacy expectations against the governmental interest at stake.[124] This rule has been used to support certain police searches at checkpoints such as sobriety

[115] *Smith*, 442 U.S. at 741 (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 167 (1977)).

[116] *Id.* at 742.

[117] United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2007).

[118] United States v. Warshak, 631 F.3d 266, 285 (6th Cir. 2007).

[119] United States v. U.S. Dist. Ct., 407 U.S. 297, 313 (1972).

[120] Legal Issues Relating to EINSTEIN 2.0, *supra* note 128, at 39.

[121] SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735, 743 (1984).

[122] Chandler v. Miller, 520 U.S. 305, 308 (1997).

[123] Nat'l Treasury Emplys. Union v. Von Raab, 489 U.S. 656, 665-66 (1989).

[124] *Id.*

roadblocks,[125] border searches,[126] and checkpoints looking for a witness to a crime.[127] However, the Court did not permit a drug interdiction checkpoint when the "primary purpose was to detect evidence of ordinary criminal wrongdoing."[128]

Here, an argument could be made that the nature of cybersecurity and the impracticability of obtaining a warrant might justify application of the special needs doctrine to the EINSTEIN program.[129] The ostensible primary purpose of the program's cybersecurity measures is not for ordinary law enforcement needs, but instead to protect the critical infrastructure of the nation. Moreover, the government will need to act quickly if the program is to be feasible.[130] It could also be argued, however, that unless the threat required immediate review, a government agency should obtain a warrant based upon probable cause to review personally identifiable information, or, at a minimum, review the communications in a redacted format that includes only the threat information and no personally identifiable information.[131] As one commentator noted, it is nearly impossible to predict what is reasonable without knowing the severity of the cybersecurity threat and the exact measures taken to meet it.[132]

Privacy and Civil Liberties Oversight

In addition to the Fourth Amendment, there may be other mechanisms for protecting the privacy of Internet users. Indeed, the Constitution is only the floor for privacy protections. In many instances, Congress and state legislatures have created privacy protections beyond what is protected under their respective constitutions. These include statutes such as the Electronic Communications Privacy Act[133] and the Privacy Act of 1974.[134]

As to existing privacy protections, EINSTEIN has several privacy safeguards. For example, federal agencies are required to post notices on their websites that computer security information is being collected.[135] The computer programs recording network flow records strip down the information so that minimal content information is exposed.[136] Further, only the raw computer network traffic that contains malicious activity is viewed by DHS personnel; any "clean" traffic is promptly deleted from the system.[137] Information is only collected when it relates to an actual

[125] Michigan Dep't of State Police v. Sitz, 496 U.S. 444, 455 (1990).

[126] United States v. Ramsey, 431 U.S. 606 (1977).

[127] Illinois v. Lidster, 540 U.S. 419, 428 (2004).

[128] City of Indianapolis v. Edmond, 531 U.S. 32, 38 (2000).

[129] Legal Issues Relating to EINSTEIN 2.0, *supra* note 128, at 54.

[130] Goldsmith, *supra* note 75, at 14.

[131] THE CONSTITUTION PROJECT, *supra* note 107, at 16.

[132] Goldsmith, *supra* note 75, at 13.

[133] Electronic Communications Privacy Act of 1986, P.L. 99-508, 100 Stat. 1848.

[134] Privacy Act of 1974, P.L. 93-579, 88 Stat. 1896.

[135] EINSTEIN 1 PRIVACY IMPACT ASSESSMENT, *supra* note 94, at 9.

[136] EINSTEIN 2 PRIVACY IMPACT ASSESSMENT, *supra* note 100, at 12.

[137] *Id.*

cyber threat.[138] Analysts handling the monitored communications are given privacy training on an annual basis.[139] These privacy protections are handled internally within DHS.

