Fordham International Law Journal

Volume 22, *Issue* 5 1998 *Article* 2

International Dimensions of Crimes in Cyberspace

David Goldstone* Betty-Ellen Shave†

*

†

International Dimensions of Crimes in Cyberspace

David Goldstone and Betty-Ellen Shave

Abstract

Part I describes a few experiences with international computer hackers in order to provide a context for the rest of the Essay. Part II extracts from that experience the central issues that have arisen-and predictably will continue to arise-in connection with investigating and prosecuting international electronic crimes. These concerns are divided into three subject areas: the substantive law, the procedural law, and operational issues. Finally, Part III summarizes international efforts to address concerns raised by crimes in cyberspace.

INTERNATIONAL DIMENSIONS OF CRIMES IN CYBERSPACE

*David Goldstone**
*Betty-Ellen Shave***

CONTENTS

* Trial Attorney, Computer Crime and Intellectual Property Section Criminal Division, United States Department of Justice.

** Special Counsel for International Matters, Computer Crime and Intellectual Property Section Criminal Division, United States Department of Justice.

The authors would like to thank all the other members of the Department of Justice's Computer Crime and Intellectual Property Section, including specifically Scott Charney (Chief), Marty Stansell-Gamm (Principal Deputy Chief), David Green (Deputy Chief), Stevan Mitchell, Greg Schaffer, Michael Sussmann, and Marc Zwillinger, for their contributions to this Essay.

INTRODUCTION

With computer networks now spanning the globe, law and law enforcement agencies must address the international dimensions of crimes in cyberspace. Criminals in an electronic world can ignore international boundaries, since they can send information and execute commands via worldwide networks. Requiring no physical presence and facilitated by the presence of the Internet, electronic crimes are readily suited for international commission.[1]

U.S. law enforcement has already had substantial experience in fighting international computer crime—specifically, hackers. While computer hacking is one good example of an international crime in cyberspace, there are many other crimes that are facilitated by computer networks, such as forgery and counterfeiting, transmission of threats, fraud, copyright infringement, theft of trade secrets, transmission of child pornography, interception of communications, and transmission of harassing communications. The computer hacking cases have repeatedly raised issues that will be of concern in all international electronic crime cases.

---

1. Indeed, the U.S. Supreme Court has characterized the Internet as "an *international* network of interconnected computers." Reno v. ACLU, 117 S. Ct. 2329, 2334 (1997) (emphasis added).

Therefore, this Essay summarizes some of the lessons from those experiences and charts a future course. Part I describes a few experiences with international computer hackers in order to provide a context for the rest of the Essay. Part II extracts from that experience the central issues that have arisen—and predictably will continue to arise—in connection with investigating and prosecuting international electronic crimes. These concerns are divided into three subject areas: the substantive law, the procedural law, and operational issues. Finally, Part III summarizes international efforts to address concerns raised by crimes in cyberspace.

While the development of cyberspace offers much promise for international interaction and growth, it also facilitates the commission of international crime. By identifying the critical international issues relating to crimes in cyberspace and addressing them, countries can try to maintain for their citizens the same security in the information society that they have traditionally enjoyed.

I. *EXPERIENCES WITH INTERNATIONAL COMPUTER HACKERS*

U.S. law enforcement already has substantial experience with one kind of international electronic criminal—hackers.[2] Perhaps the most well-known example of international computer crime was described by Cliff Stoll in his book *The Cuckoo's Egg*.[3] In 1986, German hackers attacked computers operated by the Lawrence Berkeley Laboratory, in Berkeley, California. An investigation was initiated by graduate student Cliff Stoll, then working as a system administrator at the victim site. Federal law enforcement authorities initially showed no interest in the case in the absence of a clear monetary loss. Stoll launched his own investigation, however, which eventually led to the conviction of three hackers in Germany. The investigation revealed that the

2. One relatively early commentator observed that, because a hacker need not be physically present, "[c]omputer hacking is a crime unlike any other under international law." Robert J. Sciglimpaglia, Jr., Comment, *Computer Hacking: A Global Offense*, 3 PACE Y.B. INT'L L. 199, 245 n.265 (1991). The growth and widespread use of the Internet have taught that many kinds of electronic crimes, not just computer hacking, can be substantially facilitated by means of international computer networks. *See* Part II.A.1.

3. *See generally* CLIFF STOLL, THE CUCKOO'S EGG: TRACKING A SPY THROUGH THE MAZE OF COMPUTER ESPIONAGE (1989).

hackers used access to the Lawrence Berkeley computers to obtain access to many other U.S. computers. The hackers had obtained sensitive information—such as munitions information, information on weapons systems, and technical data—and then sold it to the KGB. This case demonstrated the importance of confidentiality of information on computer systems and the difficulty of determining a loss figure for a computer intrusion case at the beginning of an investigation.

