GLOBAL INTERNET POLICY INITIATIVE

Trust And Security In Cyberspace: The Legal And Policy Framework for Addressing Cybercrime

September 2005

I. Background: The Relevance of Cybercrime Law to ICT Development

Developing countries around the world rightly see the Internet as a potentially powerful tool to advance economic and human development. At the same time, however, criminals also see the potential of the Internet – as a place to perpetrate fraud and as a communications medium of global reach and low cost. Hackers find a thrill in penetrating networks and destroying data, while terrorists could purposely disrupt the critical infrastructures that are dependent on networked computers. Meanwhile, consumers hesitate from disclosing personal and credit card data on the Internet, with security and privacy their number one concern, and businesses face losses of proprietary data, intellectual property, and online access to customers and suppliers due to security breaches and intentional service interruptions.

In order for the Internet to contribute to economic growth, human development and democratization, it must be trustworthy and secure. Lack of trust and security jeopardizes development goals that could be supported by a widely accessible and widely trusted Internet.

II. The Elements of Trust and Security Online

Effective public policy for the Internet is based on a mix of laws, industry self-regulation and technical standards that give users control. Together, these elements create the policy environment supporting investment, innovation and growth. In terms of trust and security, this environment includes the criminal law, laws of privacy and consumer protection, and the commitment of industry to build and operate more secure systems. There are at least four components to the framework for trust and security online:

- **Cybercrime** – Every country should adopt criminal laws against attacks on the security and integrity of computer systems, thereby criminalizing hacking, illegal interception, interference with the availability of computer systems.

- **Standards Defining and Limiting Government Access to Communications and Stored Data** – A nation should have clear procedures meeting international privacy standards for government access to communications and stored data when needed for the investigation of crimes. Such procedures both permit the government to carry out its investigations and also assure businesses and consumers that the government cannot unjustifiably monitor their communications.

- **Consumer Protection** – Systems and rules must be in place facilitating the use of credit cards and electronic forms of payment, in a legal framework ensuring that a consumer or small business owner who transacts business online has recourse if the transaction does not go through or the goods or service purchased online are unsatisfactory. And consumers must be assured that data they provide to merchants will not be misused.

- **Computer and Network Security** – In the final analysis, laws will not make computer networks more secure. The problem of computer crime will be solved only when makers of computer technology build more secure systems and when owners, operators and users of computer systems operate their systems in more secure manner. By and large, this is an area in which the private sector must lead. It is not the government's role to dictate standards or control technology design. Governments do need, however, to secure their own computer systems with proper security practices.

This memo focuses on the first two of these elements of cybersecurity: the criminal law and the legal standards for government surveillance.

III. Cybercrime Legislation

A. Basic cybercrime provisions

Every nation, as part of the legal framework promoting trust and confidence in cyberspace, should have basic criminal laws against activities that attack the confidentiality, integrity or availability of computer data and computer systems.

There are various ways to conceptualize cybercrime, and various names for specific offenses, but in general cybercrime law addresses four kinds of activity:

- **Data interception:** It should be prohibited to intentionally intercept, without right, by technical means, non-public transmissions of computer data to, from or within a computer system. This crime constitutes an essential element of cyber-trust, for it protects the confidentiality of communications. For example, it makes it illegal to intercept the email of another person. If the law already makes it a crime to intercept telephone conversations without legal authorization, then the telephone provision could be amended to cover all electronic communications. If the law does not protect the privacy of telephone communications, a general provision should be adopted making it a crime to wiretap telephone conversations and any other non-public electronic communications without a court order or some other permission (i.e., employers may in some countries listen to workplace conversations of employees).

- **Data interference:** It should be a crime to intentionally damage, delete, degrade, alter or suppress data in someone else's computer without right. This provision would cover, for example, intentionally sending viruses that delete files, or hacking a computer and changing or deleting data, or hacking a web site and changing its appearance. The element of intentionality is important, since otherwise producing defective software or unintentionally forwarding a virus would be a crime.