Jack Goldsmith, former head of the Office of Legal Counsel, has proposed a system of four oversight mechanisms similar to the Foreign Intelligence Surveillance Court[140] to ensure the reasonableness of the searches under EINSTEIN: (1) independent *ex ante* scrutiny to ensure that the governmental procedures stay within their statutory authority; (2) privacy protections such as minimization procedures, also subject to *ex ante* judicial review; (3) *ex post* oversight mechanisms, in which the Attorney General and the Director of National Intelligence report to Congress every six months regarding privacy compliance and the inspectors general from each agency also report to Congress on a yearly basis; and (4) a sunset provision requiring Congress to reapprove the regime four years into operation.[141]

Others have proposed there be some form of independent oversight beyond DHS's privacy office.[142] Additionally, there are proposals that content of communications not be shared with law enforcement officials or used in any non-cyber crime investigation, unless the data were obtained as part of a legitimate cybersecurity threat.[143]

Legal Issues Related to Cybersecurity Threat Information Sharing

Many policymakers have argued that there is a need for the federal government and owners and operators of the nation's critical infrastructures to share information on vulnerabilities and threats, and to promote information sharing between the private and public sectors in order to protect critical assets from cybersecurity threats. Private sector entities may wish to share information with one another about threats they have faced or are currently facing. They may also wish to collaborate in devising solutions to these security issues. Additionally, the government may have information about cybersecurity threats that would be similarly useful to potential targets in the private sector. The government may also see value in having access to information from the private sector about cybersecurity threats.

Obstacles to information sharing may exist in current laws protecting electronic communications or in antitrust law. The Fourth Amendment, the Telecommunications Act of 1934, and state laws may also affect the legality of information sharing by the private sector. Entities that share information may also be concerned that sharing or receiving such information may lead to civil and criminal liability, or that shared information may contain proprietary or confidential information that could be disclosed to competitors or government regulators.

---

[138] EINSTEIN PRIVACY COMPLIANCE REVIEW, *supra* note 107, at 4.

[139] *Id.* at 7.

[140] The Foreign Intelligence Surveillance Court is a comprised of 11 federal district court judges who are designated by the Chief Justice to hear applications for surveillance orders authorized under the Foreign Intelligence Surveillance Act of 1978. 50 U.S.C. §1803.

[141] Goldsmith, *supra* note 75, at 14.

[142] THE CONSTITUTION PROJECT, *supra* note 107, at 28.

[143] *Id.*

Electronic Communications Privacy Act[144]

Some have argued that the framework provided by the Electronic Communications Privacy Act (ECPA) may be an obstacle to sharing cyber threat information among communications service providers or between such entities and the government,[145] and may prevent them from acting to protect their customers and networks. ECPA generally prohibits (1) the interception of wire, oral, or electronic communications (wiretapping);[146] (2) access to the content of stored electronic communications and to communications transaction records;[147] and (3) the use of trap and trace devices and pen registers.[148]

ECPA generally prohibits intercepting wire, oral, or electronic communications by means of an electronic, mechanical, or other device, but sets forth a number of exceptions to the general prohibition.[149] Relevant to this discussion, ECPA provides a general exemption for communications service providers, permitting them to intercept communications when incidental to "the rendition of service or the protection of the rights or the property of the provider of that service," or protecting themselves against fraud.[150] This exemption does not apply to random monitoring except where used for mechanical or service quality control checks. Communications service providers are also permitted to intercept communications in order to assist federal and state officials operating under a judicially supervised interception order,[151] and for the regulatory activities of the Federal Communications Commission.[152] In addition, communications service providers are permitted to intercept communications with customer consent.[153]

Under the stored communications provisions of ECPA, providers of electronic communication services (ECS) to the public may not disclose the contents of any "communication while in electronic storage by that service."[154] Public remote computer service (RCS) providers similarly may not disclose the contents of

> any communication which is carried or maintained on that service – (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; (B) solely for the purpose of providing storage or

[144] See CRS Report 98-326, *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*, by Gina Stevens and Charles Doyle for a more detailed discussion of the federal laws governing wiretapping and electronic eavesdropping, along with appendices including copies of the texts of ECPA and FISA. *See also* CRS Report R41733, *Privacy: An Overview of the Electronic Communications Privacy Act*, by Charles Doyle.

