CISAC Report

Civil Liberties and Security in Cyberspace

Ekaterina A. Drozdova

August 2000

Ekaterina A. Drozdova, B.A., 1996, M.A., 1998, Stanford University, is a researcher at the Center for International Security and Cooperation and an affiliate at the Consortium for Research on Information Security and Policy at Stanford University. Her background includes information technology consulting in the Silicon Valley, and she is pursuing a Ph.D. at New York University.

Abstract

Societies are becoming more dependent on computer networks and therefore more vulnerable to cyber crime and terrorism. Measures to protect information systems are receiving increasing attention as the threat of attack grows and the nature of that threat is better understood. The primary purpose of this article is to determine what legal standards should govern the use of such measures and what nontechnical constraints are likely to be placed, or should be placed, on them. The article demonstrates that policing of computer networks poses a real threat to privacy, protection against self-incrimination and unwarranted searches and seizures, and the right to due process of law. Technological realities and the differences in national values and rules concerning the intrusiveness of law enforcement, protection of citizens' rights, and international cooperation can complicate the observance of these rights and allow misuse of systems set up for preventing, tracking, or punishing cyber crime. Another purpose of this article is to show that while technologies of crime and punishment are undergoing a rapid and profound evolution, the legal and normative principles discussed here will endure, because they are independent of specific technology. As such, they can provide a framework for building a global infrastructure and policy environment that can balance the needs for crime-free business, government, and personal communications, with the protection of property, privacy, and civil liberties. The article concludes that ensuring civil liberties in the course of legal and technological cooperation against cyber attacks is essential.

Contents

Civil Liberties and Security in Cyberspace

Introduction

Societies are becoming more dependent on computer networks, and therefore more vulnerable to cyber crime and terrorism.[1] Measures to protect information systems have received increasing attention as the threat of attacks grows and the nature of that threat is better understood. Among these measures are sophisticated technologies for monitoring computer networks and users, detecting intrusion, identifying and tracing intruders, and preserving and analyzing evidence.[2] What legal standards should govern the use of these measures? What nontechnical constraints are likely to be placed, or should be placed, on them? What importance should be assigned to these constraints in designing and implementing technologically robust solutions and international agreements to facilitate law enforcement?

Specific answers to these questions will ultimately be determined by evaluating the specific methods or agreements proposed.[3] But certain legal principles are broadly applicable, including the right to privacy, the protections against self-incrimination and unwarranted searches and seizures, and the right to due process of law. These civil liberties are supported in international law and guaranteed in varying forms by the national laws and institutions of many countries. An international regime against cyber crime and terrorism must operate within the constraints of these principles, as defined by the legal frameworks of its States Parties.

There is often a tension between protecting civil liberties and enforcing laws to maintain public safety and order. States resolve this tension differently. Agreeing upon a common global level of protection of citizens' rights is problematic due to international variance in normative standards, legal practices, and political objectives. An international common denominator could reduce the level of protections currently afforded in some states to the level of authoritarian states. In the interest of promoting international cooperation and a timely response to the growing threat of cyber a ttacks, seeking measures other than agreement on a specific level of protection is more likely to succeed.

However, the differences in domestic values and rules may allow misuse of systems set up for preventing, tracking, or punishing cyber crime. Diversion of technologies for illegitimate purposes—such as unwarranted surveillance—is a real threat, especially in countries that give little weight to civil liberty principles constraining such activities. Countries may be tempted to circumvent legal constraints, moreover, when faced with a national security threat. Systems set up for international cooperation would also introduce new cyber vulnerabilities, as they may be "hacked" or "cracked" and misused by criminals or unauthorized persons. States should address these dangers in the course of developing forms of international cooperation that extend to sharing information and coordinating technology.

This article starts out with a discussion of basic protective and reactive approaches to security in cyberspace in Part I, then considers the legal principles that apply to security measures in Parts II and III. Issues concerning search, seizure, and due process of law apply primarily to criminal law enforcement. However, threats to privacy extend beyond law enforcement into commercial and all other spheres of social life. Privacy is discussed in Part II in this broader context, including the value, law, and status of privacy protection; threats to privacy in cyberspace; and protection modes and constraints on measures against cyber crime. In Part III, the discussion turns to criminal law and constraints on police behavior in the course of investigations.

Part I. Protective and Reactive Approaches to Security in Cyberspace

The world's use of and dependence on international computer networks fosters transnational computer crime. Sophisticated criminals are able to operate from a distance, route their malicious communications through other countries, and cover up or confuse the origins of their attacks. To respond to attacks in a timely and effective manner, system operators need to monitor user behavior and detect intrusions in real time. To identify suspects and launch investigations once a crime is detected, large-scale screening, tracing, and analysis of electronic evidence may be required. Such realities not only complicate law-enforcement activities, but also require new methods for investigation and prosecution, including technological and legal arrangements for international cooperation.

Such methods demand substantial commitments of technological, economic, and human resources. States, as well as commercial and other public and private entities, face difficult trade-offs in allocating resources to fight cyber crime. Increased network security and investigative measures may come at the expense of network performance, privacy, and users' desire for anonymity. States may also find their domestic laws, national security objectives, and political or economic priorities at odds with the conditions required for effective international cooperation. Restrictions on cross-border flows of information imposed for policing purposes may impede electronic commerce and other transactions.

There are two basic approaches to security in cyberspace: a protective one and a reactive one.[4] Each is constrained in different ways. The protective approach aims to deter criminals through measures that deny access or make a potential target less vulnerable to an attack. This approach is focused on defense. It involves designing more secure Internet protocols, introducing trusted routers and virtual private networks, and utilizing firewalls, encryption, automated

intrusion detection systems, and other security measures.[5] The reactive approach, instead, seeks to deter the threat through effective investigation, prosecution, and punishment.[6]

Both approaches involve monitoring and diagnosing abnormal and unauthorized activity. The protective approach favors automation as well as oversight and decision-making by computer security experts. The reactive one depends more heavily on the participation of law enforcement and requires end-user-oriented (rather than anonymous) traffic analysis, which may be as intrusive as scanning attached files, keyword searches, and content filtering for signs of potential breaches of criminal law. Real-time investigative capabilities may extend to creating embedded data collection infrastructures and modifying hardware and/or software to provide for confidential law-enforcement access to business, governmental, and private computer networks.[7]

The two approaches can be complementary. Their relative weights depend on the preferences and capabilities of implementing parties. The protective approach is less intrusive, and it is likely to bring about greater cyber security to its users. However, there are significant obstacles to achieving adequate security.[8] The reactive approach is inherently more intrusive and more threatening to civil liberties. Nonetheless, it may be more effective in cases of inadequate defense and in safeguarding users who are unable to afford, or unwilling to implement, sufficient protective measures.

Part II. Privacy and Data Protection

Among the issues considered here, privacy in cyberspace is the most controversial and publicly debated. Privacy concerns not only the context of law enforcement, but also day-to-day business practices and an individual's ability to control the treatment of personal data made available in electronic format or accumulated during Internet use. Commercial exploitation of personal data without consent is already leading to enhanced legal protections for privacy. The enforcement of such protections will raise the issue of the desirability of using protective versus reactive methods, leading to discussions of what can be done to ensure that any method used will protect privacy interests against unwanted intrusion.

1. The Value, Law, and Status of Privacy Protection

Privacy is not an absolute, well-defined, or uniformly protected value. Individuals, organizations, and societies have traditionally sacrificed some privacy in exchange for greater security, economic gain, or convenience. Trade-offs between privacy and intrusion (by government, industry, etc.) reflect the different historical and social contexts in which they were made. The norm of privacy is linked to an individual's independence, dignity, and integrity.

Protection of privacy has evolved historically through international and domestic law. Privacy is a fundamental human right recognized by the 1948 *Universal Declaration of Human Rights* and many other international and regional instruments and treaties.[9] The *Universal Declaration* proclaims that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation," and "every-

one has the right to the protection of the law against such interference or attacks."[10] It also states that "everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[11] These provisions create the basic international law framework for the right to privacy, which extends to cyberspace.[12]