- **System interference:** It should be a crime to intentionally cause serious hindrance without right to the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data. This provision should cover things like denial of service attacks or introducing viruses into a system in ways that interfere with its normal usage. It is important that this offense include, as an element of the offense, the concept that there must be significant harm (e.g., a certain threshold of monetary loss) in order for an offense to occur; otherwise, ordinary online behavior, such as sending one or just a few unsolicited emails, would be a crime, which is not sensible.

- **Illegal access**: This is the crime of intentionally accessing, without right, the computer system of another. It can be thought of as the cyberspace equivalent of trespass. (Looked at another way, illegal access is an offense against the confidentiality of stored data and therefore is analogous to illegal interception, which is an offense against the confidentiality of data in transit.) This crime must be carefully defined, lest it include common, harmless activity. In the most serious cases, the act of illegal access is part of another crime covered by the three listed above, such as data interference, or it involves another crime covered by offline law, such as theft of proprietary data (see below). In some legal systems, the definition of the crime of illegal access is limited to situations in which confidential information (medical or financial information) is taken, copied or viewed or where there is an intent to obtain confidential information or where access is obtained only by defeating security measures.

-- Computer-related or computer-facilitated crime

Discussions of computer crime often extend into matters that are not crimes *against* computers, but are crimes *facilitated* by the use of computers. For example, theft is a crime in every legal system, and the criminal law should cover theft whether it occurs online or offline. Similarly, fraud is a crime, and ordinary fraud statutes will often use terminology that applies equally well to online conduct as it did to offline conduct. Other crimes, such as infringement of intellectual property rights or dissemination of child pornography also are not properly computer crimes – they are crimes that may be facilitated by use of a computer. Before adopting a series of separate offenses "facilitated by computer," governments should examine their traditional laws to see if they already cover computer-facilitated offenses as well. In many cases, traditional criminal laws will cover offenses committed online. And to the extent they do not, rather than establishing separate offenses for computer-related crime, it might be better to amend the general crimes laws to make it clear that they cover online conduct.

-- Application of basic criminal law concepts

Nations may also want to consider how common concepts of the criminal law such as "aiding and abetting" or "attempt" apply to cybercrime. Thus, if a nation's law has the concept of an attempted offense, then that concept might apply to cybercrime. For example, launching a virus with intent to disrupt service might be a crime under the concept of intent even if the virus didn't work as intended. Similarly, if a nation's law has the concept of aiding and abetting, that

might be applied to cyber-crime, such that one who intentionally produces a virus and provides it to another knowing or intending that it will be used to destroy data or interfere with a system may be guilty of data or network interference caused by the virus even if the virus was introduced into a network by someone else.

B. The COE Convention on Cybercrime

In 2001, the Council of Europe completed drafting a Convention on Cybercrime.[1] As of September 15, 2005, the treaty had been ratified by only 11 countries, mostly in Eastern Europe. The number of ratifications has been sufficient for the convention to enter into force, on January 7, 2004. As of September 15, 2005, the convention had not been ratified by most Western European countries, nor had it been ratified by the United States, which played a major role in its drafting and had been invited to ratify it.

As a model, the convention has some positive and some negative elements. The convention is very broad, reaching far beyond computer crime as such. And having taken on the issue of government access to computer data (for all crimes), the treaty fails to address half of the issue (the privacy and human rights half). Accordingly, developing countries must be very cautious in approaching the COE convention as a model.

The COE convention is really three conventions in one, covering three different sets of issues, and developing nations looking to it as a model need not take on all three sets of issues at the same time. The three sets of issues covered by the Convention are:

- **Substantive computer crimes.** Despite the convention's title, only the first section of the treaty is focused on viruses, hacking or other attacks against computer systems or the computer-dependent critical infrastructures, and even that section extends into areas that cannot properly be called cybercrimes.
- **Government access to communications and computer data.** The second major part of the treaty is intended to require governments to adopt laws on search and seizure of computer evidence, disclosure to governments of computerized records of any kind, and electronic interception of communications -- for all kinds of crimes. These kinds of measures pose serious privacy questions, discussed below, that are not addressed in adequate detail in the convention. Especially in developing and transitional societies, unregulated government surveillance can seriously undermine trust in the Internet.
- **Trans-border cooperation.** The third major section of the treaty aims to require governments to cooperate with other countries seeking to search and seize computers, compel disclosure of data stored in computers, and carry out real-time interceptions – in all kinds of criminal cases – in other countries. And it covers extradition for computer crimes as defined under the treaty.