[145] *See*, *e.g.*, Aaron J. Burstein, *Amending the ECPA to Enable a Culture of Cybersecurity Research*, 22 HARV. J.L. & TECH. 167 (2008).

[146] 18 U.S.C. §§2510-2522.

[147] 18 U.S.C. §§2701-2712.

[148] 18 U.S.C. §§3121-3127. Pen registers capture the numbers dialed on a telephone line; trap and trace devices identify the originating number of a call on a particular phone line. *See* 18 U.S.C. §3127(3)-(4). The USA PATRIOT Act enlarged the coverage of the Pen Register Statute to include sender/addressee information relating to email and other forms of electronic communications. P.L. 107-56, §216(c)(2).

[149] 18 U.S.C. §2511.

[150] 18 U.S.C. §2511(2)(a)(i), (h).

[151] 18 U.S.C. §2511(2)(a)(ii).

[152] 18 U.S.C. §2511(2)(b).

[153] 18 U.S.C. §2511(2)(c).

[154] 18 U.S.C. §2702(a)(1).

> computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.[155]

Both ECS and RCS providers may not disclose any "record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by [the disclosure restrictions described above]) to any government entity."[156]

However, the statute does provide a number of exceptions under which an ECS or RCS provider may disclose the contents of a communication. These exceptions cover disclosures made

- to the addressee or intended recipient of the communication;
- with the consent of the sender, addressee, or intended recipient of the communication, or to the subscriber in the case of remote computing service;
- in order to forward such communication to its destination;
- as may be necessarily incident to the rendition of the service or *to the protection of the rights or property of the service provider*;
- to the National Center for Missing and Exploited Children;
- to law enforcement if the contents were inadvertently obtained by the service provider and appear to pertain to the commission of a crime; and
- to a government entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure.[157]

With respect to pen registers and trap and trace devices, ECPA outlaws installation or use of a pen register or trap and trace device, except under one of seven circumstances:

- pursuant to a court order issued under Sections 3121-3127 (pen registers and trap and trace devices);
- pursuant to a Foreign Intelligence Surveillance Act (FISA) court order;[158]
- with the consent of the user;
- when incidental to service;
- when necessary to protect users from abuse of service;
- when necessary to protect providers from abuse of service;[159] or
- in an emergency situation.[160]

---

[155] 18 U.S.C. §2702(a)(2).

[156] 18 U.S.C. §2702(a)(3).

[157] 18 U.S.C. §2702(b) (emphasis added). The record disclosure exceptions are similar. 18 U.S.C. 2702(c).

[158] 18 U.S.C. §3121 ("Except 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 under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.)").

[159] 18 U.S.C. §3121(b).

[160] 18 U.S.C. §3125(a).

The statute permits service providers to conduct random monitoring of communications in order to perform mechanical or service quality control checks; however, these purposes may not sufficiently capture the wholesale monitoring of networks to detect or intercept cyber threats.[161] Additionally, the restrictions on voluntary disclosures of the contents of communications and addressing information are generally limited to the purpose of protecting the service provider's rights or property. Consequently, ECPA may hinder sharing of information about cyber threats where the service provider is not the target of the threat. Given this uncertainty, providers may be hesitant to share cyber threat information as violating ECPA can expose them to criminal penalties and private civil liability. As a result, some cybersecurity proposals may include explicit authority, notwithstanding the provisions of ECPA, for providers to monitor communications networks for cybersecurity threat information, and to share such information with other providers or the government.