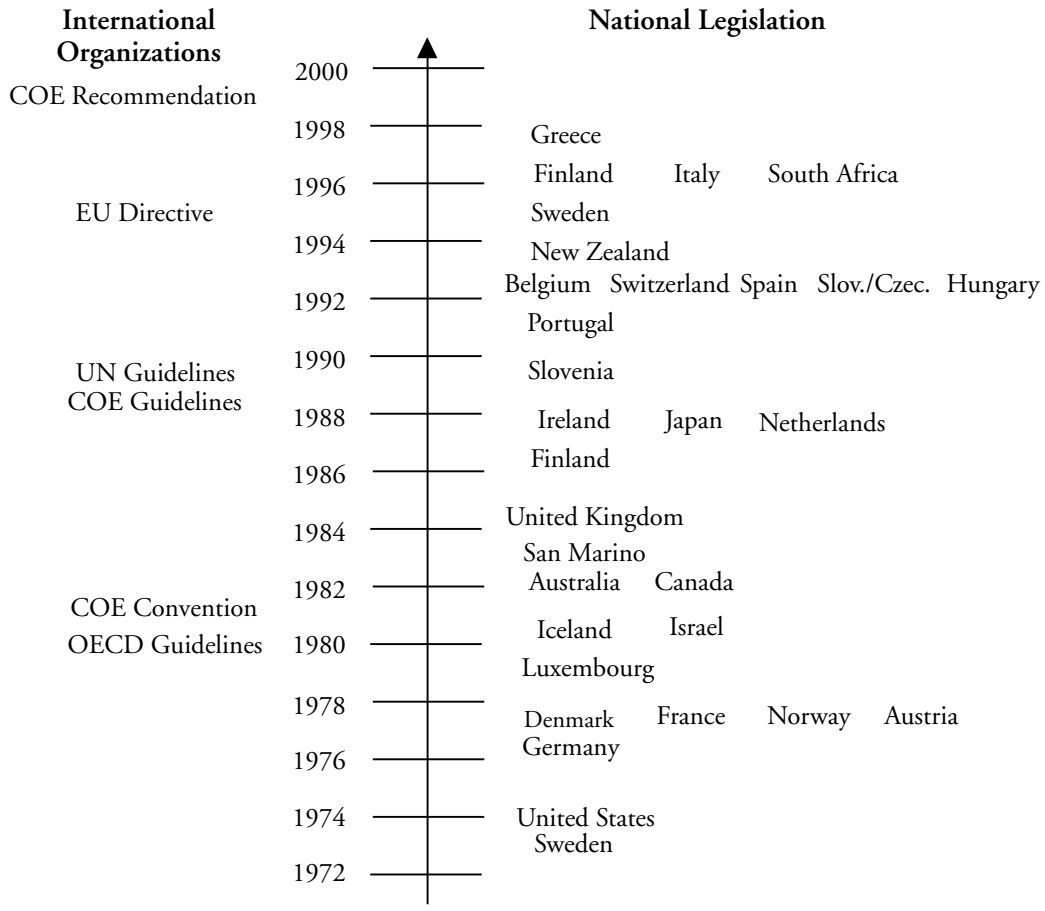
On the national level, privacy is protected through a combination of constitutional and legislative instruments and self-regulation. Nearly every country in the world recognizes a constitutional right to privacy, including at least the rights to inviolability of home and secrecy of communications. Some recently written constitutions, such as those of South Africa and Hungary, contain rights to access and control of one's personal information. In countries where the right to privacy is not explicitly guaranteed by the constitution—the United States, Ireland, and India, for example—this right has been established through other legal provisions or judicial rulings.[13] In the United States, for example, a strong privacy interest derives from the constitutional guarantees of security of person, house, property, and papers; protection against unlawful and unreasonable searches and seizures; the right against self-incrimination; and the freedom of speech and assembly.[14]

The advent of information technology provided a new context in which to consider privacy and a new legal impetus for the protection of personal data. The first modern legislation on collecting and handling personal data emerged in the early 1970s in Sweden (1973) and the United States (1974).[15] The Organization for Economic Cooperation and Development (OECD) was the first international organization to issue a policy, "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," adopted in 1980. The OECD's policy applies to personal data, whether in the public or private sectors, that pose a danger to privacy and individual liberties because of their nature or the manner in which they are processed and used.[16]

Development of international standards continued in the 1980s and 1990s. The Council of Europe (COE) adopted a "Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data" (1981) and "Guidelines on the Use of Computerized Personal Data Flow" (1989).[17] The United Nations (UN) produced "Guidelines for the Regulation of Computerized Personal Data Files" (1989).[18] These documents establish principles of minimum privacy guarantees for personal information at all stages of its collection, storage, and dissemination by other parties. They also create new rights for "data subjects"—those whose data are collected and manipulated by government agencies, businesses, etc.—requiring that accurate and up-to-date personal information must be obtained fairly and lawfully; used only for the original, intended purpose; and destroyed after the purpose is achieved. Data subjects are granted the right to access and amend information about them.

The 1995 European Union (EU) Data Protection Directive established a regulatory framework for free movement of personal data, while allowing individual EU countries to exercise their unique approaches to implementation. Data subjects are guaranteed the right to know where the data originated, the right to have inaccurate data corrected, the right of appeal in the case of unlawful processing, and the right to deny permission to use data under certain circumstances.[19] The 1999 COE Recommendation provides guidelines for the protection of privacy on the Internet.[20] While the COE and UN guidelines are recommendations, the EU directives are binding, as member states must adopt them into their domestic law.

Development of Law on Privacy Protection in Cyberspace



Source: Updated from Ulrich Sieber, "Legal Aspects of Computer-Related Crime in the Information Society" (1998).

Currently, nearly fifty countries and jurisdictions have enacted or are in the process of enacting privacy laws designed to ensure compatibility with international standards, to address past government abuses, and/or to promote electronic commerce.[21]

2. Threats to Privacy in Cyberspace

Privacy is threatened by businesses and other entities that collect and manipulate personal data, criminals who steal such data or stalk people over the Internet, and governments that pursue surveillance or allow intrusive law-enforcement practices. Sophisticated electronic capabilities to collect, analyze, manipulate, and disseminate information, as well as to enable tracking, surveillance, and interference with communications, create unprecedented challenges to privacy. Such technologies are becoming more effective, available, and affordable internationally. At the same time, globalization and growing dependence on information technology in all

spheres of society have led to a dramatic increase in the level of electronically compiled and transmitted personal data. The differences in domestic legal standards and practices also endanger private data transmitted over international networks. Even if one state has robust privacy laws, it cannot currently guarantee equivalent levels of protection once the data flow beyond its borders. Gaps in protection will be created to the extent that laws and law enforcement fail to keep up with technological capabilities and international discrepancies undermine domestic levels of protection.

Market forces tend to undervalue privacy. The U.S. Federal Trade Commission found that privacy policies, posted on many commercial web sites, did not provide sufficient protection for online consumers.[22] Businesses track online behavior, sell personal information, and misuse personal profiles built on the basis of financial, medical, and other sensitive information.[23] Employers' intrusion into electronic communications of employees in the workplace is another area of concern. Privacy protection is often subordinated to property rights of employers as the providers of their employees' electronic communication services. In the United States, for example, legislation prohibits employers from eavesdropping on the private telephone conversations of their employees at work, but no similar protection extends to electronic mail communications.[24]

Criminals take advantage of deficiencies in the protection of sensitive information transmitted and accumulated in electronic form. Identity theft is among the fastest-growing cyber crimes; in the United States alone, it has increased more than 300%, from 7,868 cases in 1997 to 30,115 in 1999. Pedophiles entice victims in Internet chat rooms and use electronic communications to arrange actual meetings. Spurned suitors forge vindictive emails inviting rape.[25] Stalkers identify victims on the Internet and threaten them physically.[26]

The spread and growing severity of cyber crime[27] require greater security and better law enforcement. Where security and policing methods are intrusive, achieving these objectives may necessitate some limitations of privacy. Should governments treat Internet communications like a phone call, paper correspondence, or a discussion in a public place? Responses to this question determine the extent of permissible infringements, as well as the specific rules governing law-enforcement functions. Responses vary among states. Even the relatively strong *European Convention on Human Rights* makes exceptions to the exercise of the right to privacy "in accordance with the law," when it is "necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[28] Although the burden of proof to establish the need for this exception rests with the potential intruder, the scope of the exception is very broad. Many national laws have similar provisions. Such breadth can lead to abuse if police attempt to assume excessive powers or governments pursue unlawful surveillance.

Caspar Bowden of the United Kingdom's Foundation for Information Policy Research warned about the implications of improving detection, prosecution, and prevention of cyber crime at the expense of privacy:

> There are now traffic-analysis tools commercially available to law enforcement which can take telephone number logs in machine-readable form and draw "friendship trees," which show the grouping and relationships between parties

> calling each other in time, and can match patterns of association automatically using sophisticated artificial intelligence programming.
>
> There is enormous potential for law enforcement in increased use of traffic analysis, but there are a number of fundamental distinctions between traffic analysis of telephony, and Internet traffic—especially in a fully wired Information Society. The Internet Protocol ("IP") abolishes any meaningful distinction between domestic and foreign communications intelligence. A well-funded national communications intelligence agency, which already captures large quantities of both traffic and content data and has the organization to process it and integrate it effectively with other forms of intelligence gathering, presents an enormous temptation to government simply to leverage that capability for wider domestic coverage.
>
> Intelligence-integrated traffic analysis is phenomenally corrosive of civil liberties. If government was in a position to know which websites you visit, what you buy online, the e-mail addresses of those who e-mail you and those you have e-mailed, and analyze and archive that information without hindrance, there is potential for an unprecedentedly serious abuse of power. [29]

The threat of systematic government intrusion into electronic communications has already received attention around the world. Russia's Federal Security Bureau (FSB) is implementing an Internet surveillance system that requires all Internet service providers (ISPs) to enable routine FSB monitoring of communications.[30] Russian human rights' advocates report that many of the country's 350 ISPs have already been forced to comply, endangering secrecy of communications and other civil liberties of users and persons whose sensitive information may be transmitted over the Internet.[31] The U.S. Federal Bureau of Investigation (FBI) is using a similar wiretapping system with specialized software that can scan millions of emails a second. When deployed, the system must be connected directly into ISPs' computer networks, which gives the government potential access to all customers' digital communications. Typical Internet wiretaps last about 45 days, after which the FBI removes the equipment. Critics contend that the system is open to abuse, raising dire privacy and security concerns.[32]

Threatening surveillance has also taken place on the international scale. The United States, Great Britain, Canada, Australia, and New Zealand allegedly engage in selective multinational screening of telephone, fax, satellite, and Internet communications for foreign intelligence purposes. This system, known as Echelon, supposedly links computers around the world to capture large volumes of information and to sort and analyze it through sophisticated keyword searches and artificial intelligence aids. The information collected is compiled and routed according to requests of the participating parties.[33] Allegations of unlawful surveillance and violation of privacy, in the United States and abroad, have been raised in regard to this system.[34]

While a system for advanced monitoring, searching, tracking, and analyzing of communications may be very helpful against cyber crime and terrorism, it would also provide participating governments, especially authoritarian governments or agencies with little accountability, tools to violate civil liberties domestically and abroad. Correspondence of innocent people can be intercepted, and people can be repressed as a result. Systems set up for international policing

of cyberspace could also be hacked or misused by an insider to undermine a participating government or to damage the interests of a state. The technology and know-how, which will be developed and provided to less technologically advanced countries in the course of international cooperation, could be used to enhance domestic surveillance and suppression by governments that disregard human rights.