Since the Cuckoo's Egg case, federal law enforcement has had experience with a variety of international computer crime cases. A review of some of those cases can provide a helpful context for considering the range of possible issues that can arise in a computer-oriented criminal investigation and prosecution.

A. *1993: Danish Hackers Attack Weather Computers*

In 1993, the National Weather Service in Maryland detected hacker activity in its systems. Since air traffic and shipping operations rely on National Weather Service data, this attack threatened to cause substantial damage. The intrusion was traced back to computers at the Massachusetts Institute of Technology ("MIT") and then back to Denmark. U.S. and Danish investigators identified thirty-two U.S. systems as well as systems in other countries, including Denmark, that hackers had penetrated. Danish authorities made seven arrests, including two juveniles. Six convictions resulted in Denmark, for attacks on both Danish and U.S. computer systems.[4]

B. *1994: Vladimir Levin's Bank Fraud from Russia*

Between June and October 1994, a theft ring headed by a computer hacker in St. Petersburg, Russia broke into a Citibank electronic money transfer system and attempted to steal more than US$10 million by making approximately forty wire transfers to accounts in Finland, Russia, Germany, the Netherlands, the United States, Israel, and Switzerland.[5] All of these transfers, except US$400,000, were recovered by Citibank.

---

4. *See, e.g.*, Jerry Seper, *4 Arrested in Denmark for Computer Hacker Scheme*, WASH. TIMES, Dec. 16, 1993, at A5, *cited in* Bradley S. Davis, Note, *It's Virus Season Again, Has Your Computer Been Vaccinated? A Survey of Computer Crime Legislation as a Response to Malevolent Software*, 72 WASH. U. L.Q. 411, 419 n.51 (1994).

5. *See, e.g.*, Dean Starkman, *Russian Hacker Enters Fraud Plea in Citicorp Case*, WALL ST. J., Jan. 26, 1998, at A6.

The leader, Vladimir Levin, was arrested in London, England, and successfully extradited to the United States two years later. In February 1998, Levin was sentenced to three years imprisonment and was ordered to pay US$240,000 in restitution to Citibank. Several accomplices have also been convicted.

C. *1995-1996: Julio Cesar Ardita's Intrusion from Argentina*

From August 1995 until February 1996, the Naval Criminal Investigative Service and the Federal Bureau of Investigation ("FBI") investigated a hacker who successfully obtained unauthorized access to multiple military, university, and other private computer systems, many of which contained sensitive research.[6] The hacker acquired unlimited access to those systems, including the ability to read the sensitive materials stored in them.

U.S. authorities tracked the hacker to Argentina and notified a local telecommunications carrier. The telecommunications company contacted local law enforcement, which began its own investigation. An Argentine investigating judge authorized the search of the hacker's apartment and the seizure of his computer equipment as the first step in an investigation of his potential criminal violations of Argentine law. The hacker was first identified to law enforcement by his user name "griton" (Spanish for "screamer") and eventually identified as Julio Cesar Ardita.

Ardita was investigated by the Argentineans for his intrusions into Argentine telecommunications systems, but Argentine law did not extend to cover his crimes against computers in the United States. For those crimes, only the United States could prosecute him. In the absence of an extradition treaty with Argentina for these offenses, Ardita eventually agreed, in May 1998, to come to the United States and plead guilty to felony charges of unlawfully intercepting communications and of damaging files on U.S. Department of Defense and NASA computers. He was fined US$5000 and sentenced to three years of probation.[7]

---

6. This case thus stands in contrast to the Danish case described above, *see supra* note 4 and accompanying text, where Denmark was able to prosecute for attacks on victims in the United States, and additional U.S. prosecution was therefore unnecessary.

7. *See, e.g.*, Pamela Ferdinand, *Argentine Pleads Guilty to Hacking U.S. Networks; Wiretap Led Authorities to Arrest*, WASH. POST, May 20, 1998, at A23; *Argentine Hacker who Invaded Pentagon Enters Guilty Plea*, WALL ST. J., Dec. 8, 1997, at B10.

D. *1996: Florida 911 Attack from Sweden*

In February 1996, the FBI investigated suspicious phone calls placed to the Northern Florida Emergency 911 system. The hacker had been able to obtain direct telephone numbers that corresponded to the lines used to receive 911 calls for eleven counties. He used them to tie up emergency lines and harass operators. A trace initiated by one affected phone company identified a potential suspect in Sweden. Swedish authorities, cooperating with the Washington Field Office of the FBI, executed a search warrant on the residence of the subject, who turned out to be a minor. The hacker was convicted of a misdemeanor in Sweden and given a suspended sentence.[8]

E. *1996: Miami Internet Service Provider Takeover from Germany*

In July 1996, a hacker gained complete control over an Internet Service Provider in Miami, Florida and captured credit card information of the service's subscribers.[9] He threatened to destroy the system and distribute the credit card numbers unless the victim provider paid US$30,000. Following investigation by the U.S. Secret Service, German authorities arrested the hacker, Andy Hendrata, when he tried to pick up the money at a post office box. A twenty-seven-year old Indonesian computer science student, Hendrata was prosecuted and convicted in Germany. He was given a one-year suspended sentence and a US$1500 fine.

