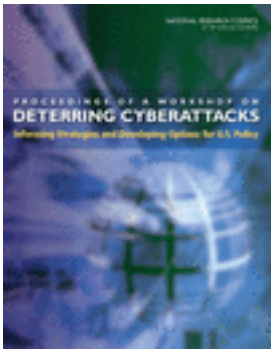

Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy

Committee on Deterring Cyberattacks: Informing Strategies and Developing Options; National Research Council

ISBN: 0-309-16086-3, 400 pages, 8 1/2 x 11, (2010)

Civil Liberties and Privacy Implications of Policies to Prevent Cyberattacks

Robert Gellman
Information and Privacy Consultant

I. INTRODUCTION

The purpose of this paper is to consider the civil liberties and privacy implications of potential policies and processes to prevent cyberattacks. Other than the general topic and a request to consider the possibility of licensing Internet users, little direction was offered. The topic raises a host of unbounded, complex, difficult, and contested legal and constitutional issues. Almost any one of the issues could be the subject of an entire paper, book, or even treatise.

What can be accomplished here is to consider some of the issues raised by possible proposals aimed at preventing cyberattacks and to suggest some of the major fault lines that demarcate the borders of what is possible from what is uncertain from what is prohibited. To characterize the analysis another way, how far can prevention policies and processes go before they hit possible legal, constitutional, or other barriers? This paper is an analysis of *selected* issues raised by this question.

The analysis of any proposal can differ significantly depending on who is performing an activity and where that activity is being performed. The federal government cannot do some things that private companies can do. Some activities would be less objectionable when done in a private, access-controlled network than when done on the Internet in general. Some activities can be more readily accomplished with the consent of data subjects than without consent. The laws of other nations may impose restrictions that are absent in U.S. law, or vice versa, which can complicate prevention of cyberattacks on a global scale.

The discussion here is organized under four main topics, search, speech, information privacy, and due process. Many potential cyberattack prevention policies and processes raise concerns under more than one of these topics, and the placement of issues under these topics is somewhat discretionary. For example, a requirement that Internet Service Providers (ISPs) retain data about a user's Internet activities raises concerns under the First Amendment, Fourth Amendment, privacy, and due process.[1] In this paper, data retention is considered in the search section.

[1]The text of the U.S. Constitution and its amendments can be found at http://topics.law.cornell.edu/constitution, accessed August 30, 2010.

II. ISSUES RELATING TO SEARCH

1. Surveillance

Cyberattack prevention activities will at times make use of the surveillance authority given to the government. It is not possible to summarize that authority in this document. There may be no more convoluted area of privacy law in the United States than surveillance law. One scholar describes the law of electronic surveillance as "famously complex."[2] The standards vary enormously, depending on numerous factors. Some of the factors that determine the nature of the surveillance that is permissible, the procedures that may be required as a prerequisite to surveillance, and the uses of the results of the surveillance include:

- who is undertaking the surveillance (the government or a private party)
- why the surveillance is being conducted (for law enforcement, national security, foreign intelligence, or private purposes)
- whether the target of the surveillance is a U.S. citizen (including a permanent resident), foreign national, or agent of a foreign power
- the form of a communication (e.g., telephone call, electronic mail)
- whether a communication is stored by a third party or is in transit
- whether a communication is transmitted by a wire
- whether the surveillance captures video or sound
- what is being intercepted (e.g., content of a communications or a telecommunications attribute, such as the telephone number dialed)
- what is under surveillance (e.g., a public place, home, workplace, locker room, toilet stall)
- where the surveillance is conducted from (e.g., a public place, a private place, an airplane, a place of employment)
- the extent to which a place under surveillance has been protected from observation
- whether the surveillance is subject to state law or to federal law
- whether the technology used to undertake the surveillance is in general public use.

The history, scope, and shortcomings of the Electronic Communications Privacy Act of 1986[3] (ECPA) are most relevant here. There are three titles to ECPA: the first amends the Wiretap Act; the second contains the Stored Communications Act; and the third addresses pen registers and trap and trace devices. The first two titles are most relevant here.

The Wiretap Act is a criminal statute that seeks (1) to protect the privacy of wire and oral communications, and (2) to set out the circumstances and conditions under which the interception of wire and oral communications may be authorized.[4] In 1986, ECPA amended the existing Wiretap Act to extend to electronic communications protections against unauthorized interceptions that existed previously only for oral and wire communications via common carrier transmissions.

The Stored Communications Act[5] seeks to protect electronic communications and voice mail from unauthorized access by defining unlawful access as a crime. The goal was to protect the confidentiality, integrity, and availability of such communications stored by providers of electronic communication service pending the messages' ultimate delivery to their intended recipients.

---

[2]Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 Hastings Law Journal 805, 820 (2003). See also Gina Marie Stevens & Charles Doyle, *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Surveillance* (2009) (Congressional Research Service), available at http://assets.opencrs.com/rpts/98-326_20091203.pdf; accessed on March 23, 2010.

[3]Public Law 99-508, 100 Stat. 1848 (1986).

[4]18 U.S.C. § 2511.

[5]18 U.S.C. § 2701.

One of the law's exception permits access to electronic communications by service providers, and this provision allows employers who directly provide (as opposed to using a third party service provider) email service to employees the ability to monitor email.[6] That monitoring ability could support the cyberattack prevention activities. Public employers remain subject to Fourth Amendment requirements and may be more limited in their ability to review email.[7] Privacy policies and terms of service established by an ISP could also be relevant to a user's expectation of privacy and could authorize monitoring of email by the ISP.

It is widely recognized today that ECPA's assumptions about technology are outmoded and that the protections that ECPA sought to provide now operate inconsistently because of changes in technology and service offerings.[8] For example, with respect to government surveillance, the law gives greater protection to email in transit than it does to email that has arrived in a user's in-box at a service provider. In addition, under the law, email that is more than 180 days old is more easily accessible to the government than newer email.[9] Because some ISPs now offer massive or unlimited storage for email, the result is a significantly differing degree of legal protection for email depending on factors that many users no longer view as significant. Other questions arise with respect to newer services such as Voice over Internet Protocol. Documents placed on cloud computing sites may also have fewer protections under current law than email because ECPA only covers electronic communications and the transfer of information to a cloud computing provider may not qualify for protection.[10]

The 1976 decision of the Supreme Court in *U.S. v. Miller*[11] illustrates an important aspect of third party storage of information under the Fourth Amendment. The Supreme Court held that the Fourth Amendment does not recognize an expectation of privacy in an individual's financial records held by a bank. Therefore, the Court allowed the government to obtain the records from the bank without providing the individual notice or an opportunity to contest the demand. The conclusion in *Miller* with its broad implication that an individual has no expectation of privacy in any record held by a third party[12] is an ever-increasing concern to civil libertarians and privacy advocates because most records of an individual's existence—and especially an individual's Internet activities—are held by third parties. ECPA partly curbs the effect of *Miller* by establishing rules and procedures that limit the ability of the government to obtain electronic communications.

2. Other Approaches to *Miller*

Shortly after the decision in *Miller*, Congress passed the Right to Financial Privacy Act.[13] The Act established limited statutory privacy protections for bank records that the Supreme Court declined to recognize under the Fourth Amendment. The Act requires the federal government (but not state governments) to notify a bank customer when it uses a subpoena or summons to obtain a record about that customer

[6]Id. at § 2701(c)(1).

[7]See *City of Ontario v. Quon*, 560 U.S. ___ (2010).

[8]The Center for Democracy and Technology (CDT) is leading a broad effort of privacy groups, businesses, and Internet companies to seek amendment and modernization of ECPA. See CDT, *Digital Due Process Coalition (Including Microsoft, Google, and More) Call for Tougher Online Privacy Laws*, http://www.cdt.org/press_hit/digital-due-process-coalition-including-microsoft-google-and-more-call-tougher-online-priv; accessed April 20, 2010.

[9]18 U.S.C. § 2703(a).

[10]*Cloud computing* involves the sharing or storage by users of their own information on remote servers owned or operated by others and accessed through the Internet. The proper characterization for ECPA purposes of cloud documents, which differs greatly in type and terms of service, is far from clear. See Robert Gellman, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing* at 17 (World Privacy Forum, 2009), available at http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf; accessed April 20, 2010.

[11]425 U.S. 435 (1976).

[12]See *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979), ("a person has no legitimate expectation of privacy information he voluntarily turns over to third parties").

[13]12 U.S.C. §§ 3401-3422.

from a bank. The customer then has an opportunity to contest the process in court before the bank hands over the records. The Act's value is questionable since the grounds upon which a customer can challenge the government are limited (must show that the records are not relevant to a legitimate law enforcement investigation), and exceptions to customer notice cover many important agencies and activities.

The federal health privacy rule[14] also contains a provision that requires notice to a patient of a subpoena for the patient's record held by a health care provider or insurer. For patients and for civil litigation, the health privacy rule's provisions are stronger than in the Right to Financial Privacy Act, but the exceptions for law enforcement investigations provide even fewer rights for data subjects than the Right to Financial Privacy Act.[15]

Recent legislation, including updates to the USA PATRIOT Act, Foreign Intelligence Surveillance Act, and ECPA also modify some effects of *Miller* by expanding requirements for judicial involvement in some electronic searches. None of the legislative changes to the *Miller* holding has broad effect with respect to all or most information held by third party record keepers, however.

Because of the tremendous volume and range of personal information held by ISPs and other third party record keepers, privacy advocates want to create a protectable privacy interest that would undermine the broad holding in *Miller*. ECPA provides some protection for electronic communications. However, email only represents a portion of the information now held by third party Internet providers, which include social networks, cloud computing service providers, photograph storage services, financial management websites, and a nearly unlimited number of other services. Indeed, a very large portion of Internet activities create records held by third parties, and the ongoing expansion of cloud computing will shift additional materials from locally owned and controlled computers to third parties. Whether and how Congress (or the courts) revise the principle that there is no privacy interest in records held by third parties will determine both the scope of that privacy interest and the ease with which government investigators can obtain personal and business records held by third parties.

Any expansion of the privacy rights of data subjects with respect to records held by ISPs and other third party record keepers could affect the conduct of cyberattack prevention and investigation activities by creating substantive or procedural barriers to government acquisition of information about Internet activities. These activities may not be affected any more than any other government investigatory activities that center on Internet conduct. It remains to be seen how broadly any future ECPA reforms will affect the basic *Miller* holding that there is no privacy interest in records held by a third party. Any significant change to these privacy protections could produce a major shift in the balance between individual rights and the government's investigatory capabilities. The stakes grow larger as the Internet continues to expand as a central feature of modern life.

At the same time, however, the issue in *Miller* is personal privacy, and not every record created on or off the Internet qualifies as personal information. Government access to non-personal information held by third parties might be unaffected by any change in the privacy interest granted to individuals in third party records. This could include, perhaps, the content of many webpages, commercial transactions, foreign government operations, activities that occur outside the United States and beyond the scope of the Fourth Amendment, and more.

3. Data Retention

In March 2006, the EU enacted a Data Retention Directive calling for the mandatory retention of communications traffic data.[16] A leading argument for the directive is for combating terrorism. The

[14]45 C.F.R. Part 164, issued under the authority of the Health Insurance Portability and Accountability Act (HIPAA). Public Law 104–191, title II, § 264, 110 Stat. 2033 (1996), 42 U.S.C. § 1320d-2 note.

[15]Id. at § 164.512(e) & (i).

[16]Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, 2006 O.J. (L 105) 54, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF; accessed April 20, 2010.

same general argument in support of data retention could be made with respect to cyberattack prevention either because cyberattacks may qualify as terrorism or because data retention would be useful in preventing cyberattacks regardless of motivation. The EU and many of its Member States required data retention to create a new capability in combating criminal and other undesirable activities. The extent to which data retention will work to achieve the stated goals is open to question and beyond the scope of this paper. Nevertheless, data retention is a tool with some potential application to cyberattack prevention.

The EU Data Retention Directive requires Member States to adopt measures to ensure that electronic communications traffic data and location data generated or processed by providers of publicly available electronic communications services be retained for not less than six months and not more than two years from the date of the communication. The Data Retention Directive requires the retention of data necessary:

- to trace and identify the source of a communication
- to trace and identify the destination of a communication
- to identify the date, time and duration of a communication
- to identify the type of communication
- to identify the communication device
- to identify the location of mobile communication equipment.[17]

The retention requirement applies only to data generated or processed as a consequence of a communication or a communication service. It does not apply to the *content* of a telephone call or of electronic mail. The data retained must be made available to competent national authorities in specific cases "for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law."[18] Thus, each Member State can establish its own standards for serious crime as well as its own judicial or other procedures for access.

The data retention directive has been controversial throughout Europe, with Internet activists strongly opposed to its implementation in many EU Member States. Litigation has resulted in some national courts finding laws implementing the directive unconstitutional. The German law suspended by the Federal Constitutional Court in early March 2010.[19] The German Court ordered the deletion of data collected. The decision did not exclude the possibility that a data retention law could pass constitutional muster, but it found that the law's provisions for security of data were inadequate and that the uses of the data were not sufficiently clear. The Romanian Constitutional Court found the Romanian data retention implementation law unconstitutional.[20]

A data retention law has been proposed for the United States, although it has not received much attention from Congress to date.[21] The constitutionality of any data retention proposed will surely be contested on First Amendment and Fourth Amendment grounds. Much will depend on the scope and the details of any enacted law. For example, a data retention requirement for Internet activities could entail the storage of information about electronic mail that could include data about the sender, recipient, header, attachment, content, and more. The retained data could be available to criminal or civil law enforcement, intelligence agencies, or private litigants after a showing of probable cause, reasonable cause, relevance, or another standard. Data subjects could have rights to object before or after retained information is disclosed or could have no rights. The details affect any privacy and civil liberties evalu-

[17]Id at Article 5.

[18]Id. at Article 1.

[19]*German High Court Limits Phone and E-Mail Data Storage*, Spiegel Online International (March 2, 2010), available at http://www.spiegel.de/international/germany/0,1518,681251,00.html; accessed April 20, 2010. The decision itself (in German) is at http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011; accessed April 20, 2010.

[20]*Romanian Constitutional Court: Data Retention Law Unconstitutional*, The Sofia Echo (Oct. 9, 2010), available at http://www.sofiaecho.com/2009/10/09/797385_romanian-constitutional-court-data-retention-law-unconstitutional; accessed April 20, 2010.

[21]See S.436, 111th Congress (2009).

ation, and any discussion of the possibilities would exceed the space available here. However, it seems clear that to the extent that a law requires the preservation of content rather than non-content information, the law will be harder to justify because existing precedents provide greater protections for the content of communications.