Antitrust Law

Companies may be assisted in combating cybersecurity threats by sharing information with one another about threats they have faced or are currently facing. Companies may also wish to collaborate in devising solutions to these security issues. The antitrust laws are often cited as an impediment to such collaboration. This is so because if a collaboration is found to violate antitrust laws, the collaborating entities may be subject to civil and criminal penalties.[162]

Section 1 of the Sherman Antitrust Act prohibits contracts, combinations, and conspiracies in restraint of trade.[163] The Supreme Court has found that not all contracts or combinations that restrain trade are forbidden by the Sherman Act; rather, only those agreements that unreasonably restrain trade are prohibited.[164] Nonetheless, when competitors share information with one another, concerns regarding violations of the antitrust laws may arise.[165] The sharing of information may create the opportunity to conspire to fix prices, restrain output, or otherwise agree to unreasonably restrain competition to the detriment of consumers.

Two types of analyses are used to determine the lawfulness of collaborative activity among competitors: per se and rule of reason.[166] The per se analysis is applied to collaborations that have been found to be always or almost always in violation of the antitrust laws because they result in raising prices or reducing output without any appreciable benefit to competition.[167] Only the most egregious collaborations, such as those to fix prices, rig bids, or reduce output, are considered to be per se illegal.[168] All other collaborations among competitors are subject to review under the

[161] 18 U.S.C. §2511(2)(a)(i).

[162] 15 U.S.C. §§1, 4, 15, 26.

[163] 15 U.S.C. §1.

[164] Standard Oil Co. of N.J. v. U.S., 221 U.S. 1, 60 (1911) (interpreting the language of Section One to require that in order for restraints in trade to be considered unlawful, the methods used to restrain the market must be undue or unreasonable).

[165] *See* Fed. Trade Comm'n & U.S. Dep't of Justice, Antitrust Guidelines for Collaborations Among Competitors (2000), available at http://www.ftc.gov/os/2000/04/ftcdojguidelines.pdf (hereinafter Competitor Collaboration Guidelines).

[166] Nat'l Soc'y of Prof'l Eng'rs v. United States, 435 U.S. 679, 692 (1978).

[167] Business Electronics Corp. v. Sharp Electronics Corp., 485 U.S. 717, 723 (1988).

[168] Competitor Collaboration Guidelines, *supra* note 208, at 3.

rule of reason standard.[169] The rule of reason consists of a flexible inquiry into the potential competitive benefits of an agreement as they are weighed against the potential competitive harms. Most agreements to share information will likely be reviewed under the rule of reason standard.[170] Most collaborations among competitors that exist for the sole purpose of combating cybersecurity threats would be analyzed under the rule of reason standard.

Collaboration among competitors may include a wide variety of activity including research and development, shared manufacturing facilities, and other joint ventures.[171] Agreements to share information may be a part of other broader collaborative activities, or an end unto themselves. The Department of Justice (DOJ), and the Federal Trade Commission (FTC) recognize that information sharing among competitors often has pro-competitive and efficiency-enhancing benefits that may outweigh any anticompetitive risks.[172] The DOJ and the FTC, therefore, have devised guidelines to aid companies in developing collaborative business plans that minimize antitrust concerns.[173] The first aspect of the agreement that the agencies will examine is the extent of the collaboration and the purpose for the collaboration.[174] To the extent that the sharing of information is limited to the purpose of aiding in combating cybersecurity threats, it is likely that the antitrust concerns raised by any potential agreement would be limited as well.[175]

Groups of competitors wishing to collaborate to combat cybersecurity threats, even when following the DOJ and FTC's guidelines, may nonetheless be concerned about antitrust scrutiny. To aid these groups, the DOJ has developed a process for the groups to submit their plans to collaborate to the DOJ for a determination by the agency of whether the proposed collaboration would raise antitrust concerns.[176] It is called the Business Review Procedure. The procedure has been used in the cybersecurity context in the past. For example, the Electric Power Research Institute (EPRI) requested that the DOJ review its proposal to share information related to cyber threats. After examining the proposal, the DOJ issued a business review letter stating that the DOJ was not inclined to initiate an antitrust enforcement action against the collaborative efforts of EPRI on the theory that the proposal would reduce cybersecurity costs and may have a pro-competitive effect.[177] Nonetheless, the DOJ, as it always does in these circumstances, reserved the right to pursue any antitrust concerns should the collaborative effort prove to have a future anticompetitive effect.