F. *1998: Ehud "The Analyzer" Tenebaum's Pentagon Penetration from Israel*

On March 18, 1998, the Israeli National Police arrested Ehud "The Analyzer" Tenenbaum, an Israeli citizen, for illegally accessing computers belonging to the Israeli and U.S. governments, as well as hundreds of other commercial and educational systems in the United States and elsewhere.[10] The arrest of Tenenbaum led to several weeks of investigation into a series of

---

8. *See, e.g.*, *911 Lines Tied Up by Hacker - In Sweden*, ORLANDO SENTINEL, Mar. 8, 1997, at D4.

9. *See, e.g.*, Matthew McAllester, *Feds Aid Miami Company in Global Hunt for Hacker*, NEWSDAY, June 8, 1997, at A41.

10. *See, e.g.*, *Israeli Teenager Questioned in Pentagon Hacking Case*, L.A. TIMES, Mar. 19, 1998, at A4.

computer intrusions into U.S. military systems that occurred in February 1998. As part of this investigation, the U.S. Department of Justice formally requested legal assistance from the Israeli Ministry of Justice, and U.S. law enforcement agents traveled to Israel to present Israeli law enforcement officials with evidence. As part of this evidence, U.S. investigators also presented the Israelis with evidence of Tenenbaum crimes against Israeli computer systems.

On February 9, 1999, Tenenbaum was indicted by an Israeli court, along with four accomplices. They were charged with illegal entry into computers in the United States and Israel, including U.S. and Israeli academic institutions and the Israeli Parliament.[11] Further action in this case is pending.

II. *ISSUES RAISED BY INTERNATIONAL COMPUTER CRIME*

As noted above, the explosive growth of the Internet worldwide has accelerated the ability of people to commit crime internationally by means of computers. While the Internet knows no borders, criminal law and law enforcement agencies are constrained by the limits of their authority. Those limits are usually reached at national borders.

While limitations related to national sovereignty are often described as "jurisdictional," these jurisdictional limitations arise in many different forms. Substantive laws may apply to domestic activity only, and even if they are given extra-territorial effect, cooperation from a foreign country is more likely with regard to activity that violates its domestic law. While some countries, such as Denmark, Israel, and Sweden,[12] may prosecute criminals for attacks on foreign victims, other countries may be limited by their legal authority to do so, as Argentina was in the Ardita case.[13] Procedural laws, such as those provisions that permit tracing of telephone calls or other communications, have clear jurisdiction over domestic processes only. At the operational level, law enforcement agents are primarily stationed and have jurisdiction to investigate crime domestically. A single electronic crime case, however, can often raise a comprehensive set of international issues.

---

11. *See, e.g., Israel Indicts Hackers*, PITTSBURGH POST-GAZETTE, Feb. 10, 1999, at A4.
12. *See supra* notes 4, 10, 8, and accompanying text.
13. *See supra* note 7 and accompanying text.

Thus, problems created by the ease of commission of international electronic crimes are exacerbated by a variety of "jurisdictional" constraints on law enforcement in protecting the public against such crime. This confluence facilitates and indeed invites commission of international crime because of the reduced risk of penalty. Commentators (and criminals, who freely discuss such matters on the Internet) have already recognized the ability to exploit safe havens. These safe havens may be used for a variety of purposes, such as:

- using foreign anonymous remailers to facilitate copyright infringement or to transmit harassing messages or child pornography;[14]
- operating gambling Web sites in countries friendly to such activity;[15] or
- hacking through computers in jurisdictions lacking an effective law enforcement presence before attacking an intended victim system in yet another country.

These concerns demand a coherent response from the public agencies that are charged with protecting public safety by enforcement of the criminal laws. In considering how to combat such international crimes, it is helpful to catalogue the kinds of novel legal problems raised for law enforcement: the substantive issues, the procedural issues, and the practical issues. Their cumulative effect is to make the task of fighting computer crime more difficult.

A. *Substantive Law*

1. Absence of Substantive Laws

As mentioned above, the United States has a wide variety of laws that prohibit crimes facilitated by computer networks. These laws prohibit forgery and counterfeiting, transmission of threats, computer hacking, fraud, copyright infringement, theft of trade secrets, transmission of child pornography, interception of communications, and transmission of harassing communications.[16]

---

14. *See, e.g.*, Jonathan I. Edelstein, Note, *Anonymity and International Law Enforcement in Cyberspace*, 7 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 231, 249-51 (1996).