---

[1] The treaty, ETS no. 185, is online at http://conventions.coe.int/treaty/EN/cadreprincipal.htm along with an extensive Explanatory Report. It is very important that nations looking to the convention as a model also carefully consider the Explanatory Report, which has extensive explanations of the meaning of the treaty's sometimes cryptic provisions.

-- Substantive criminal offenses under the COE convention

Articles 2-5 of the convention address crimes against computers, computer communications and computerized data – these are the only offenses under the treaty that can really be called "cybercrimes." As noted above, these basic cybercrimes are

- Illegal access (Article 2);
- Illegal interception (Article 3);
- Data interference (Article 4);
- System interference (Article 5).

However, in the Convention itself these provisions are drafted in very broad and vague terms that could cover a wide range of common behavior. For example, Article 2 calls upon states to establish as a criminal offense "when committed intentionally, the access to the whole or any part of a computer system *without right*" (emphasis added). On their face, these words would make it a crime to send an unsolicited email, since the sender of an unsolicited email "accesses" the recipient's computer (or the mail server of the recipient's ISP) without right. The drafters of the Convention did not intend this outcome, and nations following the Convention should be careful to make it clear that "without right" does not cover common activities inherent in the Internet. As the Explanatory Report states, "legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised." (Para. 38.) These would include, for example, sending electronic mail without it having been first solicited by the recipient; accessing a web page, directly or through hypertext links; or using "cookies" or "bots." (Para. 46, 48.)

Further point of caution: the Explanatory Report also states that the phrase "without right" may refer to conduct undertaken without contractual authority. This interpretation seems unwise, for it could make violations of a service provider's terms of service into a criminal offense. The ISP subscriber who uses the service for a purpose prohibited by the terms of service is accessing the computer of the ISP "without right." The student who uploads or downloads a single music file in violation of the university's policy for granting students Internet access is committing a crime. We recommend that the crime of illegal access not apply to situations involving the violation of contracts with service providers.

Articles 7-10 of the convention reach more broadly, covering crimes involving the use of a computer to engage in conduct that is normally already a crime offline (i.e., forgery, fraud, and the distribution, production or possession of child pornography, copyright infringement). As explained above, adopting special provisions for computer-facilitated offenses will be unnecessary in some legal systems and might improperly suggest that a crime committed online is worse than the same crime committed offline. It is wise for governments to ensure that longstanding laws against forgery, fraud and child pornography do not exempt online conduct,

but as a general matter laws should be technology neutrality, and nations should probably avoid adopting separate code provisions for fraud online and fraud offline.[2]

IV. Surveillance standards and privacy protections

Consideration of cybercrime often leads to questions about the standards under which the government is authorized to obtain access to the electronic communications and computer data that may constitute evidence of cybercrime and other types of crime. Many countries have procedural laws granting the government investigative powers to access information stored in computers. These include judicial orders for the production stored data and warrants for the immediate search and seizure of computers and computerized data. Many countries also allow real-time interception of communications and the traffic data or transactional data that shows the origin and destination of communications.

Government seizures or compelled disclosures of data stored in computers and government interceptions of communications and traffic data constitute an intrusion on personal privacy. The right to privacy is widely recognized as a fundamental human right under the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the European Convention on Human Rights, and the American Convention on Human Rights.

Under most advanced legal systems, such privacy intrusions are permissible, but only in accordance with clear standards in the law, requiring justification and prior independent approval, which in many legal systems means approval by a judge. Governments addressing interception and data access issues must be sure to address the procedural standards for government access to communications and computer data. An emerging body of international experience provides useful guidance.