However, if a data retention law covers traffic, location, or transaction data only, there are some precedents in U.S. law that allow for government access with fewer or no procedural protections for the privacy of the individuals involved. For example, U.S. law allows for the use of pen registers that record dialed numbers without a search warrant.[22] The Stored Communications Act allows the government to order a provider of wire, electronic communication services, or remote computing services, to preserve records and other evidence in its possession pending the issuance of a court order or other process.[23] The Bank Secrecy Act requires banks to keep records of various transactions, including some cash activities and, effectively, all checks.[24] The Supreme Court upheld the law in 1974 as a valid exercise of federal power under the Commerce Clause.[25]

The distinction that the law makes for Fourth Amendment purposes between content and non-content has increasingly been the subject of litigation under ECPA but litigation remains, in the words of a leading Fourth Amendment scholar, "remarkably sparse."[26] The step-by-step analogies that the courts have used to move legal reasoning from postal mail to telephone calls begin to break down when it comes to Internet activities because the content vs. non-content distinction is much harder to sustain over the wide range of Internet functions that extend far beyond basic communications. For email, the substance of a message may not be limited to the actual content of a message but may be visible in part from the header, subject line, title of attachments, or other elements. In a 2010 decision pertaining to electronic communications (albeit not on the content/non-content issue), the Supreme Court was tentative in offering guidance, observing that "[r]apid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior."[27] How the law develops in this area could make a significant difference to the ability of the government to prevent or investigate cyberattack activities on the Internet. Any expansion in the ability of the government to see content or content-like elements of Internet activities without a showing of probable cause will be strongly contested using Fourth Amendment arguments. However, at the same time, it will be argued that many Internet activities are voluntary, and a user's expectations of privacy in this context are open to debate. Those expectations may be affected by the expansive monitoring of Internet activities for commercial purposes.[28] The routine and largely unrestricted commercial availability of the entrails of a user's Internet activities could undermine arguments that the user had a reasonable expectation of privacy. Thus, privacy legislation affecting Internet monitoring of individuals by commercial entities could also be relevant to the discussion.

First Amendment challenges to data retention requirements can also be anticipated. The right to associate, to speak, and to receive information would all be affected by data retention, with the specific arguments depending on the precise requirements of a data retention regime and on the standards and procedures under which the government could retrieve information from a service provider. Advocates would argue that the First Amendment requires that a retention law be justified under a strict scrutiny

[22] *Smith v. Maryland*, 442 U.S. 735 (1979). 18 U.S.C. §§ 3121-3127.

[23] 18 U.S.C. § 2703(f). The Act is part of the Electronic Communications Privacy Act. An order under this provision is generally called *data preservation*. Data retention generally means a blanket requirement for the maintenance of some information on all communications.

[24] 31 C.F.R. § 103.34(b)(10).

[25] *California Bankers Association v. Schultz*, 416 U.S. 21 (1974)

[26] Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 Stanford Law Review (forthcoming 2010), available at http://ssrn.com/abstract=1348322; accessed July 1, 2010.

[27] *Ontario v. Quon*, 560 U. S. __ (2010) (slip op. at 11).

[28] For more on the current controversy over behavioral targeting of Internet users for advertising and other purposes, see, e.g., Federal Trade Commission, *Staff Report: Self-Regulatory Principles for Online Behavioral Advertising: Tracking, Targeting, and Technology* (Feb. 2009), available at http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf; accessed April 20, 2010.

standard—the most stringent standard of judicial review that requires that a law address a compelling governmental interest, that a law be narrowly tailored to achieve that interest, and that a law be the least restrictive means for achieving its objective.

In some contexts, however, data retention may be largely unremarkable. Routine business activities, whether online or offline, create records that must be retained for tax, credit, or many other purposes. In private networks, all activities may be monitored and recorded by the network operator, who may be a service provider, employer, or other person acting with or without notice to or the consent of the individual. Backup systems retain copies of an entire network at regular intervals. Broad rights to use, maintain, and disclose an individual's information can be reserved by a service provider through routine privacy policy or terms of service that its clients "consent" to by using the service. A recent report on cloud computing and privacy observed that a cloud provider may acquire rights over materials placed in the cloud "including the right to copy, use, change, publish, display, distribute, and share with affiliates or with the world the user's information."[29] These rights may exceed anything that laws mandating data retention require.

4. Terrorism and Cybersecurity

Congress enacted the USA PATRIOT Act less than two months after the events of September 11, 2001.[30] The Act is long and complex, and Congress amended it on several occasions, and more amendments are under consideration. Challenges to the Act have resulted in courts finding parts of the law unconstitutional. The details of the Act and subsequent litigation are too complex for this space. Generally, the Act expanded the ability of federal agencies to prevent and prosecute terrorism, with one title of the Act setting out enhanced surveillance procedures. For example, provisions make it easier for law enforcement agencies to search telephone and electronic communications and other records.

The Act also amended laws that make terrorism a crime. The basic definition of terrorism in the criminal code provides that terrorism must

> (A) Involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State;
> (B) appear to be intended—
> (i) to intimidate or coerce a civilian population;
> (ii) to influence the policy of a government by intimidation or coercion; or
> (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping.[31]

Whether cyberattacks would fall within the definition of *terrorism* is not immediately clear, but it seems a possibility, perhaps depending on the motivation of the attacker. The analysis might well depend on the facts of any given case. The USA PATRIOT Act added the Computer Fraud and Abuse Act[32] to the predicate offense list for wiretapping so at least some of the powers of the Act would be available for cyberattack prevention or investigation.[33] Other authorities provided in the Act may also be available today for some cyberattack prevention activities.

[29]Robert Gellman, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing* at 17 (World Privacy Forum, 2009), available at http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf; accessed April 20, 2010.

[30]Public Law No. 107-56, 115 Stat. 272 (2001). The Act's full name is *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*.

[31]18 U.S.C. § 2331. There is a separate definition for *international terrorism* and for *domestic terrorism*. Both use a similar definition, with the location of the activity being the difference. The part quoted here represents the core of the two definitions.

[32]18 U.S.C. § 1030.

[33]18 U.S.C. § 2516(1)(c).

A broader question is whether Congress or the public would consider cyberattack prevention to be of equal importance to terrorism prevention to justify the granting or use of powers equivalent to those under the USA PATRIOT Act. The Act has remained highly controversial and the subject of continuing congressional actions. Any expansion of the Act or enactment of a similar law for cyberattack prevention would raise the same legal, constitutional, and political controversies that have dogged the Act from its inception.

5. The Fourth Amendment and Special Needs Cases

Ordinarily, the Fourth Amendment requirement that searches and seizures be reasonable means that there must be individualized suspicion of wrongdoing. In some circumstances, the usual rule does not apply. Whether the prevention of cyberattacks could justify an exemption from strict application of the Fourth Amendment is an open question.

In the so-called *special needs* cases, the courts have upheld suspicionless searches in some circumstances. For example, the Supreme Court allowed random drug testing of student athletes; drug tests for some Customs Service employees; and drug and alcohol tests for railway employees involved in train accidents. Searches were allowed for certain administrative purposes without particularized suspicion of misconduct, provided that the searches are appropriately limited. The Supreme Court also upheld brief, suspicionless seizures of motorists at a fixed Border Patrol checkpoint designed to intercept illegal aliens and at a sobriety checkpoint aimed at removing drunk drivers from the road.[34]

Because of the international scope of cyberattacks, any inquiry must consider other law that establishes diminished Fourth Amendment protections in international matters. The Foreign Intelligence Surveillance Act establishes lower standards for conducting surveillance in cases involving agents of a foreign power or a foreign terrorist group. The details of FISA, its amendments, litigation, and history are far beyond the scope of this paper. However, even the diminished FISA standards have been held to give way to the lower standards recognized in special needs cases. Thus, the United States Foreign Intelligence Surveillance Court of Review held in 2008 that a foreign intelligence exception to the Fourth Amendment's warrant requirement exists when surveillance seeks foreign intelligence for national security purposes and is directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States.[35]

Whether prevention of cyberattacks could qualify as a special needs case is unknown. Any expansion of special needs would be controversial, and a special needs case involving domestic cybersecurity matters would be especially controversial.

III. ISSUES RELATING TO SPEECH AND ASSOCIATION

The Internet raises a host of First Amendment speech and association issues, some of which are relevant to activities seeking to prevent cyberattacks. This is an area where it is especially difficult to be comprehensive and to disentangle issues.

Two preliminary observations are offered. First, the First Amendment does not protect against actions taken by private entities, although there can be some overlap between the public and private spheres at times. The First Amendment is a protection against abridgment of speech by government, state or federal. Second, it has been famously said that on the global Internet, the First Amendment is a local ordinance. To the extent that cyberattack protections involve other nations, First Amendment protections may not be available with respect to Internet activity that originates in or passes through those other nations.

[34] *City of Indianapolis v. Edmond*, 531 U.S. 32 (2000). However, the Court refused to allow a general interest in crime control to provide a justification for suspicionless stops. Id.

[35] *In Re Directives Pursuant to Sec. 105B*, 551 F. 3d 1004 (FISA Ct. Rev., 2008).

1. Internet as a Human Right

The Internet has rapidly become a vibrant public forum for speech of all types, including news, political discussions, government communications, commercial speech, and everything else. In some countries, access to the Internet is a fundamental right of its citizens.[36] In Finland, broadband access is a legal right.[37] However, rhetoric about the fundamental importance of the Internet does little to advance the present discussion of preventing cyberattacks. Whatever right may exist is not an unlimited right.

A new law in France illustrates the point. As originally enacted, the law would have allowed a government agency to suspend an individual's user account. The French constitutional court found that the law violated constitutional free speech protections. After an amendment that required a judge to make the decision to suspend, the court allowed the law to stand.[38] During the controversy over the French law, the European Parliament voted to make it illegal for any EU country to sever Internet service unless a court finds a citizen guilty.[39]

Whatever the scope of an individual's right to use the Internet may be, the view in Europe seems to be that the right may be restricted through actions that are not disproportionate and that involve a decision by an independent and impartial judge. The right to use the Internet is, in essence, the right to due process of law before the ability to exercise the right to use the Internet is removed or restricted. The same principles may apply when the reasons for seeking termination of Internet access relate to cyberattack prevention. It may be possible to argue in some cases that immediate threats to critical infrastructure would justify a different or lesser set of due process procedures prior to termination of Internet access rights.[40] Regardless, any rules or procedures with the potential to deny an individual access to the Internet will be controversial and the subject of considerable scrutiny on constitutional or legal grounds.

2. Anonymity

Anonymity on the Internet is a feature prized by many Internet users, often for different reasons. Many Internet activities can be conducted with a significant degree of anonymity using onion routers,[41] free email accounts that do not require any form of identification, public kiosks, blogs that do not ask posters to register, and in other ways. Whistleblowers, political activists, dissidents, and ordinary users value anonymity. The extent to which Internet activities are truly anonymous is uncertain. Even a user who takes concerted action to protect identity may not succeed all the time, especially against a person or government determined to uncover that identity.

Discussing the right to anonymity online is difficult for several reasons. First, the scope of a First Amendment right to anonymity is not clear, and tracking down the borders of anonymity leads far afield from the Internet without necessarily providing clarity. Second, there are many different objectives that a right to (or interest in) online anonymity may satisfy in whole or in part. For example, victims of

[36]Colin Woodward, *Estonia, Where Being Wired Is a Human Right*, Christian Science Monitor (July 1, 2003), available at http://www.csmonitor.com/2003/0701/p07s01-woeu.html. A 2010 poll taken in 26 countries found that almost 79% of those questioned said they either strongly agreed or somewhat agreed with the description of the Internet as a fundamental right. *Internet Access Is a Fundamental Right*, BBC News (March 8, 2010), available at http://news.bbc.co.uk/2/hi/technology/8548190.stm.

[37]Saeed Ahmed, *Fast Internet Access Becomes a Legal Right in Finland*, CNN.com (2009), available at http://www.cnn.com/2009/TECH/10/15/finland.internet.rights/index.html.

[38]Eric Pfanner, France Approves Wide Crackdown on Net Piracy (Oct. 23, 2009), New York Times, available at http://www.nytimes.com/2009/10/23/technology/23net.html.

[39]Kevin J. O'Brien, *French Anti-Piracy Proposal Undermines E.U. Telecommunications Overhaul*, New York Times, (May 7, 2009), available at http://www.nytimes.com/2009/05/07/technology/07iht-telecoms.html.

[40]The discussion below regarding the administrative license suspension for driver's licenses may suggest a precedent.

[41]With onion routing, messages are repeatedly encrypted and sent sequentially through different nodes. Each node removes a layer of encryption to find instructions for sending the message to the next node. Intermediary nodes do not know the origin, destination, or contents of the message.

domestic violence have some unique interests that are not relevant here. Third, it is hard to cover every possible cybersecurity activity that might affect an anonymity interest.

In cases involving political speech, the Supreme Court has consistently overturned laws that prohibited the distribution of anonymous handbills and similar laws that prevented anonymous political speech. Political speech is the most highly favored speech under the First Amendment. However, as one scholar described cases in this area, "the Court failed to embrace the notion of a free-standing right to anonymity and instead employed what would become a characteristic (and maddening) level of ambiguity."[42]

In other areas, a right to anonymity is not clearly established. In 2004, the Supreme Court upheld the conviction of an individual who refused to identify himself to a police officer during an investigative stop involving a reported assault. A state statute required a person detained by an officer under suspicious circumstances to identify himself.[43] The case raised Fourth and Fifth Amendment issues, but it was also seen as raising broader questions about the right to remain anonymous. The case's relevance to cyberspace is limited, but it illustrates that the Court does not universally favor anonymity.

The right to anonymity on the Internet has also been raised in a series of cases that balance the right to speak anonymously against the right of those who claim injury from anonymous defamatory speech. The law here is under development in many different courts and, not surprisingly, with the adoption of different approaches. Courts tend to require a plaintiff to show that a suit is viable before ordering disclosure of the speaker's identity. According to one scholar, the standard that appears to be becoming dominant requires a showing of evidence sufficient to establish a prima facie case of defamation coupled with a balancing of the right to speak anonymously and the right to pursue a libel claim.[44]

Anonymity concerns are likely to be raised by whistleblowers, i.e., individuals who raise concerns about wrongdoing occurring in an organization. Scattered federal and state laws provide some protections for whistleblowers, and the whistleblower community continues to press for stronger protections. Anonymity can be a method for whistleblowers to raise issues while avoiding the consequences of identification. To the extent that activities take place on a private network that does not support anonymity, the availability of the Internet as an alternative way to communicate about possible wrongdoing lessens concerns about the closed nature of a particular network and the lack of any anonymous methods of communications.

Political and other dissidents may also rely on anonymity to protect their identities when complaining about government or other activities. Anonymity can also assist activists who seek to find and communicate with others who hold similar views and to organize their efforts. Anonymity can also allow those with minority views, with unpopular views, or with other needs or fears to speak and organize. Here too, restrictions on a closed network may be of lesser concern if, at the same time, the Internet otherwise allows anonymity for communications and activities. However, if protections against cyberattacks undermine or interfere with the ability to use the Internet anonymously, those protections will be significantly more controversial politically and legally. It does not seem possible in the abstract to draw a line where the federal government can lawfully prevent or punish anonymous speech, although it has broader powers with respect to a network that it operates.