Cybersecurity legislative proposals may explicitly provide that the act of sharing cyber threat information would not be considered a violation of the antitrust laws, if shared to assist with

---

[169] *Id*.

[170] Continental T.V. Corp. v. GTE Sylvania Corp., 433 U.S. 36, 49 (1977).

[171] Competitor Collaboration Guidelines, *supra* note 208, at 6-7.

[172] *Id*. at 1.

[173] *Id*.

[174] *Id*. at 12.

[175] See Letter from Joel I. Klein, Assistant Attorney General, Department of Justice, Antitrust Division, to Barbara Greenspan, Associate General Counsel, Electric Power Research Institute, Inc. (October 2, 2000), *available at* http://justice.gov/atr/public/busreview/6614.htm.

[176] 28 C.F.R. §50.6.

[177] Letter from Joel I. Klein, Assistant Attorney General, Department of Justice, Antitrust Division, to Barbara Greenspan, Associate General Counsel, Electric Power Research Institute, Inc. (October 2, 2000), *available at* http://justice.gov/atr/public/busreview/6614.htm.

information security. However, such proposals may also specify that shared information may not be used to obtain an unfair competitive advantage.

Liability for Information Sharing

Some have argued that sharing or receiving information about cybersecurity threats could potentially expose private sector entities to increased liability. To the extent that ECPA, antitrust laws, or other federal or state laws prohibit private sector entities from sharing cybersecurity threat information amongst themselves or with the government, violating these laws could lead to civil or criminal penalties imposed by the government.[178] Additionally, both ECPA and the antitrust laws provide private rights of action for harmed parties to recover damages from entities that have violated these statutes.[179] Consequently, violating ECPA or the antitrust laws may also expose entities to private civil liability.

Concerns about private civil liability for information sharing may also arise based on the effect that information sharing may have on private civil actions based on injuries caused by a defendant's negligent actions. One way of proving negligence is by convincing a jury that the defendant did not act reasonably in the face of a foreseeable risk.[180] In the absence of a foreseeable risk, a defendant typically has no judicially enforceable duty to mitigate that risk.[181] However, if a defendant has received information about an active cybersecurity threat, then that would tend to show that the risk of attack from such threat was a foreseeable one. In other words, notice of cybersecurity risks might lead a jury to find that the defendant had a duty to act reasonably. For example, if a defendant is using software package X in its information infrastructure, and the defendant receives information from other private sector entities or the government that software package X has been vulnerable to cyberattacks, the receipt of this information may lead a jury to conclude that the defendant was aware of the risk presented by using that software package. If such a duty were found, then the defendant could be liable for any harm that resulted from its negligence.

Receiving information about cybersecurity threats may also be relevant to whether the actions taken by a defendant in the face of a foreseeable risk were reasonable. In order to determine whether a defendant's actions were reasonable, juries are often asked to balance the foreseeable risks of the defendant's actions with the foreseeable risks of the defendant's inaction.[182] For example, shared cybersecurity threat information may include effective and low-cost measures that could be taken to mitigate or prevent a threat. A jury evaluating whether a defendant had acted negligently may find the fact that the defendant had knowledge of effective and low-cost preventative measures may determine that the defendant should be held to a higher standard of care than if the defendant had not received such information.[183]

[178] 15 U.S.C. §§1, 4; 18 U.S.C. §§2511, 2701, 3121.

[179] 15 U.S.C. §§15, 26; 18 U.S.C. §§2520, 2707.