15. *See, e.g.*, John Edmund Hogan, Comment, *World Wide Wager: The Feasibility of Internet Gambling Regulation*, 8 SETON HALL CONST. L.J. 815, 845 n.149, 853 n.179 (1998).

16. *See, e.g.*, 18 U.S.C. §§ 470-514 (1994 & Supp. 1997) (counterfeiting and for-

Even in the United States, some of these laws are of relatively recent vintage. For example, the last fifteen years have brought about a substantial development of the criminal law of intellectual property in the United States.[17] U.S. Congress first criminalized trademark counterfeiting in 1984,[18] and the federal law criminalizing theft of trade secrets was just enacted on October 11, 1996.[19] While infringement of copyright has been a crime, in certain cases, since 1909,[20] Congress has in recent years broadened the scope of federal copyright protection and enhanced criminal penalties, and, most recently, on December 16, 1997, President Clinton signed into law the No Electronic Theft Act ("NET Act").[21] The NET Act permits prosecution in cases involving large-scale illegal reproduction or distribution of copyrighted works where the infringers act willfully but without a discernible profit motive.

For electronic violations that occur in countries where no similar laws have been enacted, the crime may not be

---

gery); 18 U.S.C. § 844(e) (1994 & Supp. 1997) (threats to property and individuals); 18 U.S.C. § 875(c) (1994) (threats to injure individuals); 18 U.S.C. § 1029 (1994 & Supp. 1997) (access device fraud); 18 U.S.C. § 1030 (1994 & Supp. 1997) (computer fraud and abuse); 18 U.S.C. § 1343 (1994) (wire fraud); 18 U.S.C. § 1362 (1994 & Supp. 1997) (interference with communications systems); 18 U.S.C. § 1832 (1994 & Supp. 1997) (theft of trade secrets); 18 U.S.C. 2252A (Supp. 1997) (child pornography); 18 U.S.C. § 2319 (1994 & Supp. 1997) (copyright infringement); 18 U.S.C. § 2320 (1994 & Supp. 1997) (trafficking in counterfeit goods or services); 18 U.S.C. § 2511 (1994 & Supp. 1997) (interception of communications); 47 U.S.C. § 223 (1994 & Supp. 1997) (transmission of harassing and obscene communications).

17. *See generally* Computer Crime and Intellectual Property Section, Department of Justice, *Federal Guidelines for Prosecution of Violations of Intellectual Property Rights (Copyrights, Trademarks and Trade Secrets)* (1997) (visited Apr. 14, 1999) <http://www.usdoj.gov/criminal/cybercrime/ip.html> (on file with the *Fordham International Law Journal*).

18. *See* Trademark Counterfeiting Act of 1984, Pub. L. No. 98-473, 98 Stat. 2178 (codified as amended at 18 U.S.C. § 2320). For additional discussion of the crime of trademark counterfeiting, see David J. Goldstone & Peter J. Toren, *The Criminalization of Trademark Counterfeiting*, 31 CONN. L. REV. 1 (1998).

19. *See* Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3489 (codified at 18 U.S.C. §§ 1831-1839). For additional discussion of the Economic Espionage Act of 1996, see James H.A. Pooley et al., *Understanding the Economic Espionage Act of 1996*, 5 TEX. INTELL. PROP. L.J. 177 (1997).

20. *See* Act of March 4, 1909, ch. 28, 35 Stat. 1082.

21. No Electronic Theft Act, Pub. L. No. 105-147, 111 Stat. 2678 (1997) (codified at 17 U.S.C. §§ 101, 506, 507, 18 U.S.C. §§ 2319, 2319A, 2320); *cf.* United States v. LaMacchia, 871 F. Supp. 535 (D. Mass. 1994) (dismissing criminal indictment, prior to passage of No Electronic Theft Act, for large-scale not-for-profit copyright infringement).

prosecutable. Indeed, with the United States at the forefront of the so-called "information age," it makes sense that Congress adapts federal law to technological development far earlier than the legislatures of some foreign countries. Some countries do not value protecting intellectual property rights as much as the United States does. Thus, it is possible that large-scale violations of U.S. copyright could take place in a foreign country without any prosecutable crime arising under that country's laws.