3. Restraining Publication of Security Information

One method that may be relevant to preventing cyberattacks is to limit or prevent the publication of information about vulnerabilities of computer systems, whether the information is held by govern-

[42]Jonathan Turley, *Registering Publius: The Supreme Court and the Right to Anonymity*, Cato Supreme Court Review (2001-02), available at http://www.cato.org/pubs/scr/2002/turley.pdf; accessed April 20, 2010.

[43]*Hiibel v. Sixth Judicial District Court of Nevada*, 542 U.S. 177 (2004).

[44]Lyrissa Barnett Lidsky, *Anonymity in Cyberspace: What Can We Learn from John Doe?*, 50 Boston College Law Review 1373, 1378 (2009).

ment or private actors.[45] Restrictions on the availability of information about security vulnerabilities raise First Amendment issues. The practical difficulties of restricting speech on the Internet are real but not necessarily material to the legal or constitutional issues.

Source Code

It is not entirely settled that the publication of source code constitutes speech protected under the First Amendment. In a leading case that arose in the context of export regulations, the Ninth Circuit concluded in the context of that case that encryption software qualified for First Amendment protections.[46] An alternate view expressed in the dissent is that source code is a method of controlling computers and is more function than speech.[47] The case has a complex history and does not offer a broad holding. The proper characterization of source code for First Amendment purposes has many different perspectives.

Copyright

The anti-circumvention provisions of the Digital Millennium Copyright Act[48] (DMCA) principally sought to stop copyright infringers from defeating anti-piracy protections in copyrighted works. The DMCA bans both acts of circumvention and the distribution of tools and technologies used for circumvention. The law exempts some activities, including security testing and encryption research. The DMCA has been used in a variety of ways to stop publication of information about security vulnerabilities, remove content from the Internet, affect research activities, and in other ways.[49] Opponents of the law contend that many of these uses chill free speech activities. The DMCA has some relevance to private sector attempts to prevent cyberattacks, but federal government information is not subject to copyright so the DMCA may not be relevant.[50]

Contractual Methods

Tools, techniques, and policies allow for government controls over publication of some information by some individuals. Contracts that require government employees not to publish any information without pre-publication review by the government offer one approach. In the leading case, the Supreme Court upheld a contract signed by an employee of the Central Intelligence Agency that imposed the restriction as a condition for access to classified information.[51]

Classification

The classification and control of federal government information in the interest of national defense or foreign policy (security classification) is another possible approach to cyberattack prevention. Classification protects security information controlled by the federal government, makes its use and disclo-

[45]See 6 U.S.C. § 133 (establishing restrictions on the use and disclosure of information regarding the security of critical infrastructure voluntarily submitted to a Federal agency).

[46]*Bernstein v. U.S. Dept. of Justice*, 176 F.3d 1132 (9th Cir. 1999), *withdrawn*, 192 F.3d 1308 (9th Cir. 1999).

[47]176 F.3d at 1147.

[48]17 U.S.C. § 1201.

[49]See generally, Electronic Frontier Foundation, *Unintended Consequences: Twelve Years under the DMCA*, available at https://www.eff.org/wp/unintended-consequences-under-dmca; accessed April 20, 2010.

[50]17 U.S.C. § 105.

[51]*Snepp v. United States*, 444 U.S. 507 (1980).

sure subject to controls, and subjects its publication to sanction.[52] To the extent that private parties not working for the government hold the information, classifying the information may be difficult as well as expensive.

Even information in private hands is arguably subject to classification. The Atomic Energy Act provides that data about the design and manufacture of atomic weapons is *restricted data* that is *born classified* regardless of who created the information.[53] Doubts about the constitutionality of this provision persist.[54] Enforcement of a *born classified* policy in the current international Internet environment seems challenging at best and impossible at worst.

Generally, however, restricting access to or publication of information in the possession or control of the government is different from restricting information in private hands. When restrictions on information become censorship is a matter of judgment. Some countries expressly restrict the ability of citizens to access websites or to find material they want through search engines.[55] The United States has on several occasions enacted legislation to restrict access by minors to obscene material or harmful material,[56] but the Supreme Court overturned the laws on First Amendment grounds.[57] Whether a law restricting publication of or access to cybersecurity information would be constitutional is unclear, but much could depend on the justification, structure, and application. The Supreme Court upheld the Children's Internet Protection Act,[58] a law that tied certain federal financial assistance to a library to a policy of Internet safety for minors that includes the operation of filtering technology to protect against access to material that is obscene, child pornography, or harmful to minors.[59] There is no specific precedent upholding statutory limitations on publication of cybersecurity information on the same basis as Atomic Energy restricted data or in a manner analogous to allowable controls on obscenity.

Prior Restraint

Prior restraint (government banning expression of ideas prior to publication) is another possible tool that could be used to protect cybersecurity information. However, prior restraint of publication is not favored, and the Supreme Court has stated on several occasions that, "[a]ny system of prior restraints of expression comes to this Court bearing a heavy presumption against its constitutional validity."[60] Whether or when computer security or national security interests could justify a prior restraint is uncertain. Practical considerations suggest that any restraint on publication could be difficult to maintain.

4. Domain Name System

The WHOIS database is an integral part of the registration system for Internet domain names. The database records and identifies the registrant or assignee of Internet resources, such as a web site domain name or an Internet Protocol address. The database includes information on a registrant, including name,

[52]Information that is properly classified is exempt from mandatory disclosure under the Freedom of Information Act (FOIA), 5 U.S.C. §552(b)(1). The ability of the government to withhold cybersecurity information from public requesters appears to be broad even if the information is not subject to classification. Nothing prevents the government from enacting additional exemptions to the FOIA. See 5 U.S.C. § 552(b)(3).

[53]42 U.S.C. §§ 2014(y), 2162(a).

[54]An important case is *U.S. v. The Progressive*, 467 F. Supp. 990 (W.D. Wis. 1979), appeal dismissed, 610 F. 2d. 819 (7th Cir. 1979).

[55]See, e.g., Andrew Jacobs, *Follow the Law, China Tells Internet Companies*, New York Times, Jan. 14, 2010, available at http://www.nytimes.com/2010/01/15/world/asia/15beijing.html, accessed August 30, 2010.

[56]See Communications Decency Act of 1996, 47 U.S.C. § 223(a) and (d); Child Online Protection Act, 47 U.S.C. § 231.

[57]*Reno v. ACLU*, 521 U.S. 844 (1997); *Ashcroft v. ACLU*, 535 U.S. 564 (2002), aff'd on remand, 322 F.3d 240 (3d Cir. 2003), aff'd and remanded, 542 U.S. 656 (2004), judgment entered by *ACLU v. Gonzales*, 478 F.Supp.2d 775 (E.D. Pa. 2007), aff'd sub nom. *ACLU v. Mukasey*, 534 F.3d 181 (3rd Cir. 2008), cert. denied, __ U.S. __, 129 S. Ct. 1032 (2009).

[58]20 U.S.C. §§9134(f)(1)(A)(i) and (B)(i); 47 U. S. C. §§254(h)(6)(B)(i) and (C)(i).

[59]*U.S. v. American Library Association*, 539 U.S. 194 (2003).

[60]See, e.g., the Pentagon Papers case, *New York Times v. United States*, 403 U.S. 713 (1971) (per curium).

address, telephone number, and email address. The information in the WHOIS database is often public and available to any inquirer. However, domain name registrars offer to list themselves as the owner of a domain name to shield information about the real owner (i.e., proxy registrations).

A government move to prevent proxy registrations—or to require additional disclosures—in the interest of cyberattack prevention would generate First Amendment and privacy concerns. Registrants who want anonymity to avoid identification and possible harassment and registrants who merely want to shield their personal information from marketers and other secondary users of their information would object. The conflicts over the privacy of the WHOIS database have raged for some time, involve privacy laws in other countries, and will require international coordination. It is impossible to predict how the conflicts might be resolved.

Government actions seeking to cancel domain names issued to those believed to be engaged in activities that threaten cybersecurity would raise due process issues similar to the taking of any other private property by the government. However, because depriving someone of a domain name affects the ability to communicate, First Amendment arguments would likely accompany the due process issues as major points of contention. Cutting off or limiting the ability of a speaker to use the Internet or other recent means of communication will be viewed by many as a direct prohibition on speech and, especially, on political speech. Further, because domain name registration is an international activity, federal efforts could be ineffective or could have to consider international standards.

5. Beyond the First Amendment

The First Amendment does not protect some types of speech, including defamation, incitement, obscenity, and pornography produced with real children.[61] Congress has enacted laws prohibiting child pornography.[62] ISPs are required to report evidence of child pornography offenses.[63] Some state laws require computer technicians to report to police child pornography found while working on computers.[64]

Could similar laws or principles establish limits on or mandate monitoring or reporting of cybersecurity communications, information, or activities? It is possible to characterize those who undermine security protections for computers and computer networks as threatening, among other things, the exercise of free speech rights guaranteed by the First Amendment. Arguably, a case could be made that reducing or eliminating First Amendment protections for speech or actions that present cybersecurity threats actually protect the First Amendment rights of others. Framed this way, the issue might call for a balancing of interests rather than a one-sided evaluation of the rights of a speaker versus the powers of the government. The use of First Amendment values to defend some restrictions on speech is an interesting prospect.[65]

Closely related issues involving tradeoffs between speech and privacy have been a topic of debate in the context of deep packet inspection (DPI). Internet messages are broken into units called packets that are composed of header information (analogous to an envelope) and a data field (analogous to content). Packets move from place to place using the header information alone. DPI involves the opening and

[61] *Ashcroft v. Free Speech Coalition*, 535 U.S. 234, 245-6 (2002). See generally Henry Cohen, *Freedom of Speech and Press: Exceptions to the First Amendment* (2009) (Congressional Research Service), http://www.fas.org/sgp/crs/misc/95-815.pdf; accessed April 14, 2010.

[62] See, e.g., Protection of Children From Sexual Predators Act of 1998, Public Law 105-314, 112 Stat. 2974 (1998).

[63] 18 U.S.C. § 2258A. There is an exception allowing this type of disclosure in the Electronic Communications Privacy Act, 18 U.S.C. § 2702(b).

[64] See National Conference of State Legislatures, *Child Pornography Reporting Requirements (ISPs and IT Workers)*, http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/ChildPornographyReportingRequirementsISPsand/tabid/13460/Default.aspx; accessed March 29, 2010.

[65] Robert Morris's 1988 release of the so-called Internet worm that had the effect of denying service on infected computers resulted in his conviction for violation of the federal Computer Fraud and Abuse Act. The conviction shows that some computer actions are subject to criminal sanction. The line between speech, which is harder to sanction, and non-speech, which may be easier to sanction, is complex.

reading the content of a Web browsing session, email, instant message, or whatever other data the packet contains. ISPs, who assemble packets for users, can and do use DPI to identify network threats including spam, viruses and other malware, and denial-of-service attacks. These actions may well increase cyber-attack protections. DPI could be used to search for personal information, child pornography, copyright infringement, or almost anything else. DPI can also be used to set priorities for Internet activities, an issue in Net Neutrality debates.

The basic idea of using DPI to screen Internet activities for unwanted activities is not simple. Fears about the use of DPI include threats to privacy through the collection or use of more personal information for commercial or other uses;[66] filtering standards that will monitor or block non-objectionable activities or speech; increased government surveillance; interference with Net Neutrality; and other problems. Commercial use of DPI for marketing purposes has given rise to litigation.[67]

Whether government-mandated DPI program for cybersecurity purposes would pass constitutional muster would depend, in significant part, on the factual predicate for the requirement and on the level of scrutiny required by the courts. The availability and effectiveness of other tools and techniques to accomplish the same purpose would also be relevant in any ruling. The specific focus of DPI, whether for malware, spam, copyright infringement, or other purposes, would also make a difference. The waters here are largely uncharted.

Private ISPs already engage in filtering of email for spam and malware. This often happens with some degree of consent from users, although it is unclear whether consumers grant consent knowingly. In general, it is much debated today whether consent is a reasonable way of engaging consumers for privacy and other purposes. Privacy advocates and others express doubts about the value and viability of the notice-and-consent regime used for privacy and other purposes on the Internet today.[68]

IV. ISSUES RELATING TO INFORMATION PRIVACY

The general approach of the United States to the protection of information privacy is often called *sectoral*. Privacy laws often pass in response to specific incidents, and the laws often respond narrowly to the facts, industries, or institutions identified in those incidents. The result is a disparate set of laws that address the collection, maintenance, use, and disclosure of personally identifiable information often in incomplete or inconsistent ways. No privacy statute applies to many types of records and record keepers. In contrast, Europe, Canada, and much of the rest of the developed world operates under omnibus laws that establish uniform, high-level rules for most record keepers. Other nations often expressly base their privacy laws on Fair Information Practices (FIPs), a set of principles for information privacy.[69] U.S. laws often reflect elements of FIPs, and some laws address most or all of the principles to some extent.

The first law anywhere to meet FIPs standards was the Privacy Act of 1974.[70] The Privacy Act of 1974 is a federal statute that applies to records about individuals maintained by federal agencies and

[66]"DPI poses unique risks to individual privacy." Statement of Leslie Harris, President and Chief Executive Officer Center for Democracy & Technology, Before the House Committee on Energy and Commerce, Subcommittee on Communications, Technology and the Internet, The Privacy Implications of Deep Packet Inspection at 8 (April 23, 2009), http://www.cdt.org/privacy/20090423_dpi_testimony.pdf; accessed March 29, 2010.

[67]See Jacqui Cheng, *NebuAd, ISPs sued over DPI snooping, ad-targeting program*, ars technica, Nov. 11, 2009, http://arstechnica.com/tech-policy/news/2008/11/nebuad-isps-sued-over-dpi-snooping-ad-targeting-program.ars, accessed August 30, 2010. The lawsuit alleges, among other things, that DPI violates ECPA.

[68]See, e.g., Introductory Remarks, Federal Trade Commission Chairman Jon Leibowitz, FTC Privacy Roundtable (Dec. 7, 2009), http://www.ftc.gov/speeches/leibowitz/091207privacyremarks.pdf; accessed March 29, 2010.

[69]A classic statement of FIPs much more likely to be cited than the original is from the Organisation for Economic Cooperation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, http://www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html, accessed March 26, 2010. For a short history of FIPs and some of the many variations of FIPs, see Robert Gellman, *Fair Information Practices: A Basic History*, http://bobgellman.com/rg-docs/rg-FIPshistory.pdf; accessed March 26, 2010.

[70]5 U.S.C. § 552a.

by contractors that maintain systems of records on behalf of agencies. Congress took the substance of the Act largely from the recommendations of the 1972 Department of Health, Education & Welfare Advisory Committee that originally developed and proposed FIPs.[71] In establishing a privacy office at the Department of Homeland Security in 2003, the Congress assigned the office responsibility for "assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974."[72] This was the first direct U.S. statutory mention of FIPs. DHS now has its own version of FIPs, which it calls Fair Information Practice Principles.[73]

Because the Privacy Act of 1974 applies to federal agencies, it is the privacy law of greatest relevance here and is described here in modest detail. Other privacy laws applicable to the private sector or to state governments are less likely to be important in the context of cyberattack prevention, although there could be circumstances in which other laws could affect access to records needed for investigatory purposes.