These threats exist now, and they are likely to expand in the future. While today reading and analyzing communications of millions of Internet users is difficult and resource intensive, it will likely become easier as advanced computer networking pervades public and private lives and methods for intercepting and analyzing information become more sophisticated, widespread, and affordable. Integrating attributed personal data from different systems could make comprehensive, detailed profiles available for retrieval, manipulation, and abuse. Abuses by the private sector may range from inundation with unsolicited targeted advertisement to various forms of covert discrimination, such as denial of employment or medical services on the basis of prior knowledge of health conditions. Such conglomerations of data would be vulnerable to identity theft and other cyber crimes. As for possible government abuses, the totalitarian regimes of the twentieth century—with ubiquitous informers, government controls over all spheres of society, and egregious violations of human rights—should serve as a reminder and a warning.

3. Privacy Protection Modes and Constraints on Measures against Cyber Crime

Several models of data protection have emerged—public enforcement, sector-specific regulation, and self-regulation—reflecting different legal approaches to privacy. Methods are also used in combination. The EU, Australia, Hong Kong, New Zealand, Canada, and many countries of Central and Eastern Europe have adopted the first model, in which a public official (a commissioner, ombudsman, or registrar) enforces a comprehensive data-protection law. This official monitors compliance, conducts investigations into alleged violations, and requests legal action in case of a breach. The official is also typically responsible for public education and international interaction with respect to data protection and transfer. Alternatively, the United States has adopted sector-specific rules (covering video rental records or financial privacy, for example) rather than comprehensive laws. Singapore, Australia, and the United States also promote a form of self-regulation, whereby companies and industries establish codes of practice. Enforcement in these cases typically proceeds through private, as opposed to government, actions.[35]

Industry self-regulation will be insufficient so long as market forces undervalue privacy in cyberspace. Sector-specific rules may be sufficient, but protection may also fail if data are transferred or sold to entities in sectors with lower standards. Public enforcement has provided higher levels of privacy protection. However, it is vulnerable to the same problem: transmittal of sensitive data beyond the networks of the country with strong legal enforcement of privacy is likely to result in decreased levels of protection.

The countries of the European Union protect personal data more rigorously than the United States, and this discrepancy has fueled an international controversy. The 1995 EU Data Protection Directive requires that personal data may be collected only for specific, explicit, and legitimate purposes. Only relevant, accurate, and up-to-date data may be held. Member states of the EU are obliged to maintain these standards when exporting or processing information pertain-

ing to EU citizens abroad, or they must halt the movement of data in the absence of "adequate" (equivalent) protections. The United States has no similar statute, and the EU considers the U.S. industry's self-regulating approach inadequate.[36] To mitigate the ensuing limitations on transborder flow of data, a "safe harbor" agreement was reached that will enable some U.S. companies to collect data about EU citizens, if the companies demonstrate safeguards that meet European approval. These companies will be required to give notice to European citizens about how their information is to be gathered and used, allow them to withhold data, and offer them reasonable access to their own records.[37] Such partial resolution toward greater privacy standards is encouraging. The dispute, nonetheless, is alarming. If the most advanced democracies disagree on adequate protection of privacy, agreement and observance of this norm can hardly be expected in a global setting that includes less democratic and less accountable governments.

From the standpoint of security against cyber crime, the 1995 EU Data Protection Directive does not necessarily impede law enforcement activities and international cooperation in cyberspace. The directive fully applies to the first two Pillars of the Treaty of the European Union: (I) the European Community, which covers democratization of the institutions, citizenship, and economic and monetary union, and (II) the common foreign and security policy. It is the third Pillar (III), however, that addresses the issues of justice and home affairs, including police and judicial cooperation to combat drug trafficking, international fraud, and other crimes.[38] The scope of the directive does not cover law-enforcement procedures. This means that there are opportunities for international cooperation against cyber crime and also threats to privacy in the course of such cooperation. Privacy-related law-enforcement practices are being examined by the European Commission and may be subject to more intense scrutiny in the near future.[39]

To compensate for the uneven or insufficient privacy protections in commercial and public settings, and to reduce their vulnerability to cyber crime, public and private organizations and individuals can adopt existing protective measures. Encryption, anonymous remailers, proxy servers, and other technologies[40] are commercially available. Many of these technologies offer protection against cyber crime coupled with enhancement of privacy. These include more secure network protocols and routers, encryption, firewalls, virtual private networks, secure anonymous communications, challenge-response systems, and security management applications. IP version 6 (IPv6), the next generation of Internet Protocols, allows routers along delivery paths to record addresses of previous destinations in the header of the message. This feature would enable the searching and tracing of suspect messages without prior disclosure of their content or author, thus protecting the identity of the sender and the secrecy of communications.[41]

Information exchanges among computer security staff regarding modes of penetration and attack, suspected crimes, early warnings, and anomalies in computer operation can facilitate prevention and timely incident response. Incentives for greater protection can be created by placing more legal or financial responsibility on the owners and principal operators of computers and networks—be they businesses, organizations, or individuals. Stronger cyber security would deter some cyber crimes but not all. Moreover, technologically and economically advanced nations can enhance cyber security and privacy by making protective technologies available and affordable on the market, but citizens of less advanced countries may not be able to afford these alternatives.

The United States has proposed creating an international cyber police.[42] Such a system would need to be worldwide in both coverage and participation, and it would enable police to conduct rapid investigations over global communication networks. Although it is unclear what the United States intends beyond voluntary coordination, the European Union has already reacted unfavorably, citing privacy implications.[43] A full-fledged international police force would exemplify an extreme of the reactive approach. Its mere existence would pose concerns about the security and integrity of information it acquires, the reliability of its operators and users, the trustworthiness of international participants, and the possibility of its use for unlawful purposes (by member states, police officials, or criminals and terrorists).

Some forms of international cooperation will nonetheless be required to combat transnational cyber crime. With this goal, a group of researchers at Stanford University has prepared a draft "International Convention to Enhance Protection from Cyber Crime and Terrorism" (the "Draft Convention").[44] It combines protective and reactive measures with provisions for protecting privacy and other civil liberties. It calls upon state parties to establish cyber offenses as crimes under domestic law. Thereafter, investigations, extraditions, prosecutions, mutual legal assistance, and judicial proceedings are to be carried out in accordance with the laws of the States Parties.[45] Intrusive international law enforcement procedures may be allowed, but only in accordance with domestic legal standards and mutual legal assistance treaties. The Draft Convention explicitly states that it shall not be construed to require an infringement of the privacy or other human rights of any person as defined by the laws of the requested state. To ensure systematic monitoring and implementation of this provision, the Draft Convention proposes to create a group of experts dedicated to the protection of privacy and other human rights.[46]

In some cases, especially those involving international exchanges of sensitive information and monitoring of networks by law enforcement, special procedural safeguards for privacy may also be necessary. Domestic and international exchanges among technology and law enforcement experts of data regarding past and suspected computer crimes, anomalies in computer operation, network vulnerabilities, modes of penetration, alerts, and warnings, fall into this category. Such data—no doubt relevant and probably crucial for effective response to cyber crime—are likely to contain sensitive security and personal information, including aliases, identities, and passwords. Information about the citizens of one country may be provided to entities in other countries, whose privacy laws may not afford the same level of protection. An agreed-upon privacy policy—be that deference to domestic practices or a reasonable minimum level of protection—acceptable to parties in the international exchange would help guard privacy during such information exchanges.

Businesses, such as information infrastructure or service providers, may also be called upon to reveal sensitive information concerning attacks, vulnerabilities, and personnel as part of investigative or preventive measures. Even though the support of commercial entities is often required, they are reluctant to share sensitive security-related information with the government.[47] Disclosure and attribution of such information may disrupt business objectives, cause economic losses, trigger unwelcome legal proceedings, and threaten individual employees. Employees are typically subject to loss of their jobs for unauthorized revelation of suspected criminal activity. Businesses should be concerned about the personal safety and privacy of employees when dealing with a suspected crime or perpetrator, or they should be compelled to

have such concern by legislation or economic incentives. Preserving the identity of institutions and their employees in tracking, tracing, and investigating crime against them may be a crucial vehicle for building the necessary public-private sector cooperation in this area.