2. Extraterritorial Reach of Substantive Laws

A criminal can easily perpetrate an electronic crime against a victim in a country without ever setting foot there. Applying the domestic law of a country whose citizen or resident is victimized against a non-national perpetrator who has never even visited the country and may not even have known where his victim was located raises questions about the extra-territorial reach of domestic laws. International law can permit extraterritorial reach of criminal law under an "effects test"—where the non-national has engaged in extraterritorial conduct with the intention or the likelihood that it will have effects in the country whose law is to be applied, or, possibly, where a crime is committed against a nation's citizens.[22] Whether extra-territorial reach of a nation's substantive law is permitted can depend on the particular law at issue, the particular nation's jurisprudence, and most importantly, the particular facts of the case.[23] While some countries, such as Denmark, Israel, and Sweden,[24] may prosecute criminals for attacks on foreign victims, other countries may be limited by their legal authority to do so, as Argentina was in the Ardita case.[25]

3. Dual Criminality

When international legal assistance, such as extradition, is sought, it is not necessarily sufficient that a victim country's laws criminalize the conduct at issue, even if they are capable of extra-territorial application. Rather, it is frequently necessary for

22. *See* Henry H. Perritt, *Jurisdiction in Cyberspace*, 41 VILL. L. REV. 1, 51-54 (1996).

23. For example, the United Kingdom's computer misuse act provides for broad jurisdiction over crimes that take place on computer networks in the United Kingdom. Computer Misuse Act, 1990, ch. 18, §§ 4-9 (Eng.).

24. *See supra* text accompanying notes 4, 8, 10, & 11.

25. *See supra* note 7 and accompanying text.

the investigation that the substantive law of the other country where investigative support is sought criminalizes the conduct at issue in their own laws. Such parallelism is called "dual criminality" (or "double criminality"). Unless the dual criminality requirement is fulfilled, a nation may be unwilling to extradite an individual to the victim country if the act was not a crime domestically, or may be unwilling to execute searches or to take other investigative steps essential to effective law enforcement.

For example, until recently, computer crime has not received the emphasis that other international crimes have engendered. Even now, not all affected nations recognize the threat that computer crime poses to public safety or the need for international cooperation to respond effectively to the problem. Consequently, many countries have weak laws, or no laws, against computer hacking, and they may decline to assist other countries on the basis of lack of dual criminality.[26]

4. Variation Among Substantive Laws

Even if relevant substantive laws have been enacted in all of the jurisdictions where a person perpetrates electronic crime, the precise scope and application of those laws can be as complex as the underlying technology. Since the substantive laws are sure to vary, the "dual criminality" requirement discussed above is not necessarily satisfied by dual enactment of relevant criminal provisions. Those laws must incorporate the precise crime particularly at issue. For example, even if two countries have criminal copyright infringement laws, copyright infringement without a commercial motive may be a crime in one country[27] but not in another.

The complexity and rapid development of technology can give rise to complex or evolving laws that govern electronic crimes. For example, the primary U.S. computer crime statute, 18 U.S.C. § 1030, has undergone six revisions since it was enacted in 1984.[28] The statute now embodies a specific set of U.S.

---

26. *See* Scott Charney & Kent Alexander, *Computer Crime*, 45 EMORY L.J. 931, 949 (1996).

27. *See, e.g.*, 17 U.S.C. § 506(a)(2) (Supp. 1997).

28. Pub. L. No. 98-473, 98 Stat. 2190. The statute was amended in 1986, Pub. L. No. 99-474, 100 Stat. 1213; 1988, Pub. L. No. 100-690, 102 Stat. 4404; 1989, Pub. L. No. 101-73, 103 Stat. 502; 1990, Pub. L. No. 101-647, 104 Stat. 4831, 4910, 4925; 1994, Pub.

concerns.[29] Electronic crime statutes from various countries are, of course, subject to their own evolution.[30] Consequently, it is predictable that such laws will differ in their scope.

5. Conflicts Among Substantive Laws

Substantive criminal law may actually conflict between various countries. What is criminal activity in one country may be specifically protected in another. While such differences arise without the involvement of computers, the often-recognized tendency of computer networks to make the world seem "smaller" can exacerbate these differences and bring them into conflict. One example of this dilemma arises with regard to so-called "hate speech." Such speech is banned in many countries, particularly in Europe. Yet, the same hate speech in many instances is not only *not criminal* in the United States, but it is protected by the First Amendment to the U.S. Constitution.[31] Thus, for the United States, law enforcement cooperation with other countries' investigations of hate speech cases can raise constitutional concerns.[32]

B. *Procedural Law*

Investigators in computer crime cases rely heavily on communications providers to provide information regarding both computer connections and content. This information is often provided only in response to court orders issued pursuant to es-

---

L. No. 103-322, 108 Stat. 2097-2099; and 1996, Pub. L. No. 104-294, 110 Stat. 3491, 3508.

29. *See, e.g.*, Charney & Alexander, *supra* note 26, at 931-50.

30. For example, Malaysia recently enacted a substantive computer crime law that has been praised as a testament to both "the danger posed by those who use high technology as a tool and a target of crime" and "the seriousness with which the Malaysian government is taking this threat," but it may be in need of "fine-tuning." Donna L. Beatty, Comment, *Malaysia's "Computer Crimes Act 1997" Gets Tough on Cybercrime but Fails To Advance the Development of Cyberlaws*, 7 PAC. RIM L. & POL'Y J. 351, 375 (1998).