1. Privacy Act of 1974

The Privacy Act of 1974 does not apply to all personal information in the possession of federal agencies. It mostly applies to personal information maintained in a *system of records*.[74] This is a group of records from which information is actually retrieved by name, social security number, or other personal identifier. The retrieval standard is a *factual* one. While much personal information in agency hands is covered, some is not because the information is not actually retrieved by personal identifier. This "loophole" exists because of the need to attach many of the Act's requirements to an identified record-keeping structure.[75] It is one of the elements of the Act that has grown outdated with the power of modern computers to readily search and retrieve disorganized information. An agency can collect and use large quantities of personal information, but the Privacy Act is not triggered if the information is not retrieved by individual identifier.[76] Activities designated as *data mining*[77] do not have any separate requirements or distinct status under the Act. The Act generally applies to data mining if personal information in records maintained in a system of records is retrieved by individual identifier and does not apply otherwise.

Despite the evolution of record keeping from paper to mainframe computers to personal computers to databases to networks and to cyberspace since passage of the Act, the basic structure of the Act remains unchanged. Further, the explosion of private sector record keeping and the commercial availability of those private sector records allow federal agencies to examine and use more personal information on a systematic basis without maintaining system of records. Privately maintained records do not become subject to the Privacy Act merely because the federal government uses them. The record keeper

[71]Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers and the Rights of Citizens* (1972), http://aspe.os.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm; accessed March 26, 2010.

[72]6 U.S.C. §142. See also 50 U.S.C. § 403-3d(b)(5) (establishing a Civil Liberties Protection Officer within the Office of the Director of National Intelligence).

[73]http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf; accessed March 26, 2010.

[74]5 U.S.C. § 552a(a)(5). The Act's protections cover citizens and resident aliens. Id. at § 552a(a)(2) (definition of *individual*). Foreigners are not protected by the Act. Data protection laws in other countries usually cover all individuals regardless of citizenship or residency status. This limitation of the Privacy Act of 1974 has been a point of contention in disputes with the EU over the processing of travel and other information.

[75]Some provisions of the Privacy Act of 1974 have been interpreted as applying generally to agencies maintaining systems of records rather than only to information in systems of records. See Department of Justice, *Overview of the Privacy Act of 1974* (2010) at Definitions, E. Systems of Records, 3. Other Aspects, http://www.justice.gov/opcl/1974definitions.htm#aspects; accessed March 26, 2010.

[76]Whether IP addresses or even email addresses constitute personal information under the Act is not resolved. Many agencies have not established systems of records covering email activities.

[77]For a definition of *data mining*, see the Federal Agency Data Mining Reporting Act of 2007, 42 U.S.C. 2000ee-3.

must maintain the records under a contract with a federal agency, by or on behalf of the agency, and to accomplish an agency function.[78] These limitations often allow an agency to avoid the Act by using private sector records that serve additional purposes other than the agency's purpose. This limitation is a widely recognized shortcoming of the Act.

For example, if an agency reviews a credit report maintained by a credit bureau, the relevance of the Privacy Act of 1974 to the agency's review is limited because of the absence of a system of records. The situation would be different if the agency retrieved the credit report and stored it in a system of records. However, a federal agency's mere use of an Internet search engine or review of a social networking page does not by itself appear to trigger the Act. If ISPs were required by law to retain data about their customers' Internet activities, the records stored by the ISPs would not be covered by the Privacy Act of 1974 because of the absence of a contract with a federal agency, among other reasons. Federal agencies might be able to retrieve those records from ISPs without triggering the Act unless and until the records were made part of a system of records.

The Act's requirements can be generally described using FIPs principles:

- *Openness.* Each agency must publish in the Federal Register a description of personal data record-keeping policies, practices, and systems.[79] No systems or agencies are exempt from the publication requirement.
- *Individual participation.* Each agency must allow an individual to see and have a copy of records about himself or herself. An individual also has the right to seek amendment of any information that is not accurate, timely, relevant, or complete.[80]
- *Data quality.* Each agency must make reasonable efforts to maintain relevant and necessary records that are accurate, relevant, timely, and complete when disclosed to anyone other than another agency.[81] Agencies are prohibited from maintaining information about how individuals exercise rights guaranteed by the First Amendment to the U.S. Constitution unless expressly authorized by statute or unless within the scope of an authorized law enforcement activity.[82] Notably, this First Amendment provision applies to agency records even if not maintained in a system of records.[83]
- *Use limitation.* The Act establishes general rules governing the use and disclosure of personal information.[84] The broad policy that the Act attempts to implement is that information collected for one purpose may not be used for another purpose without notice to or the consent of the subject of the record. However, this policy has so many exceptions, some the result of later enacted laws, that the relevance of the general principle is questionable. The standard for uses within an agency is *need for the record in the performance of duties*,[85] although it is not clear that agencies apply this standard with much rigor.
- *Purpose specification.* The Act grants all agencies authority to make some basic disclosures.[86] However, most disclosures rely on the authority of a *routine use*.[87] Agencies have considerable discretion in defining *routine use* disclosures through a regulatory-like process. When a program changes or a subsequent law directs agencies to use records for a new purpose, the agency defines a new *routine use*

[78] 5 U.S.C. § 552a(m).
[79] Id. at § 552a(e)(4).
[80] Id. at § 552a(d).
[81] Id. at §§ 552a(e)(1), (e)(5).
[82] Id. at § 552a(e)(7).
[83] *Albright v. United States*, 631 F.2d 915 (D.C. Cir. 1980).
[84] 5 U.S.C. § 552a(b).
[85] Id. at § 552a(b)(1).
[86] Id. at § 552a(b)(4) to (b)(12).
[87] Id. at § 552(a)(7), (b)(3).

authorizing a new disclosure. For example, the President's Identity Theft Task Force[88] recommended that all agencies adopt a routine use for all systems of records to allow disclosures to address identity theft problems arising from security breaches. The effectiveness of the routine use provision as a protection against expansive uses of personal information has been questioned for years.

If the Congress or the President established deterrence of cyberattacks as a purpose of the federal government, then agency sharing of personal information would be allowable under the Act pursuant to a routine use.[89] Conceivably, if the charge were broad enough and the identity theft example were used as a model, every system of records in the federal government could include a routine use allowing disclosures for deterrence of cyberattacks. Some in the privacy community would object to the breadth and scope of such an approach, but the Privacy Act may be loose enough to allow it. As a practical matter, however, it seems highly unlikely that all agency systems of records would have information relevant to that purpose.

- *Security.* Agencies must maintain information with appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of the information and to protect against anticipated threats or hazards.[90] The security requirements are general and have been effectively superseded by later, more specific legislation.[91]
- *Collection limitation.* Agencies are required to maintain only information that is relevant and necessary to accomplish an allowable purpose.[92] In addition, agencies are supposed to collect information directly from the data subject *to the extent practicable* if the information may result in an adverse determination.[93]
- *Enforcement.* The Act includes legal remedies that permit an individual to seek enforcement of rights. Civil lawsuits provide the basic enforcement mechanism.[94] In addition, the government may seek relatively minor criminal penalties for Federal employees who fail to comply with the Act's provisions.[95] The Office of Management and Budget has a limited oversight role.[96]

All federal agencies must comply with the Privacy Act of 1974, including law enforcement and national security agencies. The Act does not completely exempt any activity or any agency from the Act. However, the Act includes two different categories of exemption that allow some agencies and some activities to avoid compliance with some provisions of the law. An agency invokes an exemption for a specific system of records through a formal rulemaking process.[97] The exemption becomes part of the agency's Privacy Act of 1974 rules and of the exempted system of records published notice.

[88]The Task Force issued a strategic plan in April 2007, http://www.idtheft.gov/reports/StrategicPlan.pdf; accessed March 23, 2010, and a follow-up report in September 2008. http://www.idtheft.gov/reports/IDTReport2008.pdf; accessed March 23, 2010.

[89]See, for example, the information sharing provisions of the Intelligence Reform and Terrorism Prevention Act of 2004, 6 U.S.C. § 485, which direct the establishment of an information sharing environment for terrorism information. The Act also calls for attention to the protection of privacy and civil liberties in the information sharing environment but includes no specifics. From a Privacy Act perspective, this statute would likely authorize agencies operating relevant systems of records to adopt routine uses allowing broad sharing of personal information with appropriate federal agencies for the purposes stated in the Act. Given the statutory direction, the Privacy Act's barriers to information sharing are essentially procedural.

[90]5 U.S.C. § 552a(e)(10).

[91]See Fair Information Principles and Federal Information Security Management Act (FISMA), 44 U.S.C. § 3541 et seq.

[92]5 U.S.C. § 552a(e)(1).

[93]Id. at § 552a(e)(2).

[94]Id. at § 552a(g).

[95]Id. at § 552a(i). Other criminal penalties under other laws may also be used to punish actions that violate the Privacy Act of 1974.

[96]Id. at § 552a(v).

[97]Id. at § 552a(j), (k).

The Act's *general exemptions* are available for (1) all records of the Central Intelligence Agency and (2) records maintained by an agency or component that performs as its principal function any activity pertaining to the enforcement of criminal laws.[98] The general exemptions allow an agency or component to not comply with many provisions of the Act for an exempt system of records. The net effect of the exemptions is to remove many of the protections that the law provides, but a core of privacy provisions remain.

The Act also provides for *specific exemptions* that are narrower than the general exemptions. Systems specifically exempt can be exempted only from access requirements, obligations to limit records to those relevant and necessary, and several other minor provisions. The specific exemptions are available for record systems that contain seven categories of records, of which only three are potentially relevant to cybersecurity. One exemption is for a system of records that has information classified for national defense or foreign policy reasons.[99] Another is for investigatory material compiled for law enforcement purposes (other than material subject to the general criminal law enforcement purposes).[100] This exemption covers civil as well as some criminal law enforcement activities. However, if an agency uses a record to deprive an individual of a right, benefit, or privilege, the agency must disclose the record except if it would reveal the identity of a source who furnished the information under an express promise of confidentiality. The third covers investigatory material compiled for determining eligibility for federal employment, contracts, or access to classified information.[101] The exemption is available only to protect a source expressly promised confidentiality.

Together, the Act's exemptions allow national security and law enforcement activities to comply with some or most of the privacy requirements otherwise applicable to the federal government. One of the principal purposes of the Act was to stop secret government record keeping, and the Act does not exempt any agency from the requirement for openness. However, all exempt systems have some protection from the access and amendment provisions of the Act and can have broad authority to collect information free from relevance requirements.

This type of special treatment that allows national security and law enforcement activities to avoid full compliance with privacy standards is not unusual. The European Union's Data Protection Directive[102] applies broadly to record keepers within Europe. However, under Article 3 of the Directive, the regulatory scheme does not apply to activities that fall outside the scope of community law, processing operations for public security, defense, state security, and criminal law activities. EU Member States may provide privacy protections for these activities.

The Privacy Act of 1974 also restricts computer matching. However, the definition of matching programs both narrow and technologically outmoded.[103] It only covers matching for federal benefit programs, for recouping overpayments for those programs, and of federal personnel records. In addition, the definition expressly excludes matching for some civil or criminal law purposes, for foreign counterintelligence, and for some other purposes. The matching restrictions are not likely to be relevant to computer matching activities supporting cyberattack prevention.

The Privacy Act of 1974 would apply to federal agency cyberattack prevention activities that create systems of records. Technical and policy activities would not likely create any covered records about individuals (except for employment records), but criminal and civil investigatory activities would. There could well be some gray areas. For example, if cyberattack prevention involved offensive and not just defensive actions—e.g., seeking to disrupt the actions of a hacker—it might not be clear whether the

[98]Id. at § 552a(j)(1) & (2).
[99]Id. at § 552a(k)(1).
[100]Id. at § 552a(k)(2).
[101]Id. at § 552a(k)(5).
[102]Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm; accessed March 26, 2010.
[103]5 U.S.C. § 552a(a)(8).

activity qualifies as a law enforcement activity that could be exempted from some of the Act's provisions. If classified, however, the activity could utilize an exemption regardless of its law enforcement characterization.

In the end, the Privacy Act of 1974 would not create a barrier to cyberattack prevention activities that is any more significant or disruptive than the low barriers it presents to intelligence, defense, or law enforcement functions. In the decades since the Act became effective, there have been few reported problems in these spheres and few amendments. This is not to suggest that the law provides the privacy rigor that advocates or civil libertarians might like or that some agencies would not prefer a broader exemption. Some controversies have not arisen sharply because of the Act's increasing technological obsolescence. For example, not all agencies define electronic mail systems as falling within the Act's scope.

Depending on the scope of cybersecurity activities, however, information privacy controversies could easily arise. The routine collection and maintenance of personal information about the Internet activities of individuals in the absence of a specific law enforcement investigation would raise questions about the scope of the activity and the corresponding obligations regarding the maintenance, use, and disclosure of the information. Obviously, the limitations of the Fourth Amendment and of surveillance statutes would be highly relevant here, establishing procedures and standards for some government actions. The Privacy Act of 1974's standards define additional privacy obligations for personal information collected, compiled, and retrieved by individual identifier. The Act's technological shortcomings create some loopholes that cybersecurity activities might lawfully use.

To the extent that personal information processing can be accomplished using de-identified data or using data minimization policies and practices,[104] privacy issues can be avoided or diminished, and privacy laws may be inapplicable. However, while advocates welcome these approaches, their utility can be limited. Although the Privacy Act's policies may gently push agencies toward using less data, most agencies have no difficulty justifying the collection and maintenance of more personal information except where another statute directs otherwise. The Act's actual barriers are minor, and an agency that wants to can always find a justification for more data. Another reality is that anonymized or de-identified information can often be re-identified, often without much difficulty. There is growing recognition that personal data cannot be successfully anonymized or de-identified.[105] Professor Latanya Sweeney, an authority on anonymity, put it this way: "I can never guarantee that any release of [deidentified] data is anonymous, even though for a particular user it may very well be anonymous."[106] That does not mean that efforts to remove identifiers will never protect a privacy interest, only that the protections that come with de-identification may be overcome.

One possible model for the sharing of de-identified data can be found in the federal health privacy rule issued under the authority of the Health Insurance Portability and Accountability Act (HIPAA). The rule provides that the removal of 18 specific data elements from a health record generally creates anonymized data that is no longer subject to the rule's requirements.[107] A second provision allows for the creation of a *limited data set* containing more data elements and that can potentially be re-identified. A limited data set can be shared for specified purposes and then only under a *data use agreement* that specifies the terms of use and disclosure and that prohibits re-identification.[108]

---

[104]See, e.g., the minimization procedures for electronic surveillance included in the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801(h).