Automation is particularly important to enhance both security and privacy. The use of automated and semi-automated tools facilitates near-real-time detection of security breaches, tracing to origin of attack, scalability of action (detecting intrusions among large volumes of data involved in normal network operations and responding to intrusions that may hop across international networks), and ultimately increased efficiency and effectiveness. Automation in searching, tracing, and tracking preserves the anonymity and privacy of innocent individuals whose messages may be subjected to search in the course of an investigation. The protection of privacy ultimately relies on a combination of automated and other protective technologies as well as laws that constrain law enforcement. Where law-enforcement methods are intrusive and automation is not available or fully reliable, legal constraints are especially necessary.

Part III. Criminal Law and Constraints on Police Behavior

Constraints on police behavior in cyberspace have received far less public attention than privacy problems. This is partly because they are narrowly focused on criminal investigation—while privacy interests span personal, commercial, and government realms—and partly because what is necessary and legally permissible in cyber-related investigation and prosecution procedures is still being determined.

The protections against self-incrimination and unwarranted searches and seizures and the rights to due process of law apply in cyberspace as anywhere else. However, technological realities can complicate the observance of these rights. Pursuit of crimes committed over international computer networks is also complicated by the differences in domestic procedures and the absence of a system of international criminal law.

1. Search and Seizure

In most legal systems, the main sources of law that govern searches, seizures, and other modes of police behavior are constitutions, legislation, and case law. Investigation and seizure of evidence in democratic states are governed by laws that protect citizens vis-à-vis the state and its law-enforcement powers. In many states, searches and seizures must be legally authorized. The competent authority to issue a search warrant is usually a judge or a magistrate. However, in China, Italy, and South Africa this authority can be vested in a member of the prosecution service or the police.[48] Searches and seizures must also be carried out with due respect for civil liberties. In the United States, for example, this principle is protected by the Fourth Amendment to the Constitution, which states that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[49]

The concept of "search" can be defined broadly to include not only the search of a place or person, but also other invasions of privacy such as wiretapping. Searches may be held upon consent of the individual to be searched, as long as specific consent criteria are satisfied. Many national legal systems prohibit the admission in criminal prosecutions of evidence obtained unlawfully. However, the rationale for and the extent of exclusion vary. U.S. courts exclude evidence obtained as a result of unlawful police conduct. Argentina, Canada, England, France, Germany, Russia, and South Africa determine the admissibility of evidence depending on the fairness of the proceedings. Courts in France and Germany enjoy some discretion depending on the rules violated in obtaining the evidence. China and Israel consider only the reliability of evidence.[50]

Such differences make it difficult for states to agree on a common international standard of police behavior. Sovereignty issues, addressed by Drew Arena of the U.S. Department of Justice, complicate international investigations:

> [T]he basic problem is presented by a nation's perception of its national sovereignty. To what extent must it assert its sovereignty to protect its citizens and enforce its criminal law? To what degree is it prepared to compromise that sovereignty for the sake of (reciprocal) international cooperation? For example, could the U.S. enter into an agreement which provided that foreign officials, armed with legal process in their country would be searching data bases in the U.S. from abroad, unless we were satisfied that the Fourth Amendment's probable cause requirements had been met? How would we reconcile such an agreement with the rigorous standards to be met for domestic law enforcement to obtain access and disclosure of electronically stored data in our criminal law (Title 18 Section 2703)? How would we avoid treating it as an unauthorized access under Title 18 Section 1030? On a practical level, how would we know that a foreign law enforcement access to a data base was not a hacker's attack? [51]

These challenges do not preclude international cooperation. For example, the proposed draft "International Convention to Enhance Protection from Cyber Crime and Terrorism" explicitly recognizes the priority of national laws. It also helps clarify which rules should apply in transnational investigations, extraditions, and judicial proceedings by establishing priority in jurisdiction and venues for cooperation and mutual legal assistance. When a requested state is asked to assist—in identifying and tracing cyber attacks, executing searches and seizures, locating or identifying persons, examining objects and sites, securing and exchanging information and evidentiary items, etc., by electronic and other means—rules of this requested state will apply.[52] Moreover, the Draft Convention requires that requests be made upon a reasonable belief that an offense has occurred and that evidence is contained in cyber systems located within the territory of a requested state. The requested state will then undertake the preservation of such data but will not be compelled to release it unless presented by the requesting state with adequate cause for release.[53]

The technology of searching and seizing electronic evidence presents challenges of a different nature.[54] Computer hardware and disks may need to be obtained as evidence. Surveillance of network and user behavior may also be necessary, along with searches and forensic investiga-

tion of email messages, user files, customer or employee records, and encryption keys. Surveillance may be needed before, during, and after an incident to determine whether a crime has occurred and how to respond. Available methods range from wiretaps on phone calls and Internet communications to various tagging and tracing techniques (user, chip or software ID, network IP address, location detector, etc.), room bugs, and cameras (possibly tied into face recognition systems). Suspect computers can be remotely monitored by capturing keystrokes, passwords, email messages, attachments, and desktop files. Police may also monitor the "computer underground"—skilled but not directly suspected hacker communities—to gain insights into the nature of the attack and possible attackers.[55]

National laws often contain exceptions to balance protective civil liberty principles with the need to maintain public safety and order. These exceptions can help guide the police to determine the legal boundaries in computer searches and seizures in the absence or in early stages of development of cyber laws. Exceptions can also create opportunities for abuse of law-enforcement powers. Many countries still lack specific computer-related laws and procedures, so they refer to general criminal laws in cyber cases. Alternatively, the U.S. Department of Justice has published, and regularly updates, specific "Federal Guidelines for Searching and Seizing Computers." The guidelines address the Supreme Court's strong preference for warrants in searches and seizures, as well as the limited exceptions to Fourth Amendment requirements. As such, the guidelines provide a suitable background for the discussion of the exceptions, drawing upon technical and international realities to evaluate their application in cyberspace. The exceptions to the warrant requirement include:[56]

(a) Lack of reasonable expectation of privacy. The Supreme Court defines a "search" as an intrusion by police into an area where individuals have a "reasonable expectation of privacy."[57] Generally, no one has an expectation of privacy as to something that can be observed by the public.[58]

Whether the Internet is a public space or a private space, where search warrants are usually required,[59] is still legally unsettled. Determinations have been made in specific cases, depending on the type of electronic transmission sent and the recipient of the transmission.[60] For example, real-time Internet conversations observed by an agent in a chat room lacked Fourth Amendment protection, as the defendant did not have a reasonable expectation of privacy vis-à-vis other participants in chat room discussions.[61] However, a determination regarding the public or private nature of the Internet cannot be made categorically, because the Internet can be used in different ways, with more or less reasonable or justifiable expectations of privacy.

(b) Informants and undercover agents. The use of informants or undercover agents to aid investigation is generally permitted by law.

In accessing electronic bulletin boards and chat rooms, undercover agents are not required to identify themselves as such but must confine their activities to those authorized for other users.[62] The sender of an email message, like the sender of a letter, runs the risk that he is sending that message to an undercover agent. A government informant or undercover agent may capture and record the contents of electronic conversations to which he is a party, just as an agent may record a conversation in which he is a participant.[63] However, the inexperience of police in Internet-related cases may lead them to draw erroneous conclusions about apparently

incriminating information. If an agent is to exercise law-enforcement powers as a result of undercover activities, he must still demonstrate probable cause and fulfill other requirements.[64]

(c) Plain view doctrine. Evidence of a crime may be seized without a warrant if a police officer is in a lawful position to observe such evidence and its incriminating character is immediately apparent. This applies to situations where police enhance their ability to observe by commonly used means, such as binoculars or a flashlight. In such cases, there is no reasonable expectation of privacy, and police observation is not considered a search. However, creating plain view by means of "moving" or "disturbing" items or using sophisticated electronic devices must be justified by probable cause.[65]

If agents with a warrant to search a computer for evidence of narcotics trafficking observe a list of passwords taped to the computer monitor, the list may also be seized.[66] The application of enhanced plain view to cyberspace is less clear. Some applications may depend on what is considered public or private space on the Internet, because government investigators can lawfully be in a public space without a warrant and they may observe illegal activity in plain view.[67] Discretion in using this exception is necessary, however, as computer and multimedia communications technologies advance very rapidly, making it difficult to distinguish what electronic devices are sophisticated and uncommon enough to require probable cause.