31. U.S. CONST. amend. I; *see, e.g.*, National Socialist Party of America v. Village of Skokie, 432 U.S. 43 (1977) (per curiam) (requiring procedural safeguards for state rule that barred Nazis from displaying swastika).

32. *See* John T. Soma et al., *Transnational Extradition for Computer Crimes: Are New Treaties and Laws Needed?*, 34 HARV. J. ON LEGIS. 317, 343-45 (1997) (describing extradition of U.S. citizen Gary Lauck from Denmark to Germany for violating German anti-Nazi criminal laws by "distributing illegal propaganda and Nazi symbols, incitement, encouraging racial hatred and belonging to a criminal group" (quoting *American Neo-Nazi Arrested in Europe*, CHI. TRIB., Mar. 24, 1995, at 3)).

tablished criminal procedures. Such court orders can give law enforcement the ability to search stored data, to access electronic mail, to trace the source and destination of communications, and to intercept communications in real time. Procedures to obtain information, and procedural safeguards to restrict access to information, are not available in computer cases in some countries, and such processes may vary from country to country.[33] On the other hand, procedures to obtain information domestically may incidentally result in transborder searches with international implications. One final procedural concern is that the availability of a means, such as extradition, to obtain a meaningful remedy may not be a real possibility.

1. Absence of Procedural Laws

A detailed framework of procedural laws can be valuable to investigations, create powers and limits, and provide clear guidance for collection of evidence by law enforcement agents. In addition, they can ensure for the public both an appropriate level of protection against unwarranted government intrusion and an expectation of regularity in government action. For example, the United States has a relatively detailed statutory scheme governing law enforcement access to stored wire and electronic communications.[34] This complicated statute provides direct guidance in investigations relating to any crimes where such data is stored in the hands of third parties. Many other countries do not have such a detailed framework or statement of legislative intent.

One valuable subsection of the United States' statute provides for preservation of data, upon government request, until the government obtains appropriate process for access to that data.[35] This ability to freeze data is essential to law enforcement in investigating many computer crime cases domestically. Yet, most other countries have no such ability to preserve data upon request pending issuance of process.

Another important procedural issue that many countries

---

33. Justice Frankfurter once observed that "[t]he history of liberty has largely been the history of observance of procedural safeguards." McNabb v. United States, 318 U.S. 332, 347 (1943). A forward-looking Justice Frankfurter might suggest that the future of liberty will be the future of the observance of procedural safeguards in computer cases.

34. *See* 18 U.S.C. § 2703 (1994 & Supp. 1997).

35. *See id.* § 2703(f).

have begun to address arises from the increased use of encryption products. The widespread use of strong encryption raises the possibility of limiting the ability of the law enforcement to protect public safety by collecting evidence as part of a legally authorized search or surveillance. International efforts regarding encryption policies are discussed below.[36]

2. Variation of Procedural Laws

The differences in national procedural laws can substantially impede investigation of a computer crime case. These differences arise due to differences in national policy or history, and idiosyncrasies related to the history of the laws governing procedure, among other reasons. For example, whereas certain evidence or certifications may be necessary in one country to obtain an order to trace a telephone call, entirely different showings may be required in another country.[37] Obtaining the necessary information to procure a foreign court order to trace a transmission may be a daunting task if domestic authorities do not know what information will be needed in a foreign court.

3. Conflict of Procedural Laws

The variation among procedural laws can be exacerbated by direct conflicts among the procedural laws of different countries. This problem is best exemplified by the scenario presented in *In re Grand Jury Proceedings (United States v. Bank of Nova Scotia)*, where a Canadian bank was held in civil contempt for failing to comply with an order enforcing a grand jury subpoena duces tecum notwithstanding the fact that compliance with the subpoena would have required the bank to violate a Bahamian bank secrecy rule.[38] As more companies take advantage of computer networks to operate internationally, those companies increasingly become subject to the laws of multiple nations. As more investigations of crime committed over those networks are conducted—and as the laws regulating privacy of electronic data evolve—more conflicts are sure to arise.

Such conflicts could be of constitutional moment. For ex-

---

36. *See* Part III.C.

37. *See, e.g.*, 18 U.S.C. § 3123 (1994).

38. In re Grand Jury Proceedings (United States v. Bank of Nova Scotia), 691 F.2d 1384 (11th Cir. 1982), *cert. denied*, 462 U.S. 1119 (1983).

ample, the laws of some countries might provide a process for compelled oral production of an unrecorded password that can be used to decrypt data. In the United States, however, such compulsion may implicate the Fifth Amendment's privilege against self-incrimination.[39] Therefore, compulsion of an unrecorded password may not be a reliable process for U.S. law enforcement to access plaintext of encrypted data, while other countries may safely presume the legality of such compulsion when designing their procedures.