[105]See, e.g., Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization,* 57 UCLA Law Review 1701 (2010). See also Robert Gellman, *Privacy for Research Data*, Panel on Confidentiality Issues Arising from the Integration of Remotely Sensed and Self-Identifying Data, National Research Council, Putting People on the Map: Protecting Confidentiality with Linked Social-Spatial Data (2007) (Appendix A), http://books.nap.edu/catalog.php?record_id=11865, accessed June 29, 2010.

[106]National Committee on Vital and Health Statistics, Subcommittee on Privacy and Confidentiality, *Proceedings of Roundtable Discussion: Identifiability of Data* (Jan. 28, 1998), available at http://ncvhs.hhs.gov/980128tr.htm.

[107]45 C.F.R. § 164.514(b)(2).

[108]Id. at § 164.514(e).

Neither HIPAA de-identification method is perfectly suited to the cybersecurity arena, but the notion of limited use, written limitations, and prohibitions on re-identification may be adapted as part of information collection or sharing. These or additional controls could be provided by statute, Executive Order, contract, oversight mechanisms, public or other reporting, administrative procedures, or other mechanisms that would impose, enforce, and oversee restrictions on personal data use and sharing. The policy could allow some or all data restrictions to be overridden under a defined standard and procedure that could be as rigorous as desired, even requiring probable cause and judicial approval at the high end. There is much opportunity here for creativity in policy and legislation.

2. Foreign Privacy Laws

Because the Internet is global, cyberattack prevention will not necessarily be domestic in scope and may involve other governments and may focus on events and activities in other countries. To the extent that cybersecurity activities involve the transfer of personal information across national borders, foreign data protection laws may impose some barriers on the export of data to the United States.[109] The best example comes from the European Union, where the EU Data Protection Directive establishes rules for the transfer of personal data to third countries.[110] The general standard allows data exports to third countries that ensure an *adequate level of protection*.[111] The EU has not made any determination whether the United States generally meets this standard, and it is unlikely to do so. Some other countries were found to be adequate, including Canada. In the absence of adequacy, the Directive allows for data exports under specified circumstances.[112] One category of allowable transfers covers those necessary or legally required on important public interest grounds.[113] This would allow personal transfers for some cybersecurity-related activities just as it allows transfers for law enforcement activities.

Outside the EU, other nations have different policies regarding personal data exports. Depending on the nature and purpose of a cyberattack prevention data export restriction, national privacy laws may or may not impose meaningful barriers. Much depends on the details. In general, data protection rules do not prevent law enforcement or national security cooperation. However, as the EU's Article 29 Working Party observed in an opinion about international cooperation on anti-doping activities in sports, "controllers in the EU are responsible for processing personal data in compliance with domestic law and must therefore disregard the World Anti-Doping Code and International Standards insofar as they contradict domestic law."[114] In other words, national data protection laws can matter regardless of international cooperative efforts.

[109]U.S. privacy laws rarely address the export of regulated data to other nations. Some data restrictions may continue to apply to exported data or to the exporters of the data, but this may not always be the case. Restrictions on use of data by financial institutions subject to Gramm-Leach-Bliley, 15 U.S.C. § 6802, would apply to international transfers to affiliates. However, health data sent to a foreign health care provider as allowed by the Health Insurance Portability and Accountability Act Privacy Rule, 45 C.F.R. Part 164, would pass outside the scope of the rule and be unregulated by U.S. law. On the other hand, the restrictions imposed by the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6506, apply to any website located "on the Internet" directed at children. Cross border enforcement of privacy laws is often problematic.

[110]The Directive establishes standards that each Member State must comply with through its own national laws. Article 4.

[111]Article 25.1.

[112]Article 26.1.

[113]Article 26.1.c.

[114]ARTICLE 29 Data Protection Working Party, *Second opinion 4/2009 on the World Anti-Doping Agency (WADA) International Standard for the Protection of Privacy and Personal Information, on related provisions of the WADA Code and on other privacy issues in the context of the fight against doping in sport by WADA and (national) anti-doping organizations* (April 6, 2009) (WP 162), http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp162_en.pdf; accessed March 29, 2010.

V. ISSUES RELATING TO DUE PROCESS, LICENSING, AND IDENTIFICATION

This section reviews three existing identification/authentication systems in order to provide background for possible consideration of licensing systems for Internet users, for software programs, services, or equipment used to access the Internet. Microsoft's chief research and technology officer recently suggested licensing individuals, machines, and programs using the Internet as a response to the crime, fraud, spying, and other unwelcome Internet activities that have become commonplace.[115] Some type of Internet licensing scheme may have application for cyberattack prevention.

The United States has experience with issuing credentials in a wide variety of contexts. We identify and authenticate people to varying degrees, depending on the purpose of the activity. Each system has its own process rules and privacy rules. The purpose here is not to suggest that any of these systems is a model for identification, authentication, or licensing on the Internet. The goal is to illustrate how we have dealt with privacy, identification, due process, and other facets of identification/authentication systems that affect the ability of people to function.

The first system described here is the security clearance system that regulates who can have access to national security information. The issuance of a security clearance for TOP SECRET information requires an intensive investigation as a precondition. The second system is the driver's license system. Because driver's licenses have become standard identifiers in many contexts, the licenses have a significance far beyond control of driving. With the enactment of the REAL ID Act of 2005, the level of controversy surrounding drivers' licenses has expanded considerably, and changes to the Act remain under consideration by the Congress. The third system is Secure Flight, the airline passenger pre-screening program run by the Transportation Security Administration. Unlike the other two systems highlighted here, Secure Flight operates in more of a real-time, case-by-case mode.[116]

1. The Security Clearance Model

A. Issuance

Only those who have a security clearance can have access to federal government information classified in the interest of national defense or foreign policy.[117] Information pertaining to cybersecurity can qualify under this standard, and those who need access to the information will require a security clearance.

---

[115]See Barbara Kiviat, *Driver's Licenses for the Internet*, The Curious Capitalist Blog (Jan. 30, 2010), at http://curiouscapitalist.blogs.time.com/2010/01/30/drivers-licenses-for-the-internet (discussing comments of Craig Mundie); accessed April 12, 2010.

[116]Another system of potential interest is a recently adopted federal government identification and credentialing system for federal government employees and contractors. The new system began with the issuance of Homeland Security Presidential Directive 12 (HSPD-12) in August 2004, available at https://www.dhs.gov/xabout/laws/gc_1217616624097.shtm#1; accessed March 16, 2010. This directive called for the establishment of a mandatory, interoperable, government-wide standard for secure and reliable forms of identification for federal government employees and contractors who access government-controlled facilities and information systems. The National Institute of Standards and Technology issued the standard in 2005. National Institute of Standards and Technology, *Personal Identity Verification (PIV) of Federal Employees and Contractors* (FIPS 201) (2006), available at http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf; accessed March 16, 2010. The standard has two parts. The first part sets out uniform requirements for verifying the identity of individuals applying for official agency credentials, issuing credentials, maintaining related information, and protecting the privacy of the applicants. The second part specifies the technical requirements for the smart cards used in the system. The identity proofing requires a background investigation, such as a National Agency Check with Written Inquiries; a FBI National Criminal History Fingerprint Check; requiring applicants to appear in person at least once before the issuance of an ID card; and requiring applicants to provide two original forms of identity source documents.

[117]Differences between clearance standards and procedures among federal agencies are not material here, nor are additional types of higher-level clearances that are prerequisites to access to specific classes of information with greater sensitivity. The description here is of the basic Department of Defense program. See generally Department of Defense, Personal Security Program, DoD 5200.2-R (1996), available at http://www.dod.mil/dodgc/doha/5200.2-R.pdf; accessed March 16, 2010. Legislation on security clearances can be found in 50 U.S.C. Chapter 15 (§§ 435-438).

Prior to issuing a clearance, the federal agency conducts an investigation, with most investigations now done by the Office of Personnel Management. The investigation inquires into an individual's loyalty, character, trustworthiness, and reliability to ensure eligibility for access to national security information. The policy sets out thirteen relevant criteria: allegiance to the United States; foreign influence; foreign preference; sexual behavior; personal conduct; financial considerations; alcohol consumption; drug involvement; emotional, mental, and personality disorders; criminal conduct; security violations; outside activities; and misuse of information technology systems.[118]

The extent of the investigation depends on whether access is required to information classified as CONFIDENTIAL, SECRET, or TOP SECRET. For a CONFIDENTIAL or SECRET clearance, the investigation consists of a National Agency Check (FBI and other federal agency files), a Local Agency Check (local law enforcement files), and a Financial Check (credit record). For a TOP SECRET clearance, the investigation adds field interviews of references, employers, and others; checks of records held by employers, courts, and rental offices; and an interview with the applicant. The TOP SECRET clearance is considerably more costly, intensive, and invasive than the lower-level clearances.

Government employees, military personnel, civilian contractors, and others who require classified information may receive clearances. Only U.S. citizens are eligible for a security clearance. Foreign nationals may be granted a "Limited Access Authorization" (LAA) in "rare circumstances" when a non-U.S. citizen possesses a unique or unusual skill or expertise urgently needed for a specific requirement involving access to specified classified information for which a cleared or clearable U.S. citizen is not available.

Applicants for a clearance complete Standard Form 86 (Questionnaire for National Security Positions),[119] a 21-page document that calls for the disclosure of large amounts of personal information. SF 86 requires the applicant to authorize broadly the disclosure of information from third parties, including employers, schools, landlords, financial institutions, criminal justice agencies, healthcare providers, retail business establishments, and others.

The security clearance process operates subject to the Privacy Act of 1974,[120] a law that provides a reasonably full set of fair information practices. Standard Form 86 includes a Privacy Act notice, an explanation of the process, and a statement that false or inaccurate statements may be a criminal violation of law.

The cost and time to obtain a clearance are not simple numbers to report. A statutory standard calls for completion of at least 80 percent of initial clearances within an average of 120 days.[121] In 2008, the Government Accountability Office (GAO) found that the Office of Personnel Management and DOD made initial decisions on clearances within 87 days.[122] However, GAO also found that 39 percent took more than 120 days. The cost of the basic background investigation for a TOP SECRET clearance begins at $3888, and this does not include other required investigations and administrative costs. Depending on the specifics of any individual clearance, cost can exceed $10,000.[123] CONFIDENTIAL or SECRET clearance do not take as long (estimates of one to three months) and cost less (several hundred dollars to $3,000).

People with security clearances must be routinely reinvestigated at intervals depending on their level of clearance. For a TOP SECRET clearance, periodic reinvestigations should occur every five years.

---

[118]Congress has also intervened from time to time to establish some specific standards for denial of clearances. For a discussion of recent legislation, see Sheldon I. Cohen, *The Smith Amendment, 10 U.S.C. §986 Has Been Repealed and Replaced By 50 U.S.C. 435b § 3002* (2008), available at http://www.sheldoncohen.com/publications/Smith_Amendment2008.pdf; accessed March 16, 2010.

[119]http://www.opm.gov/forms/pdf_fill/sf86.pdf; accessed March 16, 2010.

[120]5 U.S.C. § 552a.

[121]50 U.S.C. § 435b(g). The statutory goal is to reduce the time to 60 days.

[122]*Personnel Security Clearances: Progress Has Been Made to Reduce Delays but Further Actions Are Needed to Enhance Quality and Sustain Reform Efforts* (GAO-09-684T) (2009), available at http://www.gao.gov/new.items/d09684t.pdf; accessed March 16, 2010.

[123]See Office of Personnel Management, *Investigations Reimbursable Billing Rates for FY 2009* (Notice 08-04) (2008), available at http://www.wrc.noaa.gov/wrso/forms/Investigations%20Reimbursable%20Billing%20Rates.pdf; accessed March 16, 2010. The quoted cost is for the Single-Scope Background Investigation.

B. Denial and Revocation

For investigations that do not produce results favorable to the applicant, the due process protections include two levels of review by higher-ranking adjudicative officials. The denial process also provides additional reviews at a higher level and approval of a letter of intent to deny or revoke. The subject of an unfavorable action must receive a written statement of the reasons for the action. The statement must be as comprehensive and detailed as permitted by national security and by the confidentiality provisions of the Privacy Act of 1974 that protect information from sources expressly promised confidentiality. The individual is entitled to request a copy of releasable records of the investigation. The individual has 30 days to reply in writing, and the individual is entitled to a prompt written response to any submission.

The individual also has an opportunity to appeal a letter of denial to the appropriate DOD Component Personnel Security Appeals Board. If requested, an administrative law judge of the Defense Department's Office of Hearings and Appeals holds a hearing. The individual is entitled to a written final decision. Judicial review of a security clearance denial appears precluded under current law, although some argue that there should be limited appeal rights. Judicial deference to the executive branch in national security matters explains the absence of a judicial appeal.

Once granted, an agency can suspend a security clearance if it has information raising serious questions as to the individual's ability or intent to protect classified information or to execute sensitive duties until a final determination. The individual is entitled to written notice and a brief statement of the reason. Resolution of the suspension must occur as expeditiously as circumstances permit

C. Discussion

A security clearance is typically a requirement for employment, so the interest of an applicant for or holder of a clearance is high. The administrative procedures that surround the approval and revocation of a clearance generally reflect both the importance of that interest to the individual and the interest of the government in protecting material that would "cause exceptionally grave damage" to national security if publicly available (the standard for information classified as TOP SECRET). The process for granting a clearance is complex and expensive, can be time consuming, includes significant procedural and other protections, and has established written standards. The system operates under general federal government privacy rules, although it can and does make use of exemptions that exist in those rules. While the granting or denial of a clearance requires considerably judgment ("an overall common sense determination based upon all available facts"), the layers of review and the rights to appeal are designed to address the possibility of bias or unfairness.

While it would be too strong to suggest that there is no concern at all about the due process protections of the security clearance process, it is probably fair to suggest that the existing procedures are not so unbalanced as to raise significant public concerns or to cause ongoing debates. Congress has intervened from time to time to adjust the standards, although that intervention has been controversial, potentially disruptive, and hard to change, all features typical for the political process. Congress has also expressed concern about and legislated to limit delays in the clearance system in the interest of efficiency. Delays in obtaining clearances for employees are costly to the government and to its contractors that hire employees with security clearances.

2. The Driver's License Model

A. Issuance and Identification

The issuance of licenses for drivers is a state function, and the rules and procedures vary across the states and territories. Different types of drivers' licenses (car, truck, motorcycle, taxi, etc.) exist, including

permits for learners issued before driving proficiency has been demonstrated. The parts of the licensing process of greatest interest in a civil liberties and privacy context are the identification requirements and the rules for revoking a license. Rules about demonstrating ability to drive are not material here and are not discussed.

The driver's license has become a de factor identifier accepted for many purposes in the United States.[124] As a result, Departments of Motor Vehicles also issue an identification card comparable to a driver's license that identifies individuals but does not authorize driving. An ID card typically resembles a driver's license and has the same security and identification features as a license to drive. Some states also issue enhanced licenses and ID cards that combine a regular driver's license with the specifications of the new US passport card, a wallet-size travel document that can be used to re-enter the United States from Canada, Mexico, the Caribbean, and Bermuda.[125] Driver's licenses may include other information (e.g., organ donor status).