(d) Wiretaps. Wiretaps may be performed by federal agents only for certain, specific crimes, upon application to a judge through high-level officials at the Department of Justice. State agents must gain approval of high-level state law-enforcement officials. Approval may be waived in case of emergencies that involve "conspiratorial activities threatening to national security," "conspiratorial activities characteristic of organized crime," and "immediate danger of death or serious bodily injury to any person."[68]

It may be difficult to detect and determine, in a timely manner, whether an Internet surfer is engaged in conspiratorial activity rather than electronic commerce or mere chatting. "Trawling warrants" have been proposed to assist such detection and determination. A required "trawling warrant" would specify a logical circuit or domain of capture, rather than allowing the capture of all messages on a topic or from or to a person. Signals from this specified domain would be automatically selected by computer against a "certificate" issued by a Secretary of State (or similar authority) that contains the description of the target subject matter suitable for machine searching. To limit abuse, the issuer would need to guarantee that noncertified intercepted material would not be looked at, read, or listened to by any person. Exemptions for extended interceptions for national security reasons could be given on a case-by-case basis only.[69] However, facing the difficulty of such narrow, targeted wiretapping of speedy and possibly disguised electronic communications, law enforcement may be and has been tempted to utilize large-scale, indiscriminate, and intrusive surveillance instead.[70]

(e) Exigent circumstances. "When destruction of evidence is imminent, a warrantless seizure of that evidence is justified if there is probable cause to believe that the item seized constitutes evidence of criminal activity."[71] Investigators must consider the degree of urgency, the time necessary to obtain a warrant, whether the evidence is about to be removed or destroyed, the destructibility of evidence, the possibility of danger, and whether suspects are aware that they are being observed or followed. This exception also justifies warrantless searches if the circum-

stances would cause a reasonable person to believe that an immediate search is necessary. Such circumstances involve the need for immediate aid,[72] escape of a suspect, or another emergency or frustration of legitimate law-enforcement objectives.[73] A warrantless seizure under exigent circumstances does not automatically justify a warrantless search.[74]

If police lawfully observe a suspect's computer screen displaying evidence of crime and then see the suspect modifying or deleting files containing such evidence, police may justifiably download them or seize the computer. However, the application of exigent circumstances to searching and seizing data from two or more computers on a wide-area network, used by individuals other than suspects, is less clear and should be determined upon a careful examination of each situation.[75] Electronic data are generally perishable. Integrity of data can be compromised by humidity, temperature, vibrations, physical mutilation, strong magnetic fields, computer commands to erase or reformat, etc. This condition may strengthen the grounds for this exception, but only in the presence of probable cause.

(f) Consent search. Neither probable cause nor a warrant is required if a police officer obtains a suspect's consent for a search. The police are not required to inform the suspect of his right to withhold consent.[76] The only criterion that must be satisfied is "voluntariness," defined in terms of whether a reasonable "person would feel free to decline the officers' requests or otherwise terminate the encounter."[77] The burden is on the government to prove that the criterion is met.

Defining the scope of consented search on a networked computer can be problematic when consent to search one computer does not necessarily extend to other computers or equipment that may be physically or virtually connected to it. Encryption creates another challenge. An encrypted computer file can be analogous to a locked file cabinet (because the owner is attempting to preserve secrecy) or to a document written in a language foreign to the reader. A warranted search would authorize searching for and seizing encrypted information, as well as requesting authority to decrypt (to "break the lock" on the cabinet or to "translate" the document). However, if the search is based on consent, a court may find that a target who encrypted data and did not disclose the necessary decryption key has tacitly limited the scope of consent. If police do not ask explicitly for consent to search the encrypted material, or such consent is refused, a warrant may be required for the encrypted data.[78]

(g) Border search. As a condition of crossing the border or its "functional equivalent," officials can search people and property without a warrant and without probable cause.[79] Incoming baggage, persons, and mail, as well as diskettes, tapes, computer hard drives, and other media, fall under this exception.[80]

This exception highlights the quintessential law-enforcement problem created by cyberspace. On the one hand, cyberspace is tied to physical locations of ISPs and Internet users within some sovereign territory. On the other hand, sending an email message is categorically different from crossing a national border in person or sending a paper letter. Regular mail travels intact and enters its international destination through an established border post. Email travels in the form of several packets of coded information that may separate en route and pass through servers located in various countries. The border search exception does not readily apply to data transmitted electronically because the justification for this exception, based on the sovereign's

power to exclude illegal articles from the country, no longer applies once such articles have come into the country undetected.[81]

Network monitoring, as a protective measure conducted by computer security specialists (without involvement of law enforcement) for the purposes of optimizing network performance and ensuring security, generally will not face constraints of criminal law. Cooperation among ISPs and computer security professionals could be summoned to protect hardware, software, and databases. This would serve not only the goal of combating cyber crime (which may have a lower priority in nongovernmental, for-profit organizations), but also immediate goals of meeting contractual commitments to customers, maintaining continuity of business, and guarding against liabilities that may arise from allegations of negligence. More effective computer security and timely detection of and response to unauthorized access or use of cyber systems would help reduce both cyber crime and intrusive law enforcement.

Should police investigation become necessary, the use of automated near-real-time intrusion detection, tracking, containment, response, and reporting capabilities would more readily satisfy the legal constraints imposed on this activity. Automation may not solve all problems, but where available and appropriate, it could provide grounds for probable cause, identify suspects, and collect a certain amount of evidence, while preserving the anonymity of uninvolved network users. Some automated methods may be limited in scope to local orientation and reaction, which is ineffective in the internetworked global environment. A global response to cyber crime demands capabilities to correlate intrusion/attack symptoms occurring seemingly independently in different parts of the network. Reaction must be coordinated and uniform. Constraints on search, seizure, and due process of law under these circumstances are necessarily more important.

2. Due Process of Law

International human rights' agreements and many national constitutions guarantee equal and proper treatment of individuals before the law. This guarantee entitles individuals to protection against self-incrimination and arbitrary arrest, detention, or exile. If arrested, one must be informed at the time of arrest of the reasons for the arrest and the charges made. The *Universal Declaration of Human Rights* and the *International Covenant of Civil and Political Rights* entitle every person to a fair and public hearing by a competent, independent, and impartial tribunal, in the determination of the person's rights and obligations and of any criminal charge. Moreover, everyone charged with a penal offense has the right to be presumed innocent until proved guilty according to law in a public trial and the right to call and confront witnesses and to introduce evidence. No one may be found guilty of any penal offense that did not constitute a penal offense under national or international law at the time it was committed, nor may a heavier penalty be imposed than the one applicable at the time the penal offense was committed.[82]

States implement such provisions through national criminal justice systems. Suspects typically have the right to silence, although the levels of protection differ. In the United States, the Fifth Amendment to the Constitution provides that no person "shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, with-

out due process of law."[83] In Israel, a suspect under arrest must be informed that anything he says might incriminate him. The suspect has the right to silence, but refusal to answer questions could strengthen evidence against him.[84] China recognizes no right to silence.[85] The *European Convention on Human Rights* has no explicit provision against self-incrimination.[86]

Due process of law is generally interpreted to require a trial or other legal proceedings, which provide fair procedures under accepted standards of national law and international norms. The right to qualified counsel is fairly common, but it differs in scope. South Africa, England, Italy, and Germany are among the strongest protectors of this right from the perspective of the accused.[87] Russian citizens have a constitutional right to qualified legal counsel, but the law permits both licensed attorneys and non-lawyers (members of a social organization or close family) to act as defense counsel in criminal proceedings.[88] In China, judges appoint legal counsel to criminal defendants if they consider it necessary.[89]

Regardless of the existing domestic and international legal safeguards, violations of due process principles persist around the world. The U.S. State Department reports widespread denials of basic legal protections and due process to criminal defendants, detentions without trial or charge, prolonged pre-trial detentions and trial delays, illegal searches, and infringements on citizens' privacy rights.[90]

Requirements for due process of law and accountability apply fully to computer-related cases. They also augment technological, legal, and organizational challenges involved in combating cyber crime. Effective and timely information exchanges among ISPs, technical experts, and law enforcement can improve investigative functions. A global incident-response capability may require teams of technical, legal, and police experts, linked to their respective organizations, to track trends and activities of known and potential cyber criminals and terrorists. Accomplishing such cooperation among individuals and organizations with different goals, cultures, and procedures is likely to be difficult from the operational standpoint. The legitimacy of specific methods used to accomplish such goals will be judged according to specific situations.

General warnings are also appropriate. Proposals have been made to assign a presumption of guilt to suspects who withhold decryption keys, unless the defense could somehow prove nonpossession.[91] Reversing burdens of proof in this manner may deprive an accused of the right to a fair trial. Extensive profiling of individual behaviors on the Internet may lead to self-incrimination. Once an infrastructure for policing of international networks is in place, it could be used to the detriment of private citizens. The extent of intrusion justified in a targeted and warranted police investigation is unacceptable in the general societal context.[92]

Concern over due process of law in the course of international cooperation against cyber crime and terrorism has led to a number of provisions in the proposed Draft Convention. As a minimum level of protection, it allows States Parties to insist on the preservation of national norms. It entitles any person detained by a State Party to rights extended under national law to: communicate without unnecessary delay with the appropriate representative of the detained person's state or authority entitled to protect his or her rights; be visited by a representative of that state; have this representative physically present to observe any legal proceedings that may result in punishment; and be informed of these entitlements promptly after detention. The Draft Convention prohibits any denial or impairment of these entitlements.[93]

The Draft Convention also prohibits extradition or legal assistance if there are grounds to believe that a suspect will be prosecuted or punished on account of political offense, or on account of that person's race, religion, nationality, ethnic origin, or political belief. Although strong differences exist among states concerning restrictions on expression and political activity, this provision allows states to prevent or hinder politically motivated or unfair prosecutions by refusing or ceasing cooperation with the prosecuting state.[94] In case of a serious and unresolvable situation of abuse of the international regime of technical and legal cooperation, effective economic and political sanctions should be imposed on the offending state. The sanctions may extend to denial of technological and economic assistance under the regime, expulsion from the regime, and measures to limit the ability of the offending government to benefit from participating in the international information infrastructure.