[180] *See*, *e.g.*, First Electric Cooperative Corp. v. Pinson, 642 S.W.2d 301, 303 (Ark. 1982) ("there is no negligence in not guarding against a danger which there is no reason to anticipate").

[181] *Id.*

[182] *E.g.*, Schuldies v. Service Machine Co., 448 F. Supp. 1196, 1199 (E.D. Wis. 1978) ("a person fails to exercise ordinary care when, without intending to do any wrong, he does an act or omits a precaution under circumstances in which a person of ordinary intelligence and prudence ought reasonably to foresee that such act or omission will subject the interests of another to an unreasonable risk of harm").

[183] *E.g.*, Rodriguez v. New Haven, 439 A.2d 421, 424 (Conn. 1981) ("knowledge of a dangerous condition generally (continued...)

In order to address these concerns, cybersecurity legislation may provide some degree of immunity from causes of action based on an entity's use, receipt, or disclosure of cyber threat information, or for any act or omission following the lawful receipt of such information. As with civil liability protections in the context of critical infrastructure regulation,[184] such immunity may be complete or qualified, and may be made contingent upon certain actions taken by the entity seeking immunity. For example, in order to further incentivize sharing of threat information, a proposal may only provide immunity from liability arising from information that the defendant has previously shared with a central cyber threat information exchange. Under such a scenario, a defendant that had received cyber threat information, but had not shared it with an exchange would not receive any immunity from suits based on the defendant's receipt of that information.

Protection of Proprietary or Confidential Business Information

Sharing cybersecurity threat information may raise concerns about how that information would be used. For example, there may be concerns that other businesses could use the information to gain a competitive advantage. There may also be concerns that cybersecurity threat information shared with the government might be used for regulatory purposes unrelated to cybersecurity. As a result, some private sector entities may be hesitant to voluntarily share cybersecurity-related information with other businesses or with the government.

For example, voluntary sharing of cybersecurity threat information with the government may be inhibited by concerns that such information might be made publicly available under the Freedom of Information Act of 1974 (FOIA), which regulates the disclosure of agency records held by the federal government.[185] Other potential obstacles to sharing information with the government are agency rules or judicial doctrine regarding ex parte communications, the rules of discovery in civil litigation, and state open records laws requiring public disclosure.

Information that is designated as critical infrastructure information (CII) under the Critical Infrastructure Information Act (CIIA) is protected from disclosure under FOIA. Similarly, the CIIA provides that CII will not be subject to agency rules or judicial doctrine regarding ex parte communications. With respect to concerns about litigation, CIIA limits the use of CII in civil litigation and provides that sharing CII with the agency does not count as the "waiver of any applicable privilege or protection provided under law," such as trade secret protection or the attorney-client privilege.[186] CIIA also authorizes the use or disclosure of such information by officers and employees in furtherance of the investigation or the prosecution of a criminal act; or for disclosure to Congress or the Government Accountability Office.

Many of these concerns are also raised in the context of protecting information collected from critical infrastructure, and are discussed in more detail *supra* at "Freedom of Information."

(...continued)

requires greater care to meet the standard of reasonable care").

[184] Discussed *supra* at "Liability Concerns."

[185] 5 U.S.C. §552.

[186] *See* FED. R. EVID. 501.

Privacy and Civil Liberties

Privacy and civil liberties advocates argue that some proposed cybersecurity information sharing measures go too far in eroding privacy protections.[187] For instance, some proposals may permit private sector use of cybersecurity systems and sharing of cyber threat information notwithstanding any other provision of law, overriding privacy protections such as ECPA and the Privacy Act of 1974. One commentator noted that although some changes are necessary to authorize cyber activities, a broad exclusion of these laws in the cybersecurity area would be "inconsistent with the promise of privacy that undergirds the Wiretap Act and the SCA."[188]

There is also concern among privacy and civil liberties groups that defense agencies like the National Security Agency (NSA) would have access to Internet information obtained through cybersecurity information sharing programs. Generally, defense agencies are not employed in the domestic law enforcement arena.[189] These groups warn that defense agencies like the NSA are not subject to the same oversight and transparency as civilian agencies such as DHS.[190] Observers point to its warrantless wiretapping program in 2001 as proof that the NSA should not be given control over monitoring of domestic Internet activity.[191] These advocates suggest that any proposed information sharing plan clearly state which civilian agencies will have access to this information.[192] This would prevent, in their view, the NSA or other military agencies from inadvertently getting access to this data.