A. International standards for real-time interception

Given the grave privacy intrusion that real-time interception represents, strict legal standards apply to its authorization. Based upon developing national and international standards,[3] it is possible to identify certain elements that should govern any legal system for live interception of communications:

- The standards for interception should be fully and clearly spelled out in legislation available to the public, with sufficient precision to protect against arbitrary application

---

[2] That said, child pornography, which is internationally condemned, is easily facilitated by computers and governments should be sure that their laws adequately prohibit the production and dissemination of such material., lest they become havens for its production or online hosting. Likewise, protection of intellectual property is one of the important building blocks of cyberlaw.

[3] Perhaps the most developed body of international law on communications interception can be found in Europe, where the basic privacy principle in Article 8 of the European Convention of Human Rights has been given greater definition by the European Court of Human Rights (ECtHR). The principles outlined here are drawn from the case law of the ECtHR.

and so that citizens are aware of the circumstances and conditions under which public authorities are empowered to carry out such surveillance.

- Approval should be obtained from an independent official (preferably a judge),[4] based on a written application giving reasons and setting forth facts justifying the intrusion, and the approval should be manifested in written order.
- The legislation should limit surveillance only to the investigation of specified serious offenses.
- Approval should be granted only upon a strong factual showing of reason to believe that the target of the search is engaged in criminal conduct.
- Approval should be granted only when it is shown that other less intrusive techniques will not suffice.
- Each surveillance order should cover only specifically designated persons or accounts – generalized monitoring should not be permitted.
- The rules should be technology neutral – all one-to-one communications are treated the same, whether they involve voice, fax, images or data, wireline or wireless, digital or analog.
- The scope and length of time of the interception should be limited, and in no event should the surveillance extend longer than is necessary to obtain the needed evidence.
- The surveillance should be conducted in such a way as to reduce the intrusion on privacy to an unavoidable minimum necessary to obtain the needed evidence.
- The enabling legislation should describe the use to which seized or intercepted material could be put; information obtained for criminal investigative purposes may not be used for other ends.
- The law should specify procedures for drawing up summary reports for a judge's review and precautions to be taken in order to permit inspection of the recordings by the judge and by the defense.
- In criminal investigations, all those who have been the subject of interception should be notified after the investigation concludes, whether or not charges results.
- Personal redress should be provided for violations of the privacy standards.

These elements should be embodied in any national law for interception of communications (telephone calls, e-mail, and other electronic communications). Many of the same provisions are also applicable to search and seizure orders for computer data.

-- COE Convention must be supplemented with privacy protections

The COE Convention on Cybercrime explicitly requires that interceptions of communications and searches and seizures for stored data be conducted pursuant to the privacy

[4] Klass v. Germany, 6 September 1978, 2 EHRR 214 ("The Court considers that, in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge.").

principles set forth in the European Convention on Human Rights. Article 15 of the Cybercrime Convention provides:

> 1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, … and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.
> 2. Such conditions and safeguards shall, as appropriate in view of the nature of the power or procedure concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation on the scope and the duration of such power or procedure.

Unfortunately, the drafters of the treaty failed to spell out specific procedures that would comply with the European Convention of Human Rights. Nations not bound by the human rights principles of the COE should nevertheless look to the principles laid down by the European Court, summarised above, as well as to the surveillance laws of countries like Canada and the United States that have strong traditions of an independent judiciary and protection of privacy. Especially in developing and transitional societies, which may not have a fully defined set of rules for searches and seizure and surveillance in the offline world, it is important to give close attention to the development of strong standards for government surveillance in the digital context.

B. Data retention and other government design mandates

A number of developed countries (including the United States) have imposed design mandates on telephone common carriers (and, in some countries, ISPs), requiring that communications networks be designed to support government surveillance. Some countries have adopted, or are debating the adoption of, laws requiring service providers to retain traffic data on all communications for a specified period of time (a mandate referred to as "data retention"). These mandates have been very controversial. They threaten the privacy of citizens and they impose considerable costs on service providers. It should be noted, therefore, that the COE Cybercrime Convention does *not* impose design mandates, technical standards, or data retention requirements on service providers.[5] The treaty is intended solely to set procedures for preserving, seizing or accessing whatever data is otherwise available for business purposes, using whatever current technical capabilities companies may have, and it does not require changes in technology or business practices.