Conclusion

The extent to which the rights to privacy, the protections against unwarranted searches and seizures, and the rights to due process of law constrain an international regime against cyber crime and terrorism depends on the regime and the domestic laws of participating states. National laws often contain exceptions or special privileges for law enforcement to pursue criminal investigations. States have different attitudes toward privacy, law enforcement powers, and due process. However, unilateral responses to cyber crime are not likely to be effective. Confronted with the need for international cooperation, states will look for ways to reconcile these differences or attempt to justify some inappropriate behavior. Greater emphasis on protective technological and legal measures will help reduce the latter outcome.

Overall, protective measures, which aim to reduce cyber vulnerabilities and rely on computer security staff for initial reaction to incidents, are less intrusive than measures designed to allow extensive law enforcement presence in cyberspace. The protective approach can be implemented through encryption, automation, and anonymous tagging and tracking—recording fields in packet header information, for example, which does not intrude on the content of messages, or router-assisted fingerprinting of packets without disclosure of their originator unless sufficient evidence of crime emerges. Although better measures will need to be designed and updated continuously to keep up with offenses, this approach can afford greater protection against both cyber crime and intrusive law enforcement.

The reactive approach necessarily involves the participation of law-enforcement officials, who will likely scan files, review content, and engage in other surveillance of communications to collect evidence and to identify perpetrators. Engaging in such activities on a wide "preventive" scale, rather than in targeted and warranted investigations, would raise legal and moral concerns of unduly intrusive policing. Furthermore, even in specific cases of suspected crime, limiting the scope of targeted surveillance may be technologically and operationally difficult. This approach places communications of innocent people and their private information at risk. The reactive approach requires greater scrutiny.

While clearly threatening to civil liberties, reactive measures would not necessarily result in fewer crimes and better law enforcement. Even in most technologically and economically developed countries today, police lack equipment and training to meet the growing challenge of the electronic dimensions of crime. Technical experts agree that greater automation is crucial for a timely, scalable, and less intrusive response to international cyber crime. This offers hope that—in the name of both efficiency and civil liberties—relatively nonintrusive technological measures will be developed and implemented in the near future. Such solutions should provide a more suitable balance among security, law enforcement, and civil liberties in cyberspace. Reactive measures will also be enhanced, however, and will need to be fashioned and monitored to ensure adequate protection of human rights.

The technologies of crime and punishment are undergoing a rapid and profound evolution. Such technologies constitute a moving target for evaluation. However, the legal and normative principles discussed here will endure, because they are independent of specific technological means. As such, they can provide a framework for building a global infrastructure and policy environment that balances the needs for crime-free business, government, and personal communications with the protection of property, privacy, and civil liberties.

Where trade-offs between security and civil liberties are required, these trade-offs should be carefully examined with the awareness of threats and social implications of measures against cyber crime and terrorism. Ensuring the protection of fundamental rights to privacy and due process of law is essential. Such protections should be prominent among the design criteria for technological, policy, and legal measures and should be enforced by law and strong economic and political incentives.

Governments value liberty, privacy, and security differently. National rules concerning the intrusiveness of law enforcement, protection of citizens' rights, and international cooperation reflect the country's normative choices about the roles of the state, market, and individual. Comprising the basis of domestic law, these norms affect the international behavior of nation-states. An international regime can help influence these norms over time. Today, when an international regime to combat cyber crime and terrorism is becoming a reality, there is a special opportunity to promote greater respect for human rights. At the very least, methods for international technological and legal cooperation against cyber crime and terrorism should not be permitted to become a vehicle for governments to oppress society.

Notes

[1] Cyber crime and terrorism involve attacks that may target the information infrastructure—any computer or network of computers used to relay, transmit, coordinate or control communications of data or programs—or use it as a channel to reach other targets. The word "cyber" is used here to refer to such infrastructures and systems and to conduct that affects them. The Internet, for example, has been used to steal intellectual property or services, distribute viruses and other malicious code, destroy data files, and perpetrate fraud, theft, and extortion. Terrorists may use it as a target or a channel for harassment, coercion, or destruction of information resources or social institutions. Countries are increasingly criminalizing such behavior and seeking means for international cooperation to prosecute and deter cyber crimes.

[2] On modes of attack and computer security measures see generally Dorothy E. Denning, *Information Warfare and Security* (Reading, MA: ACM Press and Addison Wesley Longman, 1999); Eric A. Fisch and Gregory B. White, *Secure Computers and Networks: Analysis, Design, and Implementation* (Boca Raton, FL: CRC Press, 2000); Ryan Henry and Edward Peartree, eds., *The Information Revolution and International Security* (Washington, D.C.: The Center for Strategic and International Studies Press, 1998).

[3] See *International Cooperation to Combat Cyber Crime and Terrorism* (forthcoming, Hoover Press). Proposals for voluntary international cooperation have been advanced and are being implemented. See, e.g., "Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime" (Moscow, Oct. 19–20, 1999), communiqué available at <http://www.library.utoronto.ca/g7/adhoc/crime99.htm>. See also Internet Alliance, policy materials posted at <http://www.Internetalliance.org/policy/index.html>, and information on the "G8 Paris Conference: A Government/Industry Dialogue on Safety and Confidence in Cyberspace" (Paris, May 15–17, 2000), available at <http://www.g8parishightech.org/index.htm>. An international treaty approach has also been proposed. The Council of Europe produced a "Draft Convention on Cyber-Crime," released for public discussion on April 27, 2000, available at <http://conventions.coe.int/treaty/en/projects/cybercrime.html>. For a different draft treaty, see Abraham D. Sofaer, Seymour E. Goodman, Mariano-Florentino Cuéllar, Ekaterina A. Drozdova, David D. Elliott, Gregory D. Grove, Stephen J. Lukasik, Tonya L. Putnam, George D. Wilson, "A Proposal for an International Convention on Cyber Crime and Terrorism" (forthcoming, Center for International Security and Cooperation, Stanford University). Both treaties are largely consistent, and both assume, on the basis of empirical observations, that a substantial consensus exists regarding criminalizing certain activities in cyberspace. The treaties differ mainly in that, while the Council of Europe proposes definitions of specific cyber activities that must be made criminal by States Parties, the Stanford group proposes to criminalize types of activities and let States Parties define them as consistent with their domestic law. The latter Draft Convention also proposes to establish an agency that will prepare and promulgate standards and recommended practices to enhance the protective and investigative measures.

[4] As discussed at the Conference on International Cooperation to Combat Cyber Crime and Terrorism, Stanford University (Dec. 6–7, 1999). Neither exhaustive nor mutually exclusive, the two approaches provide a useful framework for evaluating, with respect to civil liberties, the technical and legal measures against cyber crime and terrorism.

[5] See Denning, *supra,* note 2.

[6] See Whitfield Diffie, presentation at the Conference on International Cooperation to Combat Cyber Crime and Terrorism, Stanford University (Dec. 6–7, 1999).

[7] Forms of this are being implemented by the Russian and U.S. governments, as discussed in the privacy section below.

[8] These obstacles include budget constraints, technical complexity, unclear responsibilities, security weaknesses in products, lack of awareness, lack of good security tools, lack of competent information security personnel, privacy and ethics issues, and legal or regulatory issues. Yet computer security requires a comprehensive and integrated approach that extends throughout the entire information life cycle and recognizes the interdependencies of information security with such factors as system management, organizational management, legal issues, and physical and personnel security. See Denning, *supra,* note 2, pp. 396–400.

[9] The *Universal Declaration of Human Rights*, UN GA Res. 217A (III) (1948). The 1976 *International Covenant on Civil and Political Rights* (UN GA Res. 2200A [XXI] [1966, entry into force 1976]) obliges state signatories to

adopt legislative and other measures to protect against unlawful and arbitrary interference with and attacks on privacy by state authorities or natural or legal persons. The 1950 *European Convention on Human Rights* (Council of Europe, European Treaties, ETS No. 5) is a binding treaty that obligates its signatories to protect privacy interests, such as the right to private and family life, home, and correspondence, and enforces this obligation through the European Court of Human Rights. A state, person, nongovernmental organization or group of individuals claiming to be a victim of a violation by a contracting party may apply to the court for redress.

[10] *Universal Declaration of Human Rights*, Article 12, *supra,* note 9.

[11] Ibid., Article 19.

[12] Stein Schjolberg, Chief Judge, Moss Byrett City, Norway, "Legal Mechanisms for International Cooperation—Protecting Privacy and Other Rights" (presented at the Conference on International Cooperation to Combat Cyber Crime and Terrorism, Stanford University, Dec. 6–7, 1999).

[13] The 1995 U.S. Department of State review on human rights' practices reported that 110 countries guaranteed the right to privacy in their constitutions. See David Banisar, "U.S. State Department Reports Worldwide Privacy Abuses," excerpts from *U.S. Department of State Country Reports on Human Rights Practices for 1995,* Privacy International, available at <http://www.privacy.org/pi/reports/1995_hranalysis.html>. The 1999 survey by the Electronic Privacy Information Center (EPIC) ("Privacy & Human Rights: An International Survey of Privacy Laws and Developments") reported that at least 55 countries do not have constitutional provisions on privacy but establish protections through other legal means. For a discussion of privacy law in the United States, see Robert Gellman, "Does Privacy Law Work?" Philip E. Agre and Marc Rotenberg, eds., *Technology and Privacy: The New Landscape* (Cambridge, MA: MIT Press, 1998), pp. 193–218.