4. Transborder Searches

Procedures to obtain information domestically may incidentally have international implications. For example, a search of computer data on a domestic branch of a foreign corporation may be authorized pursuant to a search warrant. Upon executing the search, however, the law enforcement officers may discover that the data is actually stored on a file server in the home country of the corporate headquarters (or some other country). The foreign search might also take place without the officers' recognizing that the data is stored abroad. Either way, investigations of international electronic crime can give rise to unusual questions of national sovereignty without a law enforcement agent's ever leaving his or her home country's soil. It may be legitimate and important for law enforcement to be allowed to conduct a remote search of computers in a foreign country. At present, there is no way to know how often such searches take place, and the laws governing them are patchy and conflicting. These issues are discussed further below, in relation to the work of the G-8.[40]

5. Remedy Issues

An investigation that uncovers substantial crime in a "victim country" and successfully identifies a perpetrator in a foreign country may nevertheless be subject to certain limits. For example, a home country may be unwilling or unable to extradite its national for many crimes, particularly since there is substantial

39. Philip R. Reitinger, *Compelled Production of Plaintext and Keys*, 1996 U. CHI. LEGAL F. 171, 203-05 (1996).

40. *See* Part III.A. The G-8 is made up of Canada, France, Germany, Italy, Japan, Russia, the United Kingdom, and the United States.

variation regarding enforcement and punishment of electronic crimes.[41] Even if a country is willing to extradite a criminal, it can extradite him or her to only one country at a time. This is problematic since a criminal in cyberspace could have committed crimes in many countries without leaving his or her home country.

As an alternative to extradition, a home country may have the option of prosecuting the perpetrator. This process, however, may not, particularly in a criminal case, vindicate the rights of the victim country to prosecute and punish the wrongdoer. Victim countries have legitimate interests to prosecute crimes against the State, crimes that take place within their borders, and crimes upon their citizens. Yet, a home country may not be empowered to prosecute wholly foreign, albeit related, crimes. Moreover, the home country may not be inclined to devote the same commitment of time and resources to that prosecution as the victim country would have. Indeed, if the home country can identify no crime actually committed by the wrongdoer in his or her own country, it may not be willing or able to prosecute him or her at all.[42]

C. *Operational Issues*

In addition to the formal concerns related to substantive laws and procedural laws, international computer crime investigations are hampered by a variety of operational issues. Among these concerns are expertise and coordination, communication, and timeliness.

Each of these aggravates the others. The time spent finding and informing the technically literate law enforcement personnel in a foreign country who are authorized to address the crime under investigation makes it more difficult for law enforcement to combat crime quickly. The technical nature of the subject heightens the potential for problems arising because of language barriers. And those language barriers can further slow law enforcement response to computer crime. Indeed, differences in language, culture, and national interests create situations ripe for misunderstandings to arise. For all of these reasons, opera-

41. *See* Soma et al., *supra* note 32, at 333, 369 (observing that extradition is as much product of diplomacy and foreign relations as it is mechanism created by treaty).

42. For a fuller discussion of closely related issues, see Part II.A.2.

tional issues are among the most intractable that arise in the course of an international computer crime case.

1. Expertise and Coordination

Electronic crime investigations require specialized training and experience on the part of law enforcement agents and prosecutors, as well as substantial computer equipment and resources. In the United States and in numerous other developed countries, the need for such training and resources has been recognized for some time.[43] Elsewhere, comparatively fewer law enforcement agents and prosecutors are trained to address such crimes.[44] In certain cases, it may be crucial to find the law enforcement personnel in another country who have been trained or who have experience in computer cases. Without well-developed coordination, this task can be difficult.

2. Communication

Communication is essential to cooperative electronic crime investigations. Law enforcement agents, however, can be stymied by language barriers and time differences that do not necessarily deter criminals in cyberspace. The common language of the Internet is English (and, to a lesser extent, Unix), and networked computers are often in operation twenty-four hours a day, seven days a week. With the Internet, instantaneous access can be achieved with ease regardless of the target computer's locale. Thus, a criminal from an English-speaking country could easily commit a crime on a victim in a Spanish-speak-

---

43. For example, at the Federal Bureau of Investigation ("FBI"), data forensics (i.e., extracting information from computers) is coordinated by the Computer Analysis and Response Team ("CART"), which is headquartered in Washington, with trained agents in offices nationwide. Similarly, for computer intrusion cases, FBI efforts are coordinated by the National Infrastructure Protection Center ("NIPC"). *See* <http://www.nipc.gov> (visited Apr. 14, 1999). On the prosecution side, these efforts are coordinated in Washington D.C. by the Department of Justice's Computer Crime and Intellectual Property Section ("CCIPS") and throughout the country by Assistant United States Attorneys designated as Computer-Telecommunications Coordinators ("CTCs"). *See* <http://www.usdoj.gov/criminal/cybercrime> (visited Apr. 14, 1999).