---

[5] Similarly, the European Union in 2002 adopted a directive on privacy in the communications sphere that permits but does not require member countries to adopt data retention requirements.

Articles 20 and 21 of the COE convention specifically state that the real-time interception laws required under the convention shall empower competent authorities to "compel a service provider, *within its existing technical capability*," to collect or record, or to co-operate and assist the competent authorities in the collection or recording of, traffic data and communications content. The Explanatory Report states: "The article does not obligate service providers to ensure that they have the technical capability to undertake collections, recordings, co-operation or assistance. It does not require them to acquire or develop new equipment, hire expert support or engage in costly re-configuration of their systems." Para. 221.

The COE treaty also recognizes the legitimacy of anonymous communications. The Explanatory Report makes it clear that the convention does not impose on service providers any obligation to keep records of their subscribers. Thus, under the Convention, a service provider would not be required to register identity information of users of pre-paid cards for telephone service, nor is it obliged to verify the identity of subscribers or to resist the use of pseudonyms by users of it services. Para. 181.

C. Encryption:

Any legal rules limiting the import, export or use of encryption should be eliminated. Strong encryption is crucial to securing the Internet, and the developed countries, which previously sought to control encryption, have in recent years concluded that, on balance, the general availability of encryption will improve security, not interfere with it. Accordingly, most developed countries no longer restrict encryption. The 1997 OECD Guidelines on Cryptography Policy and the 1998 European Commission report express strong support for the unrestricted development of encryption products and services. Based on these statements, Canada, Germany, Ireland, and Finland announced national cryptography policies based on the OECD Guidelines, favoring the free use of encryption. France, which had long restricted encryption, reversed that policy in January 1999 and announced that people can use encryption without restrictions. In December 1997, Belgium amended its 1994 law to eliminate the provision restricting cryptography. The United States, which had sought to limit use of encryption by limiting its export, lifted almost all restrictions on the export of encryption in 2000.

V. Resources

The United States has one of the most fully developed bodies of cybercrime laws and detailed surveillance laws. The U.S. Department of Justice has published *Federal Guidelines for Searching and Seizing Computers* to provide guidance to police agencies in the U.S. but the document may also be useful to policymakers in developing and transitional societies: http://www.cybercrime.gov/searching.html. The DOJ website has many other materials, at http://www.cybercrime.gov

Various international bodies have worked on this issue, resulting in a body of material that could provide a roadmap to developing and transitional countries:

- **European Union:** The European Commission has issued a series of cybersecurity recommendations, in the Communication "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime," available online at the EU Cybercrime Forum, http://cybercrime-forum.jrc.it/default/. Also available at that site, which is not being updated, is the EU recommendation on network security, 2002. Other EU resources are at: http://www.eu.int/scadplus/leg/en/s21012.htm#SECURITY and http://www.eu.int/information_society/policy/cybercrime/index_en.htm. Resources on the EU debate on data retention are available at http://www.edri.org/issues/privacy/dataretention and http://www.epic.org/privacy/intl/data_retention.html.
- **OECD**: The OECD Guidelines for the Security of Information Systems and Networks (May 2004) - http://www.oecd.org/document/42/0,2340,en_2649_37441_15582250_1_1_1_37441,00.html an important benchmark for industry and other stakeholders to protect critical information infrastructures. See also the accompanying implementation guide. See also OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (October 2004) - http://www.oecd.org/document/20/0,2340,en_2649_37441_15589524_1_1_1_37441,00.html
- **World Bank**: Information Technology Security Handbook (December 2003) http://www.infodev-security.net/handbook/ - sponsored by the infoDev project of the World Bank - a major resource, covering security for individuals and for organizations, government policy and IT security for technical administrators. Includes a chapter on government policy: http://www.infodev-security.net/handbook/part4.shtml

Other resources include:

- **ABA**. The American Bar Association's has compiled the International Guide to Combating Cyber Crime, the International Guide to Cyber Security, and the International Guide to Privacy, which are available online at http://www.abanet.org/scitech/computercrime/home.html

For more information, contact: Jim Dempsey, GIPI Policy Director, jdempsey@cdt.org