The most important current federal law on the issuance of licenses is the REAL ID Act of 2005.[126] This controversial law establishes federal standards for security, authentication, and issuance of state driver's licenses. While the federal standards are not exactly mandatory, a state license must meet those standards for the federal government to accept the license for official purposes, such as using a driver's license for boarding commercially operated airline flights and for entering federal buildings and nuclear power plants.

The current status of REAL ID is somewhat uncertain, and Congress is considering amendments that would make some significant changes.[127] Nevertheless, the law provides an example of a stricter set of policies for identifying and authenticating recipients. Unlike a security clearance that requires regular renewal following a reinvestigation, a driver's license can usually be retained and renewed without further review of the holder.[128]

REAL ID requirements include:

> *Document Standards*: A license must include: (1) individual's full legal name, (2) date of birth, (3) gender, (4) DL/ID number, (5) digital photograph, (6) address of legal residence, (7) signature, (8) physical security features designed to prevent tampering, counterfeiting or duplication for fraudulent purposes, and (9) a common machine-readable technology. Radio frequency identification (RFID) is not required [for] a card meeting REAL ID standards. Compliance with a bar code standard is required.
>
> *Minimum Issuance Standards*: (1) A photo identity document; (2) documentation showing date of birth; (3) proof of a SSN or verification that the individual is not eligible for an SSN; and (4) documentation showing name and address of principal residence.
>
> *Foreign Documents*: A state may not accept any foreign document other than an official passport.
>
> *Verification of Documents*: A state must (1) verify, with the issuing agency, the issuance, validity and completeness of each document presented; (2) confirm a full SSN with the Social Security Administration; and (3) establish an effective procedure to confirm or verify a renewing applicant's information.

---

[124]Interestingly, federal law at one time required states to put Social Security Numbers on the license. Now it prohibits displaying an SSN on a license.

[125]Department of State, 7 Foreign Affairs Manual 1300, Appendix P (The Passport Card), available at http://www.state.gov/documents/organization/122897.pdf; accessed March 15, 2010.

[126]49 U.S.C. § 30301 note. For a summary of the law from the non-partisan National Conference of State Legislatures, see http://www.ncsl.org/IssuesResearch/Transportation/RealIDActof2005Summary/tabid/13579/Default.aspx; accessed March 15, 2010.

The Driver's Privacy Protection Act (DPPA), 18 U.S.C. § 2721-2725, is a federal law that regulates the disclosure of personal information by state motor vehicle departments. The law allows non-consensual disclosures for specified purposes, including for governmental, judicial, law enforcement, and motor vehicle activities. Disclosure for a marketing use requires affirmative consent. The law largely ended the availability of information about drivers and vehicles for marketing purposes. Some motor vehicle licensing and registration information still ends up in the hands of commercial database companies because they manage automobile recall activities. The information disclosed for authorized purposes is not supposed to be used otherwise. The DPPA pre-dates and bears no express relationship to the REAL ID Act, but the two laws are not incompatible.

[127]See, e.g., PASS ID Act, S.1261, 111th Congress (2009).

[128]Some states require older drivers to demonstrate a continued ability to drive.

Immigration Requirements: A state can only issue a REAL ID license to citizens, lawfully admitted residents, and selected other immigrants and only with verified and valid documentary evidence of status.

Security and Fraud Prevention Standards: A state must (1) ensure security for document materials and locations where they are produced; (2) have security clearance requirements for producers of IDs; and (3) establish fraudulent document recognition training programs for employees engaged in the issuance of licenses.

Data Retention and Storage: A state must (1) capture digital images of identity source documents for storage and transfer; (2) retain paper copies of source documents for at least seven years or images at least ten years; and (3) maintain a state motor vehicle database that contains all data fields printed on a license, and drivers' histories, including violations, suspensions, and points.

Linking of Databases: A state must provide all other states with electronic access to information contained in the motor vehicle database of the state.

Many aspects of REAL ID have drawn objections, including but not limited to the cost of compliance by states and individuals and the unfunded mandate. A study conducted by the National Conference of State Legislatures, National Governors Association, and the American Association of Motor Vehicle Administrators estimated that state costs could be more than $11 billion over five years. The Department of Homeland Security estimate is $3.9 billion.[129] Many states have taken some formal action to object to—or even to prohibit compliance with—REAL ID.[130] State objections are not solely based on cost.

There are also strong objections to REAL ID among public interest and advocacy organizations all along the political spectrum. Some contend that REAL ID will become a national identity system or internal passport used to track and control individuals' movements and activities. Another objection is that it will not be effective against terrorism because ID documents do not reveal anything about evil intent and because fraudulent documents will be available. Bureaucratic concerns are the center of other objections because of the difficulty of verifying documents (e.g., foreign birth certificates and the like), long times for the issuance process, and higher fees.

Other objections to REAL ID center on the creation of a single interlinked database and on the storage of copies of every birth certificate and other documents as a new resource for identity thieves. Some fear exploitation of a machine-readable card by private sector actors scanning a magnetic strip on a driver's license for credit card or age verification purposes and then collecting additional data for marketing or other purposes. Another concern is that the REAL ID database will grow over time and acquire additional identity-based missions. Objections also focus on the effects on immigrants and possible discrimination against foreigners or those who look foreign.[131] The Act's failure to accommodate those who have a religious objection to having their photographs taken is a point of controversy.[132] Constitutional objections include First and Tenth Amendment arguments, as well as arguments about limitations on the right to travel.

[129]For a summary of various REAL ID cost estimates, see National Conference of State Legislatures, *REAL ID Cost Estimates*, available at http://www.ncsl.org/Default.aspx?TabId=13578; accessed March 15, 2010.

[130]For a summary of anti-REAL ID activities in the states, including some states that enacted laws prohibiting implementation, see http://www.realnightmare.org/news/105/, accessed August 30, 2010.

[131]For a website of REAL ID opponents, see http://www.realnightmare.org/; accessed March 15, 2010. For a Department of Homeland Security website on REAL ID, see http://www.dhs.gov/files/laws/gc_1172765386179.shtm; accessed March 15, 2010. The rule establishing minimum standards is at http://edocket.access.gpo.gov/2008/08-140.htm; accessed March 15, 2010.

[132]Religious objections can arise with any form of required identification. See Cynthia Brougher, *Legal Analysis of Religious Exemptions for Photo Identification Requirements* (2009) (Congressional Research Service), available at http://www.fas.org/sgp/crs/misc/R40515.pdf; accessed March 15, 2010. See also Council on American-Islamic Relations Research Center, *Religious Accommodation in Driver's License Photographs: A review of codes, policies and practices in the 50 states* (2005), available at http://moritzlaw.osu.edu/electionlaw/litigation/documents/LWVJ.pdf; accessed March 15, 2010. The Religious Freedom Restoration Act, 42 U.S.C. § 2000bb et seq., which statutorily mandates a standard of protection of heightened scrutiny for government actions interfering with a person's free exercise of religion, may have bearing on any resolution of these issues.

Some DHS actions to address privacy and other concerns include: (1) a phased enrollment that allows states to put off compliance on those born before December 1, 1964 an additional three years; (2) technical measures for verifying documents from issuing agencies in other states through a hub-based network and messaging system with end-to-end data encryption; (3) requiring states to collect a minimum of information; (4) and issuing a set of privacy and security best practices that are built on the Fair Information Principles and Federal Information Security Management Act[133] (FISMA) standards to help guide the states in protecting the information collected, stored, and maintained pursuant to the REAL ID; and (5) no preemption of state law that may provide additional protections.

Not every aspect of REAL ID has drawn complaints. There is more support for the standardization of drivers' licenses among the states and for better security in the issuance process. Because a driver's license is a breeder document (i.e., an identification document that can be readily used to obtain other documentation that confers status or privileges), greater control over issuance draws broader support.

B. Revocation

The revocation of a driver's license can arise under a variety of circumstances. In most cases, notice, a right to a hearing, and other elements of procedural due process are routinely available and do not usually raise major fairness concerns. The proceedings address the conflicting interests, and decisions come through a process designed to be fair and balanced.

The cases that raise the sharpest due process issues are those involving administrative license suspension (ALS) laws. ALS involves the automatic suspension of a license when a driver refuses to submit to chemical testing for alcohol or when a driver submits to testing and the results indicate a high level of blood alcohol content. The consequences come immediately and without formal proof of guilt. Case law on the constitutionality of ALS is clear.

It is worth noting as a preliminary matter that the traditional distinction between a right and a privilege does not appear particularly helpful here. Whether a license is viewed as a right protected by constitutional guarantees or a privilege granted by the state that can be revoked, it is not permissible for the state to impose unconstitutional conditions or to act in most instances without appropriate due process. A license holder typically has a clear property interest in the license, and that interest must be respected.

In a leading case on this specific subject, the Supreme Court held that the "suspension of a driver's license for statutorily defined cause implicates a protectable property interest; accordingly, the only question presented by this appeal is what process is due to protect against an erroneous deprivation of that interest."[134] The Court identified three relevant factors:

> First, the private interest that will be affected by the official action; second, the risk of an erroneous deprivation of such interest through the procedures used, and the probable value, if any, of additional or substitute procedural safeguards; and finally, the Government's interest, including the function involved and the fiscal and administrative burdens that the additional or substitute procedural requirement would entail.[135]

While the driver's interest in the license is substantial, ALS provides for a limited period of suspension with an opportunity for a hearing in a reasonable period. The state's substantial interest in keeping drunk drivers off the roads is an important factor in upholding the immediate suspension. The Court observed that it "traditionally accorded the states great leeway in adopting summary procedures to protect public health and safety."[136] Presumably, the Court was well aware of heightened public concern in recent decades about the dangers of drunk driving.

---

[133]44 U.S.C. § 3541 et seq.
[134]*Mackey v. Montrym*, 443 U.S. 1 (1979) (footnote omitted).
[135]Id. at 10.
[136]Id. at 17.

C. Discussion

The system for licensing drivers has some significant differences from the system for granting security clearances. The driver's license process is decentralized among the states, whereas only the federal government grants clearances (albeit different agencies have their own policies and procedures). While drivers must demonstrate skills, knowledge, and physical abilities, no substantive standard requires judgments about an individual's intentions or loyalty. Drivers of the proper age and skill expect to obtain and keep a driver's license for most of their lives without further questioning. However, security clearances must be renewed regularly after an updated investigation, although a clearance is not normally revoked if a required reinvestigation has not occurred.

The driver's license system operated successfully under privacy regimes that varied considerably from state to state until the federal Driver's Privacy Protection Act (DPPA) established a national floor of privacy protection.[137] While controversial in some respects, the DPPA did not undermine the fairness of the licensing system from a driver's perspective.

Revocations are not that dissimilar for clearances and for licenses. Using recognized grounds, both can be revoked or suspended immediately with due process rights for affected individuals that can be pursued after-the-fact rather than before.

It remains unclear at this time how, when, and whether REAL ID will be fully implemented. Therefore, it is impossible to predict how the existing process will change. However, if nothing else, the history of REAL ID demonstrates that identification systems can generate considerable public controversy in the United States. An identification system that affects more people and that has more consequences for them will be the subject of political debate and likely litigation. Millions of people have security clearances, but hundreds of millions of people are likely to need REAL ID identification.

3. The Air Travel Clearance Model

A. Clearance

Following the events of September 11, 2001, and subsequent air travel incidents, the systems for clearing passengers for air travel have changed and evolved. An early program called *Computer Assisted Passenger Prescreening System* (CAPPS II) has been replaced by *Secure Flight* administered by the Transportation Safety Administration (TSA) of the Department of Homeland Security (DHS).[138] Secure Flight offers a different model for clearing individuals for a particular activity, one that is based on weeding out those who have been determined through an independent (and largely secret) process not to be allowed to fly.

Secure Flight makes individualized decisions of who may fly on commercial flights. A major part of Secure Flight is matching names of passengers with the *No Fly* list of individuals not allowed to fly and with the *Selectee* list of individuals who must undergo additional security screening before boarding an aircraft. These two lists are maintained by the Terrorist Screening Center (part of the Federal Bureau of Investigation) and are subsets of the Terrorist Screening Center Database compiled using information from law enforcement and intelligence agencies. At times, TSA may consult lists other than the *No Fly* and *Selectee* lists for clearing passengers, and the process can include random searches and real-time decision making based on interactions between would-be travelers, airline staff, TSA, and intelligence and law enforcement agencies.

The clearance process mostly takes place behind-the-scenes by TSA and the airlines. The process compares information in airline reservation systems, including but not limited to the information pro-

[137] 18 U.S.C. §§ 2721-2725.

[138] The Secure Flight program is authorized under 49 U.S.C. § 44903. TSA's 2008 Privacy Impact Assessment for the Secure Flight Program is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_secureflight2008.pdf; accessed March 15, 2010.

vided by a passenger when making an airline reservation, with information on the watch lists. In order to do better matches of records, TSA and the airlines started requiring passengers to provide full name, data of birth, and gender at the time of a reservation. These additional elements are supposed to help prevent misidentification of passengers with similar names. Other information that TSA receives from the airline includes itinerary, passport number (for an international flight or if otherwise available to the airline), and reservation control number. TSA can obtain a full Passenger Name Record (PNR), which reveals other information including food, health, and other preferences.

TSA retains records for individuals not identified as potential matches by the automated matching tool for seven days after completion of travel. TSA keeps records of an individual who is potential or confirmed match for no less than seven years. TSA keeps records of an individual who is a confirmed match for 99 years. Data retained by airlines is not subject to these limits, and TSA may obtain the data from the airlines.

A *registered traveler* program allowed passengers who paid a fee and submitted to a background check to use reserved security lanes with shorter waits at airport checkpoints. The program was voluntary and run by the private sector. An applicant provided additional information, including a biometric, and received a smart card credential. When the company that provided the bulk of the service went out of business, the registered traveler program disappeared. Some criticized the program as providing special treatment for wealthy travelers.

B. Redress

TSA has a program offering redress to travelers who experience denied or delayed airline boarding, who experience denied or delayed entry into and exit from the U.S., or who are continuously referred for additional (secondary) screening. The *Travel Redress Inquiry Program* (DHS TRIP) basically allows an individual to ask for a review in order to minimize or eliminate future watch list name confusion. TSA will not reveal whether an individual is on a watch list, however. An individual seeking redress fills out a form and may be asked to provide additional documentation. A successful traveler will receive a Redress Control Number that airlines collect and that may help to minimize identification or screening problems. An individual who is dissatisfied with the DHS TRIP process may file an appeal with DHS. Effective judicial review of DHS actions may not be available.

The Secure Flight program collects and maintains information on international travelers from airlines, travel agencies, and tour operators in other countries. This brings aspects of the program under the purview of foreign data protection laws. For example, in 2007, the European Union and DHS entered into an agreement about the processing and transfer to DHS of Passenger Name Records (PNR) by airlines operating in Europe.[139] The agreement reflects a determination by the European Commission that U.S. laws, in conjunction with DHS policies regarding the protection of personal data and the U.S.-EU Passenger Name Record Agreement, are adequate to permit transfers of PNR data to the U.S government and that the transfers comply with EU standards under the Data Protection Directive. The agreement is now subject to ratification by the European Parliament,[140] where some members have been critical of the terms of the data transfers.