Preemption

As the body of federal cybersecurity law grows, the possibility that it will preempt conflicting state law will increase with it. After September 11, 2001, states took various measures to protect their critical infrastructure. This included defining "critical infrastructure," creating security standards for these entities, and carving out exceptions under public disclosure laws so vital information would not get into the hands of bad actors.

It is well established that the Supremacy Clause of the United States Constitution can invalidate any state law that interferes with or is contrary to federal law.[193] This is known as preemption. The preemptive effect of a federal statute can be either expressly stated in the statute or implied by the structure and purpose of the legislation.[194] If there is express language, the court will

[187] *See e.g.*, Center for Democracy & Technology, Concerns Mount Over Unresolved Privacy Issues in CISPA, https://www.cdt.org/blogs/greg-nojeim/1804concerns-mount-over-unresolved-privacy-issues-cispa.

[188] *Cybersecurity Information Sharing and the Freedom of Information Act: Hearing Before the S. Comm. on the* Judiciary, 112th Cong. (2012) (statement of Paul Rosenzweig, Visiting Fellow, The Heritage Foundation), *available at* http://www.judiciary.senate.gov/pdf/12-3-13RosenzweigTestimony.pdf.

[189] Under the Posse Comitatus Act, the military is prohibited from executing domestic laws. 18 U.S.C. §1385.

[190] Michelle Richardson, *Cybersecurity Information Sharing Legislation and Privacy Implications in the 112th Congress*, AMERICAN CIVIL LIBERTIES UNION (April 16, 2012), http://www.aclu.org/files/assets/aclu_interested_persons_memo__re__cyber_leg_info_sharing_april_16_2012.pdf.

[191] Greg Nojeim, *Cybersecurity's 7-Step Plan for Internet Freedom*, CENTER FOR DEMOCRACY AND TECHNOLOGY (March 28, 2012), https://www.cdt.org/blogs/greg-nojeim/2803cybersecuritys-8-step-plan-internet-freedom.

[192] *Id.*

[193] Hillsborough County v. Automated Med. Labs., Inc., 471 U.S. 707, 713 (1985).

[194] Gade v. Nat'l Solid Wastes Mgmt. Ass'n, 505 U.S. 88, 98 (1992).

interpret the words used by Congress and assume that the ordinary meaning of the text expresses the legislative purpose.[195] For example, if Congress uses broad language in its preemption provision, the court will construe its preemptive effect broadly.[196] Absent explicit preemptive language, there are two types of implied preemption: (1) field preemption, where the federal regime is "so pervasive to make the reasonable inference that Congress left no room for the States to supplement it";[197] and (2) conflict preemption, where state law "stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress."[198]

Certain categories of state laws may be more likely to be preempted by legislative cybersecurity proposals, such as those state laws that directly regulate industrial facilities. For example, New Jersey has enacted the Toxic Catastrophe Prevention Act, which was designed to prevent the release of hazardous substances from industrial plants and provide an abatement and evacuation plan in the event a catastrophic release occurs.[199] That act requires that an owner or operator of a covered facility establish a risk management program. Likewise, Maryland requires that any facility where hazardous materials are stored analyze the security of the facility every five years in accordance with rules adopted by the Department of State Police.[200] Similarly, New York requires the commissioner of the state division of homeland security to review security measures for all critical infrastructure relating to energy generation and transmission in the state every five years.[201] The state public service commission has the discretion whether to require the owners of these facilities to implement these plans. The application of these and other similar state requirements to covered critical infrastructure may be preempted either explicitly or implicitly by federal cybersecurity legislation. It has been argued in the past that "the law of preemption recognizes that state laws must give way to Federal statutes and regulatory programs to ensure a unified and coherent national approach in areas where the Federal interests prevail—such as national security."[202] Because cybersecurity has been equated with national security, this deference theory could apply here.[203]