[14] Specific aspects of these guarantees are addressed by such legislation as the *Fair Credit Reporting Act* (15 *U.S. Code* §§1681–1688t), *Family Education Rights and Privacy Act* (20 *U.S. Code* §1232g.), the *Electronic Communications Privacy Act* (Public Law 99–508, 100 Stat. 1848–73 [1986]), and other statutes. See Gellman, *supra,* note 13, pp. 193–218.

[15] Ulrich Sieber, "Legal Aspects of Computer-Related Crime in the Information Society—COMCRIME-Study—Prepared for the European Commission," Version 1.0 (Jan. 1, 1998), Section I.B.2.a, "Protection of Privacy," pp. 62–64.

[16] "Implementing the OECD Privacy Guidelines in the Electronic Environment: Focus on the Internet," Group of Experts on Information Security and Privacy, OECD, DSTI/ICCP/REG(97)6/FINAL, pp. 6–10.

[17] The Convention (ETS No. 108, 28 January 1981, entry into force Jan. 10, 1985) has since become law in over twenty countries. See "Privacy & Human Rights: An International Survey of Privacy Laws and Developments," Electronic Privacy Information Center (EPIC) in association with Privacy International (1999), p. 10.

[18] UN GA Res. 44/132, 44 UN GAOR Supp. (No. 49) at 211, UN Doc. A/44/49 (1989).

[19] Directive 95/46/EC of the European Parliament and of the Council "On the protection of individuals with regard to the processing of personal data and on the free movement of such data." "Council Definitively Adopts Directive on Protection of Personal Data," European Commission Press Release: IP/95/822 (July 25, 1995).

[20] Recommendation No. R (99) 5 of the Committee of Ministers to Member States for the Protection of Privacy on the Internet: "Guidelines for the Protection of Individuals with Regard to the Collection and Processing of Personal Data on Information Highways," adopted by the Committee of Ministers at the 660th meeting of the Ministers' Deputies (Feb. 23, 1999), available at <http://www.coe.fr/cm/ta/rec/1999/99r5/htm>.

[21] Electronic Privacy Information Center (EPIC) Privacy Survey (1999), p. v. For specifics on laws and instruments for the protection of privacy and personal data in various countries see "Inventory of Instruments and Mechanisms Contributing to the Implementation and Enforcement of the OECD Privacy Guidelines on Global Networks," OECD, DSTI/ICCP/REG(98)12/FINAL; and "Excerpts on Privacy from U.S. State Department Human Rights Guides," prepared by Global Internet Liberty Campaign, available at <http://www.gilc.org/privacy/>.

[22] See Schjolberg, *supra,* note 12.

[23] See Jeffrey Rosen, "The Eroded Self," *The New York Times Magazine* (Apr. 30, 2000), pp. 46-53.

[24] Ann Beeson, "Privacy in Cyberspace: Is Your E-mail Safe From the Boss, the SysOp, the Hackers, and the Cops?" American Civil Liberties Union, *Cyber-Liberties* (1996), available at <http://www.aclu.org/issues/cyber/priv/privpap.html>.

[25] Stephen J. Lukasik, "Combating Cyber Crime and Terrorism" (presented at the Technical Seminar, Center for International Security and Cooperation, Stanford University, May 2, 2000). Identity theft figures were reported by the Social Security Administration, id.

[26] Sam Howe Verhovek, "Creators of Anti-Abortion Web Site Told to Pay Millions," *New York Times* (Feb. 3, 1999), A11.

[27] See generally Richard Power, ed., "2000 CSI/FBI Computer Crime and Security Survey," VI *Computer Security Issues & Trends* (Spring 2000); Seymour E. Goodman and Abraham Sofaer, "Cyber Crime and Security: The Transnational Dimensions," Chapter 1, *International Cooperation to Combat Cyber Crime and Terrorism* (forthcoming, Hoover Press).

[28] *European Convention on Human Rights*, *supra,* note 9, Article 8.

[29] Caspar Bowden, "Unprecedented Safeguards for Unprecedented Capabilities," Foundation for Information Policy Research (FIPR), United Kingdom (presented at the Conference on International Cooperation to Combat Cyber Crime and Terrorism, Stanford University, Dec. 6–7, 1999).

[30] This System to Conduct Investigations and Field Operations in Russia is known as SORM, which stands for Sistema Operativno-Rozysknykh Meropriiatii. In an open letter to the Russian government, representatives of the Russian Internet community and organized Internet societies stated that "particular danger nests in the Technical Requirements for SORM. Today's version of legislation puts the control for the presence of a jury or prosecutor's warrant in the hands of the same authority, which is doing wiretapping. This approach can not guarantee in practice to Internet users their constitutional rights." The letter can be viewed in Russian and downloaded in English at <http://www.libertarium.ru/eng/>. See also Moscow Libertarium, <http://www.libertarium.ru/>, for a discussion and background documents on SORM.

[31] "Russia's Security Agency Spies on Internet," Features and Commentary, *HPCwire* (Feb. 25, 2000). Article 23 of the Constitution of the Russian Federation (1993) guarantees the right to privacy of correspondence, telephone communications, mail, cables, and other communications. Article 24 forbids gathering, storing, using, and disseminating information on the private life of any person without his or her consent and obligates state and local authorities to provide to each citizen access to any materials directly affecting his rights and liberties unless otherwise stipulated by law. The Law on Operational Investigative Activity permits FSB, the Tax Police, and the Ministry of Interior to monitor telephone and other types of communication pursuant to a court order. *Zakon Operativno-Rozisknoi Deiatelnosti* (The Law on Operational Investigative Activity), No. 144-FZ, (8/12/1995). Also see Catherine Newcombe, "Russian Federation," in Craig M. Bradley, ed., *Criminal Procedure: A Worldwide Study* (Durham, NC: Carolina Academic Press, 1999), pp. 294–295.

[32] Neil King Jr. and Ted Bridis, "FBI's System to Covertly Search E-mail Raises Privacy, Legal Issues," *The Wall Street Journal* (July 11, 2000).

[33] See *Echelon Watch,* <http://www.aclu.org/echelonwatch/>, administered by the American Civil Liberties Union in conjunction with the Free Congress Foundation, the Electronic Privacy Information Center, Cyber-Rights and Cyber-Liberties (UK), and the Omega Foundation. See also, "An Appraisal of Technologies of Political Control," European Parliament, Scientific and Technological Options Assessment, Working Document (Jan. 6, 1998), Luxembourg, available at <http://cryptome.org/stoa-atpc.htm>.

[34] See "Memo on International Electronic Surveillance Concerns" (addressed to the United States Congress by the American Civil Liberties Union, Center for Democracy and Technology, Eagle Forum, Electronic Frontier Foundation, Electronic Privacy Information Center, and Free Congress Foundation, June 7, 1999), available at <http://www.aclu.org/

congress/l060899a.html>; "Lawsuit Seeks Memos on Surveillance of Americans; EPIC Launches Study of NSA Interception Activities," Electronic Privacy Information Center Press Release (Dec. 3, 1999), available at <http://www.epic.org/open_gov/foia/nsa_suit_12_99.html>; "French Prosecutor Starts Probe of U.S. Spy System," *Reuters* (July 4, 2000), reported at <http://news.excite.com/news/r/000704/08/news-france-usa-dc>.

[35] Global Internet Liberty Campaign (GILC) Privacy Survey 1997, *Models of Privacy Protection.* Also see David Flaherty, "Controlling Surveillance: Can Privacy Protection Be Made Effective?" in Agre and Rotenberg, *supra,* note 13, pp. 167–192. Mr. Flaherty is the Information and Privacy Commissioner for British Columbia, Canada.

[36] Hearing: "The European Union and Data Protection," European Parliament, Committee on Citizen's Freedoms and Rights, Justice and Home Affairs, the Committee on Legal Affairs and the Internal Market (Feb. 22–23, 2000). The hearing program, statements, and background documents can be viewed at <http://www.europarl.eu.int/dg2/hearings/20000222/libe/agenda/en/default.htm>.

[37] Robert O'Harrow Jr., "U.S., EU Agree on Privacy Standard," *The Washington Post* (June 1, 2000), E01.

[38] The Maastrict Treaty that established the European Union and the three Pillars can be viewed at <http://www.felixent.force9.co.uk/europe/eu.html>.

[39] See Hearing, *supra,* note 36.

[40] See Stephen J. Lukasik, "Current and Future Technical Capabilities," *International Cooperation to Combat Cyber Crime and Terrorism,* Chapter 4 (forthcoming, Hoover Press), Section II, "Defending Information Systems Against Cyber Attack," and Conclusion. See generally, *supra,* note 2.

[41] Dynamically allocated IP addresses may still present a tracking problem. Moreover, IPv6 allows for the allocation of unique addresses for each network node (addresses in the current IP version 4 have been depleted). This will enable greater clarity and reliability in determining originators and recipients of suspect messages. See Lee Garber, "Steve Deering on IP Next Generation," *Computer* (April 1999), pp. 11–13. However, if the nondisclosure feature is not used, privacy may be compromised.