C. Discussion

The Secure Flight process differs significantly from the process for granting security clearances and drivers' licenses. While Secure Flight is not quite a real-time clearance, it can be close to that. Normally,

[139]http://www.dhs.gov/xlibrary/assets/pnr-2007agreement-usversion.pdf; accessed March 15, 2010.

[140]See European Parliament, Legislative Observatory, available at http://www.europarl.europa.eu/oeil/file.jsp?id=5836052; accessed March 15, 2010. On May 5, 2010, the European Parliament showed its displeasure with the agreement by postponed voting on its approval. http://www.europarl.europa.eu/news/expert/infopress_page/019-74146-125-05-19-902-20100505IPR74145-05-05-2010-2010-false/default_en.htm; accessed May 21, 2010.

there is no review of identity documents other than a limited check at an airport security checkpoint or the presentation of passports for international travel. The program mostly matches individuals against lists of people not allowed to fly or who require additional screening. These lists are compiled by TSA and other agencies separately and based on criteria that are not publicly known. TSA will not directly inform an individual if he or she is on one of the lists, although inferences are possible from the way that the individual is treated at the airport. Clearance operations are not conducted in public view, and travelers do not know the details of the review process. Secure Flight clears as many as several million people daily and hundreds of millions of people annually, many more people than seek security clearances or drivers' licenses.

The Secure Flight redress process came as a legislative direction that followed regular news reports of continuing problems with the clearance process. Congress intervened several times during the development and implementation of airport passenger clearance systems to express concern about privacy and about redress. Secure Flight also raises directly issues of international privacy standards that are absent from drivers' licenses and security clearances. It is possible that the international consequences of any standards for cybersecurity activities would require negotiations with other countries similar to the negotiations with the EU about Secure Flight. Finally, Secure Flight has been controversial, with interest groups raising privacy and constitutional objections to the data collection, screening, and secrecy.

4. Other Methods, Other Models

Broader use of identification for general purposes or for cybersecurity purposes will raise harder political, legal, and constitutional issues. The precise terms of any identification use, issuance procedures, due process rules, and information processing policies will shape the arguments about constitutionality and effects on civil liberties and privacy. It is not possible here, to make all the arguments or resolve any of them. However, it is apparent that an identification system has the potential to impinge on anonymity, inhibit speech and association, affect the right to travel, affect other fundamental constitutional or statutory rights, and perhaps exceed the authority of the federal government in other ways (Tenth Amendment). Whether the courts would recognize any of these concerns at the constitutional level is impossible to predict, but it seems certain that these issues will arise.

In 2008, the Supreme Court upheld a state law requiring citizens voting in person to present government-issued photo identification.[141] It may or may not be telling that the identification requirement did not extend to those who did not vote in person. However, the Help America Vote Act of 2002 requires first time registrants voting by mail to include a copy of identification with the ballot.[142] The Court did not require strict scrutiny of the voter ID law, but judicial consideration of a requirement that affects broad First Amendment speech issues is less likely to use the same, weaker standard of judicial review. Regardless, it is difficult to use this decision to assess possible Internet identification requirements because the facts and the particulars could make a major difference. Still, the Court upheld the identification requirement here and reached a similar outcome in the *Hiibel* case discussed above. Clearly, the Court is not strongly averse to identification requirements.

The federal government is already exploring and implementing identity, credentialing, and access management systems to provide a consistent approach for clearing and managing individuals requiring access to federal information systems and facilities.[143] Identification and authorization systems can be unremarkable from a privacy and civil liberties perspective, but they can also raise a host of questions depending on the standards used, due process procedures, scope of application, and data collected and retained. These same issues can arise with any type of identification or licensing system.[144]

[141]Crawford v. Marion County Election Bd., 553 U.S. ___, 128 S. Ct. 1610 (2008).

[142]42 U.S.C. § 15483(b)(3).

[143]See http://www.idmanagement.gov/drilldown.cfm?action=icam; accessed April 15, 2010.

[144]See generally Committee on Authentication Technologies and Their Privacy Implications, National Research Council, *Who Goes There? Authentication Through the Lens of Privacy* (2003).

In particular, an Internet identification or authentication system can be a surveillance mechanism if the system routinely creates a central record of all Internet activities of each user as a result of the clearance process. An Internet identification or authentication system would raise privacy and security concerns that could easily exceed in range and detail the information about the exercise of First Amendment rights collected in a driver's licensing system, by Secure Flight, or even through the security clearance process. A system that fails to properly assess the degree of risk involved or that makes unwarranted demands on users may exacerbate civil liberties and privacy concerns.[145] If the federal government relied on credentials issued by private entities, those concerns could extend beyond government functions and spill over into the rules and procedures of those private entities.

The federal government's use of systems to control access to *government* computers is not the most troublesome part of credentialing or licensing. A broader government requirement for a license for general use of the Internet beyond access to government facilities would be of greater concern. If licensing were the only way to overcome security problems that made the Internet significantly dysfunctional, the argument for licensing might be stronger than if the purpose of the licensing were to require complete identification and accountability for all Internet activities so that criminals could be identified more readily after the fact. The circumstances that result in licensing of users would make a significant difference to the analysis.

The narrower the purpose and application of an ID system/technology, the less likely it will be to raise these concerns. Despite their widespread de facto use as general-purpose identifiers, drivers' licenses were not as controversial until the REAL ID Act sought to alter the process of issuance, mandated collection and maintenance of more personal information, and established requirements and potential for its use that extended beyond established norms. The 1994 Driver's Privacy Protection Act addressed some of the privacy concerns that surrounded the marketing and other secondary uses of drivers' information.

The widespread use of Social Security numbers (SSNs) for identification has, after many years, brought legislative responses at the federal and state level restricting the collection, use, or display of SSNs in some contexts.[146] Many but not all of these responses followed the explosion of identity theft and of complaints from individuals about the consequences of identity theft.

For many individuals, an identification requirement or other prerequisite for using the Internet (as opposed to a prerequisite for using a particular website) would almost certainly be viewed today as similar in importance to a driver's license, if not more important. Access to the Internet, whether or not a fundamental human right, is now for most people in the United States necessary for employment, communication, routine commercial activities, and many other essential, routine, and daily activities.

None of the licensing models described in this section affects an activity as close to the heart of First Amendment values as an Internet licensing scheme would. A governmentally established identification/authorization prerequisite to general Internet access would be, to say the least, controversial. The level of controversy would vary with the scope of the requirement and the amount of information about Internet access and usage that was retained.

However, a governmentally established prerequisite to access a non-public government network would not be controversial or even novel. The federal government operates classified systems with access limited to individuals who have security clearances. A private requirement for access to a private network or website is largely unremarkable as well. It is not that civil liberties and privacy concerns are entirely absent, but that the basic notion of controlling access to some information and facilities is familiar.

---

[145]The Office of Management and Budget calls for a risk assessment for authentication and a matching of risks to an appropriate assurance level. OMB Memorandum to the Heads of all Departments and Agencies, *E-Authentication Guidance for Federal Agencies* (Dec. 16, 2003), http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf; accessed April 15, 2010.

[146]Section 7 of the Privacy Act of 1974, Public Law 93-579, 88 Stat. 1909 (1974), 5 U.S.C. § 552a note, restricts collection of SSNs by federal, state, and local government agencies. This was one of the first legislated restrictions on SSN use. Many more followed in the 1990s and later.

When an identification/authorization requirement is narrow in application, limited in scope, and simple to meet (e.g., user name and password), controversy is less likely to arise. Indeed, simple, limited purpose identification and authorization systems are in widespread use today with few objections. To the extent that private activities (whether voluntary or required by law) collect and maintain additional records about Internet usage by individuals, those records can become available to the government without notice to or participation by the subject of the records. The availability to the government of a list of every website visited by every Internet user would be controversial, to say the least.[147] The earlier discussion about *U.S. v. Miller* and the lack of privacy protections for records held by third party record keepers is relevant here.

If we split the issue of authorization from identification, we face different choices and analyses. Identification might be required for some functions, but there might be a range of allowable activities that call for demonstrating other attributes (e.g., age) rather than identification.[148] An individual might only receive authorization to undertake some activities (e.g., change computer settings or use a private network) after showing competence in security matters.

Drawing lines, however, is not that simple. Even if restricting access to private networks—whether operated by the government or others—is not on its face problematic, much will depend on what activities occur on the private network. We already have private systems with varying identification and authentication prerequisites. Some may raise civil liberties or privacy concerns, but private sector activities will fall outside most constitutional and statutory protections. However, if a citizen must have some form of identification or authorization in order to communicate or conduct ordinary, non-national security business with a government agency, the argument about the propriety of the identification requirement would turn in part on the nature of the communication or the business at issue. The requirement would raise, for example, concerns about impinging on the right to petition the government for a redress of grievances, the right to associate with others, or perhaps the right to practice a religion, all rights protected by the First Amendment.

An Internet identification/authentication requirement could make it impossible or unduly difficult for a citizen without identification to fulfill legal duties (e.g., file tax returns), obtain benefits available by law, or exercise rights. The REAL ID Act is controversial, in part, for this reason. That Act could make it difficult or impossible for a citizen to enter a federal building without an identification document that qualifies under the Act. The analysis would be different if the user of a particular government activity had no alternative to using an identification-restricted Internet than if use of a restricted Internet were one of several options. For example, if meeting particular Internet identification requirements in order to vote or receive Social Security benefits were the only option, the conclusion might be different than if in-person or postal mail alternatives also existed at the same time.

Even an Internet identification/authentication requirement for a private network operated principally for private purposes, it still could raise concerns about how citizens can carry out basic tasks essential to function in society, many of which remain entangled with government activities or regulations. For example, for many people the health care sector is an amalgam of private and government players and actions. A private requirement for an Internet ID that effectively served as a prerequisite to interfacing with the governmental part of the health care system could raise more intensive civil liberties

[147]The issuance of a driver's license or an automobile license plate has not in the past resulted in the reporting or collection of information about where an individual or automobile goes. However, with the use of electronic toll collection devices, congestion pricing for highways, and other automated automobile information collection systems, the compilation of additional records about driving habits may become both more commonplace and more controversial. One difference between driving and Internet usage is that driving typically takes place in a public space and much Internet usage does not. The extent of privacy rights in public spaces appears to be undergoing some rethinking at present. *United States v. Maynard*, decided in August 2010 by the D.C. Circuit, is one of several recent cases where the issue of the applicability of the Fourth Amendment to tracking an automobile in public by use of a GPS device arose. http://pacer.cadc.uscourts.gov/docs/common/opinions/201008/08-3030-1259298.pdf.

[148]Identification or authentication requirements could offer additional privacy protections (by limiting identity theft) or assist with other objectives (keeping children away from websites aimed at adults). Whatever other benefits might arise, they do not necessarily relate to the cybersecurity matters under discussion here.

concerns. Additionally, if a government Internet ID were adopted by the private sector and became a practical prerequisite to using the Internet even for private activities, the government process might be questioned for its practical effect on citizens, for any discriminatory effect that the process might have in design or in practice, for its privacy consequences, and otherwise.

Depending on the purpose of identification in the narrower context of preventing cyberattacks, it remains open to debate whether a greater use of identification would be successful in either deterring bad actors or finding them after the fact. The prevalence of identity theft suggests that those interested in using the credentials of others for cyberattack purposes might have little difficulty doing so by stealing the elements needed to impersonate another. Further evidence on this point is the ability of malfeasors to establish and control remotely other computers connected to the Internet. A significant percentage of computers connected to the Internet may be part of a botnet. Botnets could be another channel for cyberattacks unaffected by identification requirements for users because the computers on the network have credentials.

In addition to identifying individuals using the Internet, it is also possible that the government could require Internet users to demonstrate proficiency in some important Internet skills pertaining to security or otherwise. Automobile drivers must pass both written tests and road tests that demonstrate knowledge of laws and rules and the ability to drive. Arguably, the same types of prerequisites could apply to some or all Internet usage. The cost and difficulty of managing a proficiency requirement and keeping it up-to-date aside, any proposal would likely be challenged as a limit on the exercise of First Amendment rights. It would likely be seen as the equivalent of requiring a government license to read a newspaper, use a telephone, or mail a postal letter. It might well prove difficult or impossible to show that a proficiency requirement is compatible with the First Amendment. An employer, including the government, may impose training requirements on its workers, but a general-purpose rule applicable to the population at large would be more challenging to justify.[149]

In all of these cases, whether or not an Internet prerequisite violated a constitutional standard, it is nevertheless the case that civil liberties, due process, and privacy would be affected by the rules and procedures that attach to the prerequisite, by the process for issuing the identification, by the amount of personal information collected and maintained, and by the secondary uses for the information. Even with privately issued identification, some or all of these issues would arise, whether or not a public or private network relied on the identification. Laws prohibiting discrimination would presumably apply to private sector identification schemes, for example. The discussion of security clearances, driver's licenses, and flight clearance shows is that we have found ways to balance the rights and interests involved in licensing schemes. That does not mean, however, that acceptable balances will always be found for the next licensing idea.

Licensing computer technicians, programmers, cybersecurity specialists, or other professionals whose activities directly affect cybersecurity on the Internet is another possibility. We have considerable experience in licensing professionals through state or private sector actions, with due process and privacy concerns similar to the licensing activities discussed above. Licensing of Internet professionals would be less controversial than licensing Internet users. Licensing requirements for computer programs is another possibility, and one that would raise more civil liberties concerns because computer programs are intertwined with speech and are protected by the First Amendment. Whether any of these types of licenses would have any significant effect on preventing unlicensed actors or malware from affecting use of the Internet is far from clear, however. For some users, computer maintenance is accomplished by grandchildren and not by professionals. A system that effectively controls computer programs is difficult to envision. As with any licensing system, a criminal who engages in an illegal activity is not likely to care that his or her actions also violate the obligation to obtain a license.

[149]The HIPAA health privacy rule contains a requirement that covered entities train health care workers in privacy. 45 C.F.R. § 164.530(b). This seems unremarkable. However, a training requirement for *patients* would be another matter and considerably more difficult to carry out or justify.

We have not exhausted the identification requirements that might arguably be relevant to preventing cyberattacks. Instead of, or in addition to, licensing individuals to use the Internet, it is possible for government to require identification or licensing of machines that access the Internet. Individual computers or other devices could be required to have and to disclose as a condition of access to the Internet a unique identifier that might be required to be registered in advance or subject to association with particular individuals after the fact. An alternative approach might require that computers accessing the Internet contain specific hardware or software with particular functionality (e.g., virus checking software). Another approach could require regular inspection of Internet devices to determine if they meet specific requirements and are up-to-date.