Cybersecurity legislation to encourage sharing of cybersecurity threat information may also preempt state laws. For example, all 50 states have included electronic communications in their respective wiretap laws which prohibit the interception and disclosure of certain communications.[204] Federal laws that would permit electronic communications providers to monitor communications networks for cyber threats would likely preempt the application of such state laws to that monitoring.

---

[195] Morales v. TWA, 504 U.S. 374, 383 (1992).

[196] Metropolitan Life Ins. Co. v. Massachusetts, 471 U.S. 724, 739 (1985).

[197] Fidelity Fed. Sav. & Loan Assn. v. De le Cuesta, 458 U.S. 141, 152-53 (1982) (quoting Rice v. Sante Fe Elevator Corp., 331 U.S. 218, 230 (1947)).

[198] Hines v. Davidowitz, 312 U.S. 52, 67 (1941).

[199] N.J. STAT. ANN. §13:1K-19.

[200] MD. ENV. CODE §7-701.

[201] N.Y. EXEC. LAW §713 (2011).

[202] Chemical Facility Anti-Terrorism Standards, 71 *Federal Register* 78,276, 78,293 (December 28, 2006).

[203] *See* President Barack Obama, Remarks on Securing Our Nation's Cyber Infrastructure (May 29. 2009) ("[I]t's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation."), available at http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure; *cf.* Michael Jo, *National Security Preemption: The Case of Chemical Safety Regulation*, 85 N.Y.U. L. Rev. 2065, 2087 (2010).

[204] NATIONAL CONFERENCE OF STATE LEGISLATURES, ELECTRONIC SURVEILLANCE LAW, http://www.ncsl.org/issues-research/telecom/electronic-surveillance-laws.aspx.

State open records laws are another category that would likely be preempted under recent cybersecurity legislation being considered by Congress. Currently, states take a varied approach to exempting security information from state FOIA requirements.[205] Some states, including Indiana[206] and Alabama,[207] provide for specific disclosure exemptions for certain categories of information such as vulnerable assets or security plans. Others states, including Maryland, simply provide that anything protected under the federal FOIA statute is protected under their state statute.[208] Still others have more broadly stated FOIA protections such as "in the public interest," as used in Arkansas.[209] However, cybersecurity legislation may explicitly provide that cybersecurity information shared with state and local governments shall not be subject to any state or local law requiring disclosure of information or records.[210]

Author Contact Information

Edward C. Liu
Legislative Attorney
eliu@crs.loc.gov, 7-9166

Alissa M. Dolan
Legislative Attorney
adolan@crs.loc.gov, 7-8433

Gina Stevens
Legislative Attorney
gstevens@crs.loc.gov, 7-2581

Richard M. Thompson II
Legislative Attorney
rthompson@crs.loc.gov, 7-8449

Kathleen Ann Ruane
Legislative Attorney
kruane@crs.loc.gov, 7-9135

Andrew Nolan
Legislative Attorney
anolan@crs.loc.gov, 7-0602

[205] *See* National Association of Regulatory Utility Commissioners, Information Sharing Practices in Regulated Critical Infrastructure States (2007), http://www.naruc.org/Publications/NARUC%20CIP%20Information%20FIN.pdf.

[206] IND. CODE §5-14-3-4.

[207] ALA. CODE §36-12-40.

[208] MD. CODE ANN. STATE GOV'T §10-615(2).

[209] ARK. CODE. ANN. §23-2-316.

[210] S. 2151, §102(f)(3).