[42] José Luis Barbería, "Los países europeos del G-8 rechazan el plan de EE UU de crear una 'ciberpolicía' mundial," *El País Digital* (May 16, 2000), reported at <http://www.elpais.es/p/d/20000516/sociedad/ciberpol.htm>. "Rich Nations to Work Together Against Cyber Crime," by Reuters, *The New York Times On The Web* (May 15, 2000), reported at <http://www.nytimes.com/reuters/international/international-crime-c.html>. Joelle Diderich, "G8 to Work Together Against Cyber Crime," Reuters (May 14, 2000), available at <http://www.zdnet.com/zdnn/stories/news/0,4586,2569402,00.html>. Anne Swardson, "International Officials Admit Internet Security Holes," *The Washington Post On Line* (May 16, 2000), reported at <http://washingtonpost.com/wp-dyn/articles/A12013-2000May16.html>.

[43] Reuters, "Rich Nations," *supra,* note 42. Also Diderich, "G8 to Work Together," *supra,* note 42.

[44] Researchers from Stanford's Center for International Security and Cooperation (CISAC), Consortium for Research on Information Security and Policy (CRISP), and the Hoover Institution include: Cuéllar, Drozdova, Elliott, Goodman, Grove, Lukasik, Putnam, Sofaer, and Wilson. The Draft Convention was created as part of the preparation for the Conference on International Cooperation to Combat Cyber Crime and Terrorism, Stanford University (Dec. 6–7, 1999). For text of the convention and commentary see *supra,* note 3.

[45] "International Convention to Enhance Protection from Cyber Crime and Terrorism," *supra,* note 3, Articles 2-8.

[46] Ibid., Article 13.

[47] Donn B. Parker, "Sharing Infrastructures' Cyber Crime Intelligence," SRI Consulting (unpublished paper, Dec. 1999), pp. 16-17, and David J. Thelander, presentation at the Conference on International Cooperation to Combat Cyber Crime and Terrorism, Stanford University (Dec. 7, 1999).

[48] See Johannes Lensing, "General Comments," in Bradley, *supra,* note 31, p. 427.

[49] The Constitution of the United States.

[50] See Lensing, in Bradley, *supra,* note 48, p. 427–429.

[51] Drew C. Arena, "Obstacles to Consensus in Multilateral Responses to Cyber Crime" (presented at the Conference on International Cooperation to Combat Cyber Crime and Terrorism, Stanford University, Dec. 6–7, 1999), pp. 5–6.

[52] Draft "International Convention to Enhance Protection from Cyber Crime and Terrorism," *supra,* note 44, Articles 5, 6, and 11.

[53] Ibid., Article 9.

[54] As discussed by Dorothy E. Denning, "Constraints to Technical Cooperation" (presented at the Conference on International Cooperation to Combat Cyber Crime and Terrorism, Stanford University, Dec. 6–7, 1999).

[55] See generally, Whitfield Diffie and Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption* (Cambridge, MA: The MIT Press, 1998).

[56] "Federal Guidelines for Searching and Seizing Computers," available at <http://www.usdoj.gov/criminal/cybercrime/search_docs/toc.htm>, additional documents available at <http://www.usdoj.gov/criminal/cybercrime/searching.html>. Also Craig M. Bradley, "United States," in Bradley, *supra,* note 31, pp. 395–424. Specific cases establishing the principles are noted.

[57] *Katz v. United States,* 389 U.S. 507 (1967).

[58] For example, flying over a suspect's land in a helicopter to verify the growing of marijuana (*Florida v. Riley,* 488 U.S. 445 [1989]), searching trash bins left at the curb of the house for pickup (*California v. Greenwood,* 486 U.S. 35 [1999]), and using an electronic beeper to track a car's location on the highway (*United States v. Knotts,* 460 U.S. 276 [1983]) are not considered to be "searches." However, placing an electronic beeper in a container of chemicals to determine whether the container remained inside the suspect's house was considered a "search" subject to Fourth Amendment requirements (*United States v. Karo,* 468 U.S. 705 [1984]).

[59] See Bradley, *supra,* note 56, p. 403, for a discussion and references on searches in private versus public spaces, such as in structures versus outdoors. See generally Noah D. Zatz, "Sidewalks in Cyberspace: Making Space for Public Forums in the Electronic Environment," *Harvard Journal of Law & Technology*, Volume 12, Number 1 (Fall 1998), pp. 149-240.

[60] Supplement to Federal Guidelines for Searching and Seizing Computers (1999), available at <http://www.usdoj.gov/criminal/cybercrime/supplement/s&suppii.htm#IIF>.

[61] *United States v. Charbonneau,* 979 F. Supp. 1177 (S.D. Ohio 1997).

[62] *United States v. Aquilar,* 883 F. 2d 662, 705 (9th Cir. 1989), *cert. denied,* 498 U.S. 1046 (1991); *Pleasant v. Lovell,* 876 F. 2d 787, 803 (10th Cir. 1989).

[63] Supplement, *supra,* note 60.

[64] See *Steve Jackson Games, Inc. v. United States Secret Service,* 816 F. Supp. 432 (W.D. Tex. 1993), *affd,* 36 F. 3d 457 (5th Cir. 1994). The court ruled that, even though the agent believed the probable cause in good faith, his lack of due diligence in learning about the suspect and his seizing of materials, which were intended for publication but not recognized as such by the agent, were unlawful.

[65] Creating plain view by moving or disturbing items was ruled unlawful in *Arizona v. Hicks,* 480 U.S. 321 (1987). In *United States v. Place,* 462 U.S. 696 (1983), the Supreme Court concluded that the limited and "low tech" nature of enhanced plain view intrusion did not require probable cause. However, the use of sophisticated devices to enhance plain view would intrude upon a citizen's reasonable expectation of privacy and does require probable cause. See Bradley, *supra,* note 56, pp. 403–404.

[66] "Federal Guidelines," *supra,* note 56.

[67] See generally Zatz, *supra,* note 59. Also see generally Larry Downes, "Electronic Communications and the Plain View Exception: More 'Bad Physics,'" *Harvard Journal of Law & Technology,* Volume 7, Number 2 (Spring 1994).

[68] 18 U.S.C. §§2510-2518.

[69] Bowden, *supra,* note 29.

[70] According to Mark Rasch, a former federal computer-crime prosecutor, the wiretapping system used by the FBI is "the electronic equivalent of listening of everybody's phone calls to see if it's the phone call you should be monitoring." See King and Bridis, *supra,* note 32.

[71] *United States v. David,* 756 F. Supp. 1385, 1392 (D. Nev. 1991). For a discussion of exigent circumstances in computer searches and seizures see "Federal Guidelines," *supra,* note 56.

[72] *Mincey v. Arizona,* 437 U.S. 385, 392-93 (1978).

[73] *United States v. Arias,* 923 F. 2d 1387 (9th Cir.), *cert. denied,* 112 S. Ct. 130 (1991).

[74] *United States v. David,* 756 F. Supp. 1385, (D. Nev. 1991).

[75] "Federal Guidelines," *supra,* note 56.

[76] *Schneckloth v. Bustamonte,* 412 U.S. 218 (1973).

[77] *Florida v. Bostick,* 501 U.S. 429 (1991).

[78] *United States v. David,* 756 F. Supp. 1385 (D. Nev. 1991). "Federal Guidelines," *supra,* note 56.

[79] *United States v. Ramsey,* 431 U.S. 606 (1977), *cert. denied,* 434 U.S. 1062 (1978).

[80] "Federal Guidelines," *supra,* note 56.

[81] Ibid.

[82] *Universal Declaration of Human Rights*, *supra,* note 9, Articles 6–11, and the *International Covenant of Civil and Political Rights*, *supra,* note 9, Articles 9 and 14. The binding *European Convention on Human Rights* embodies these principles in the "right to liberty and security," the "right to fair trial," and the prohibition of "punishment without law," Articles 5, 6, and 7 respectively, *supra,* note 9.

[83] The Constitution of the United States.

[84] Boaz Guttman, "The Right of Non-Self-Incrimination in Israeli Law in the Context of Computer Crimes" (Apr. 20, 2000); Israeli Criminal Procedure Order (Testimony), 1927, paragraph 2(2); Israeli Evidence Order (new version), 1971, paragraph 47(a); Israeli Criminal Procedures Order (combined version), 1982, paragraph 152(b) Criminal Procedures Law (Enforcement–Arrest), 1996, paragraph 28(a).

[85] Liling Yue, "China," in Bradley, *supra,* note 31, p. 86.

[86] The *European Convention on Human Rights*, *supra,* note 9.

[87] Lensing, *supra,* note 48, pp. 427–428.

[88] Newcombe, *supra,* note 31, p. 290.

[89] Liling Yue, *supra,* note 85, p. 88.

[90] "1999 Country Reports on Human Rights Practices," Bureau of Democracy, Human Rights, and Labor, U.S. Department of State (Feb. 25, 2000), available at <http://www.state.gov/www/global/human_rights/99hrp_index.html>.

[91] Bowden, *supra,* note 29.

[92] This view was also argued by Barry Steinhardt in his presentation at the Conference on International Cooperation to Combat Cyber Crime and Terrorism, Stanford University (Dec. 6–7, 1999).

[93] "International Convention to Enhance Protection from Cyber Crime and Terrorism," *supra,* note 52, Article 10.

[94] Ibid., Article 19.