All of these techniques are used today for automobiles. Each automobile has a Vehicle Identification Number (VIN), a unique serial number used by the automotive industry to identify individual motor vehicles. Automobiles must display unique license plates issued by governments. Most states mandate some form of safety inspection, including an inspection for emissions in some areas.[150] Federal rules require auto manufacturers to install safety equipment, such as airbags. States require proof of insurance before allowing an automobile to be registered.

The federal government likely has the power under the Commerce Clause to regulate computers in similar ways, at least up to the point where the regulations clash with First Amendment interests. Requiring serial numbers for some or most Internet access devices may be possible. For technical reasons, cell phones are identified to the cellular network in order to function so identification seems less of an issue. Internet devices typically use Internet Protocol addresses, which offer a type of identification that may or may not be constant for each device over time. A fixed IP address could serve as an identifier.[151] Registration or identification requirements for other devices would be controversial, of course. In the last 1990s, Intel proposed to produce computer chips with a unique Processor Serial Number (PSN). Objections from the privacy community ("Big Brother Inside") pressured the company into abandoning its plans, and the PSN was dropped.[152] Google released its Chrome browser with a unique identifier with criticism from some privacy advocates, but reports suggest that Google plans to abandon the identifier.[153]

Computers that access the Internet now include many types of devices—including televisions and refrigerators—and requiring some types of inspection seems impractical. The so-called Internet of things (connection of routine objects and devices to the Internet) could result in a vast expansion of items connected to the Internet, including every household item connected to the electrical grid, articles of clothing, body parts, and much else.[154] As a practical matter, it may be unworkable to design and implement a system that mandates and enforces an identification requirement for every Internet device.

One can envision, possibly, a remote inspection of all Internet access devices for security purposes. The government might be able to mandate remote inspection using powers available under the Commerce Clause. A possible precedent is the Communications Assistance for Law Enforcement Act (CALEA), a 1994 law intended to "to make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes, and for other purposes."[155] The law requires telecommunications carriers and manufacturers of telecommunications transmission and switching equipment to ensure that equipment, facilities, and services allow the government to isolate and intercept all wire and electronic communications. Essentially, CALEA forces telecommunications

[150]See generally 42 U.S.C. § 7401 et seq.

[151]It is a contested issue today whether an IP address is a personal identifier. The value of an IP address as a personal identifier is cloudy when there are multiple users for a single computer.

[152]See http://bigbrotherinside.org/; accessed March 17, 2010.

[153]Ryan Whitwam, *Google to Drop Unique IDs from their Chrome Browser*, MaximumPC, available at http://www.maximumpc.com/article/news/google_drop_unique_ids_their_chrome_browser; accessed March 17, 2010.

[154]See, e.g., Commission of the European Communities, *Internet of Things—An Action Plan for Europe* (June 18, 2009) (COM(2009) 278 final), http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf; accessed April 15, 2010.

[155]47 U.S.C. §§ 1001-1010.

carriers to design their networks so as not to impede authorized law enforcement surveillance requests. CALEA does not directly affect consumer devices, but Congress might require consumer devices include the capability of allowing for government access via remote inspection under specified circumstances. Again, the practicalities of implementing and enforcing a remote inspection scheme for all Internet devices seem overwhelming, and the constitutional issues are most difficult.

Enforcement of some or all of these requirements would be additionally challenging because many of these devices enter the country or access the Internet from abroad every day. The government has broad authority to conduct suspicionless border searches of laptops and other electronic storage devices, although it would be hard to do a search of every person and every device.[156] Further, devices in other countries that access networks in the United States present additional compliance and enforcement issues. A uniform international scheme for controlling Internet devices seems a remote possibility at best. The global nature of the Internet and the presence of multiple and potentially overlapping regulatory regimes raise other vexing questions. These include the extent to which any national government could impose or seek to impose requirements on Internet users in other countries or users crossing borders, whether their own citizens or others, that would affect privacy or civil liberties.

It would certainly be argued that any type of regulation that affects the means of speech on the Internet would be akin to regulating speech directly or to licensing printing presses. The regulation would be strongly challenged on First Amendment grounds. The level of judicial scrutiny of an Internet access regulatory scheme would be an important and debatable point. If the government's actions were strictly content neutral, proponents would argue for intermediate scrutiny under which the actions would only have to serve an important or substantial governmental interest unrelated to the suppression of speech and could not burden speech more than is necessary to satisfy that interest. For example, a mandate that personal computers use parts that are readily recyclable would be more likely to be seen as a content neutral regulation.

Yet it is much more likely that a requirement that every computer include a permanent and unerasable keystroke logger would draw very strong objections on First Amendment grounds, with demands for review under the strictest scrutiny standard that would require the government to demonstrate that the regulation furthered an overriding state interest and was drawn with narrow specificity to avoid any unnecessary intrusion on First Amendment rights. A potentially intermediate example might be a requirement that every computer have virus protection software installed and kept up-to-date. Other possible intermediate examples are a requirement that all ISPs examine Internet messages for malware or a mandate that all browsers include specific features.

Regardless of the standard that would apply for constitutional assessment of these requirements, it seem certain that there would be considerable political controversy about any increased role for the federal government in defining prerequisites for access to or use of the Internet. There would likely be strong objections to even the most mild-mannered mandate because it would open the door to stronger and more invasive legislative mandates in the future.

In the absence of a specific identification, licensing, or authentication system, the discussion is quite abstract and unsatisfying. Controls that may have some appeal at a high level of abstraction can face overwhelming practical implementation problems and significant costs in additional to the legal, constitutional, and political objections. The REAL ID law, which is much less sweeping in scope than an Internet licensing scheme would be, started with enough political support to become law, but rapidly became the target of practical, cost, and civil liberties objections. Years after passage, REAL ID languishes with few steps toward implementation actually accomplished.

[156]In 2009, the Department of Homeland Security issued directives on border searches of electronic media. U.S. Customs and Border Protection, *Border Search of Electronic Devices Containing Information* (CBP Directive No. 3340-049, (Aug. 20, 2009), available at http://www.dhs.gov/xlibrary/assets/cbp_directive_3340-049.pdf; accessed March 18, 2010; U.S. Immigration and Customs Enforcement, *Border Search of Electronic Devices* (Directive No. 7-6.1) (Aug. 18, 2009), available at http://www.dhs.gov/xlibrary/assets/ice_border_search_electronic_devices.pdf; accessed March 18, 2009. The Department's Privacy Impact Assessment for these policies is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_laptop.pdf; accessed March 18, 2009.

It is easy to suggest that licensing of users or similar schemes will have benefits, but it another thing to develop a system that will actually work to meet its objectives in the worldwide Internet with untold number of devices connected to it, hundreds of millions of users connecting and disconnecting every day, and rapid technological changes. A licensing system that controlled 99% of users and devices would still leave plenty of opportunities for evasion by those who are motivated, assisted by insiders within the licensing administration, supported by hostile foreign governments, or others.[157] Identity thieves already operate a robust, underground market where stolen information and illegal services are sold and advertised.[158] An expansion of these activities to include information about Internet identities and licensees can be anticipated.

The goals of any licensing system could matter a great deal. We regulate drivers not with the expectation of removing every improper driver or car from the road. The overall regulatory system results in improvements and not perfection. Despite laws, we still have unregistered cars, unlicensed drivers, stolen license plates, and uninsured motorists on the road every day. A system to prevent cyberattacks could have narrower goals of improving privacy and security on the Internet without necessarily expected to avoid everyone who is highly motivated or well-financed. However, to the extent that a licensing system affects the exercise of First Amendment values, narrower goals may make it harder to justify sweeping restrictions.

On the other hand, proponents of regulating Internet devices would argue that licensing and credentialing have the potential to provide *better* privacy and other protections to individuals. Problems for users that result from spam, malware, identity theft, and the like might diminish with the adoption of broad licensing and credentialing systems. Thus, societal costs from computer viruses might decrease if all computers had adequate anti-virus protection. Still, the benefits of licensing Internet users or activities still might not be enough to overcome the constitutional limitations on governmental powers. The issues involved here are obviously multidimensional and cannot be fairly assessed using a single scale.

Regardless of the applicable standard, however, Internet device regulation that restricts or limits speech in any way might well fail to be upheld because of First Amendment concerns. One hypothetical analysis of the constitutionality of licensing printing presses concluded that it is fairly certain licensing would be unconstitutional.

> The difficulty that a licensing regime would have in satisfying First Amendment standards is reflected in the consensus view: "Although it is virtually impossible to find a case that directly so holds, it is fairly clear that any attempt to license a newspaper or magazine would violate the Constitution."[159]

For Internet regulation, the arguments—and perhaps the result—would surely vary depending on the specific type of regulation, the problem that the government sought to address, and the factual justification for the regulation. However, it seems likely that the burden of defending a regulation would be great.

VI. CLOSE

The principal purpose of this closing section is to identify some issues that, for a variety of reasons including lack of space, have not been discussed in any depth. There are no conclusions because meaningful conclusions are not available given the largely abstract review of issues addressed. Proposals for

[157]Any type of activity that creates central information about Internet users has a similar potential to create a resource that could be exploited by identity thieves or others for criminal purposes. The same information could also be used by government for other purposes that may affect privacy or civil liberties interests.

[158]See NextAdvisor, *Inside the Internet's Financial Black Markets—How Identity Thieves Buy and Sell Your Personal Information Online*, http://www.nextadvisor.com/blog/2008/09/16/inside-the-internets-financial-black-markets-%E2%80%93-how-identity-thieves-buy-and-sell-your-personal-information-online/; accessed July 2, 2010.

[159]Stuart Minor Benjamin, *The Logic of Scarcity: Idle Spectrum as a First Amendment Violation,* 52 Duke Law Journal 1, 31 (2002) (footnote omitted), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=310121; accessed March 17, 2010.

preventing cyberattacks can only be fully evaluated for their civil liberties and privacy consequences when the details are available because the specific elements will make a significant difference to the evaluation.

Criminal laws that seek to deter unwanted activities and to punish those who engage in them have not been addressed. A leading example is the Computer Fraud and Abuse Act,[160] which generally protects computers belonging to the federal government or a financial institution or to any computer affecting interstate or foreign commerce. Laws about identity theft are also not addressed in detail, although some of these laws have non-criminal law components. Generally, the tools and techniques of criminal law enforcement have some relevance to cybersecurity (e.g., deterrence), but further analysis is not possible in the available space.

Some federal and state[161] legislation also establishes security standards for computer systems. For example, the 2002 Federal Information Security Management Act (FISMA)[162] directs the head of each federal agency to provide "information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of" agency information or information systems.[163] Laws establishing private sector security requirements are not common, but there are some, including:

- Section 404 of Sarbanes-Oxley[164] requires a publicly owned company's management and the external auditor to report on the adequacy of the company's internal control over financial reporting. Because the financial reporting processes of many companies depend on information technology systems, controls over those systems may fall within the scope of a required assessment of financial risks.
- The Gramm-Leach-Bliley Financial Services Modernization Act includes a few privacy and security provisions. It expresses a policy that each financial institution has an affirmative and continuing obligation to protect the security and confidentiality of nonpublic personal information about customers.[165] Financial services regulatory agencies issued regulations with more detailed standards.[166]
- The Health Insurance Portability and Accountability Act[167] (HIPAA) requires the Secretary of Health and Human Services to issue security rules for covered entities (mostly health care providers and insurers). The rules cover electronic health information.[168] The HIPAA security requirements are more detailed than some comparable rules, rely on industry standards, and give covered entities considerable discretion in application.

Legislation is a crude tool for mandating security, and legislators appear to understand its limitations. Security legislation is typically stated in broad, high-level terms with few details, and the civil liberties and privacy implications of current legislation are of lesser significance here. That could change. Some security laws call for the use of encryption, which can have value in deterring cyberattacks. Encryption can be employed or mandated in a multitude of different ways and, depending on the specifics, can have significant consequences for privacy and civil liberties. A Clinton Administration proposal (Clipper Chip) for mandatory encryption of data communications involving the escrow of encryption keys

[160] 18 U.S.C. § 1030.

[161] See, e.g., the Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 CMR 17.00, available at http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf; accessed March 15, 2010, and the implementing regulations at 201 CMR 17.00, available at http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf, accessed August 30, 2010.

[162] 44 U.S.C § 3541 et seq.

[163] 44 U.S.C. § 3544(a)(1)(A).

[164] 15 U.S.C. § 7262.

[165] 15 U.S.C. § 6801.

[166] See, e.g., 16 C.F.R. Part 314 (Federal Trade Commission).

[167] 42 U.S.C. §1320d-2(d).

[168] 45 C.F.R. Part 160 and Part 164, Subparts A & C.

with the government was highly controversial among civil liberties advocates, Internet users, industry, and others. The proposal was eventually dropped.[169]

Some other subjects that are largely outside the scope here are better training, consumer education, reporting and collaborative efforts,[170] voluntary activities,[171] security breach notification,[172] and polygraph regulation. Most but not all of these activities are less likely to raise privacy or civil liberties concerns.

Emergency powers may allow the President to seize property; organize and control the means of production; seize commodities; assign military forces abroad; institute martial law; seize and control all transportation and communication; regulate the operation of private enterprise; restrict travel; and, in a variety of ways, control the lives of United States citizens.[173] The scope of these powers with respect to the Internet is not immediately clear, but any exercise would raise civil liberties and privacy concerns that cannot be considered here. Recent circulation of a draft legislative proposal by a Senator that would expand the authority of the emergency powers of the President with respect to operation of the Internet attracted considerable controversy. Direct presidential control over the operation of the Internet or the collection of information about Internet activities data raises a large number of issues for individuals, companies, and organizations. The inherent borderlessness of the Internet does nothing to simplify these issues.

Also unexplored here are uses of incentives for those individuals, companies, or other entities that adopt better cyberattack protections. The range of possible incentives is broad, including civil liability that would make software, hardware, service vendors, or users responsible for their failure to provide adequate security measures or their failure to use adequate security measures; civil liability for ISPs who fail to verify the identity of users; and subsidies or tax incentives for "good" behaviors. It is not apparent in the abstract that any of these would necessarily raise significant civil liberties or privacy concerns, although civil liability can raise constitutional questions about violations of the Due Process Clause by grossly excessive or arbitrary punishments.[174] The use of incentives to induce the private sector to adopt protections that the federal government could not impose directly has the potential be controversial.

[169]See, e.g., A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. Pa. L. Rev. 709 (1995).

[170]See, e.g., United States Computer Emergency Readiness Team (US-Cert), http://www.us-cert.gov/; accessed March 17, 2010.

[171]See, e.g., the Critical Infrastructure Information Act, 6 U.S.C. §§ 131-134.

[172]Both the federal government and the states have enacted security breach notification laws, but there is no general federal statute (either preemptive or otherwise) despite much congressional activity over several years.

[173]Harold C. Releya, *National Emergency Powers* (2007) (Congressional Research Service), http://www.fas.org/sgp/crs/natsec/98-505.pdf; accessed April 14, 2010.

[174]See, e.g., *State Farm Mutual Insurance Co. v. Campbell*, 538 U.S. 408 (2003).