44. Law enforcement personnel have sometimes been criticized for being insufficiently attentive to computer crime. *See* Marc D. Goodman, *Why the Police Don't Care About Computer Crime*, 10 HARV. J.L. & TECH. 465, 489 (1997). While the U.S. Department of Justice has been actively working in this area since the 1991 Computer Crime Initiative, increasing levels of computer crime will require even more training and resources. *Id.* at 493-94.

ing, Chinese-speaking, or Hebrew-speaking country (or vice-versa) located on the other side of the world.[45] For law enforcement agents to respond to such an attack effectively would require communication among people of two or more different languages at odd hours. Many countries are not yet well-equipped to meet this challenge.

3. Timeliness

To say that an electronic criminal can commit crimes around the world in the time that it takes to blink an eye is not an exaggeration. Law enforcement must attempt to respond promptly. Indeed, criminals in cyberspace can commit multiple crimes all over the world simultaneously. Yet, computer logs are often routinely erased within a week on many systems or are never kept at all.

In traditional physical-world crimes, law enforcement is not often asked to respond to a public safety threat of such exigency. Indeed, one commentator has observed that computer crime requires law enforcement to be coordinated at a speed and to a degree never before maintained "[o]r even envisione[d]."[46] Law enforcement specialists are not necessarily available twenty-four hours a day. Moreover, legal requirements, such as those for the issuance of a search warrant, and law enforcement policies are not designed to galvanize an immediate law enforcement investigation. Investigations of international cases, which can sometimes move at the speed of the slowest country, are particularly prone to delay.

III. *JUSTICE DEPARTMENT EFFORTS TO ADDRESS INTERNATIONAL ELECTRONIC CRIME CONCERNS*

Both individual nations and multinational organizations have been actively addressing the international electronic crime concerns outlined above.[47] The Justice Department has pursued

45. Of course, if the files on a computer are maintained in a language other than English, that language barrier may act as a deterrent to foreign attackers who would like access to the contents of those files.

46. Stephen P. Heymann, *Legislating Computer Crime*, 34 HARV. J. ON LEGIS. 373, 390 (1997).

47. Commentators have long observed that countries "must . . . foster international cooperation." Steve Shackelford, *Computer-Related Crime: An International Problem in Need of an International Solution*, 27 TEX. INT'L L.J. 479, 503 (1992).

formal multilateral initiatives in many fora, such as the G-8, the Council of Europe (or "COE"), and the Organization for Economic Co-operation and Development (or "OECD"). The Justice Department efforts through these formal processes are described in detail below.[48]

Important international efforts have taken place in other fora, such as at the United Nations.[49] In fact, the United Nations is planning to increase awareness of electronic crime issues by sponsoring a workshop on "Crimes Related to the Computer Network" at the Tenth United Congress on Crime Prevention and the Treatment of Offenders scheduled to be held in Vienna in April 2000.[50] At the request of the Centre for International Crime Prevention in Vienna, the United Nations Asia Far Eastern Institute ("UNAFEI") assumed responsibility for coordinating the workshop. In October 1998, UNAFEI hosted an experts meeting in Fuchu, Tokyo to begin preparations for this workshop. The group of experts, including representatives from Australia, Canada, India, the Netherlands, Japan, Korea, South Africa, and the United States, is planning a workshop program that will demonstrate the legal and technical difficulties of tracking criminal activities over computer networks, as well as the problems associated with searching and seizing evidence stored on computer networks. The Department of Justice has attended planning meetings on behalf of the United States in this effort.

---

48. Many commentators have discussed the ability of nation-states to "regulate" cyberspace and their likelihood to do so. *See, e.g.*, Edelstein, *supra* note 14, at 286 (describing international convention as "the ultimate solution"); *see also* Hogan, *supra* note 14, at 852 (describing international convention on Internet gambling as "undoubtedly . . . the most appealing solution" and favorably citing conventions of World Intellectual Property Organization ("WIPO") dealing with proprietary rights). One commentator has noted that it can be useful "to think of the Internet less as a place and more as a regime of transnational norms and rules (a logical counterpart to transnational law) that regulates international interactions between individuals." Timothy S. Wu, Note, *Cyberspace Sovereignty? The Internet and the International System*, 10 HARV. J.L. & TECH. 647, 663 (1997).

49. For example, the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders adopted a resolution in 1990, U.N. Secretariat, Report of the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, U.N. Doc. A/CONF.144/28/Rev.1 at 140, U.N. Sales No. E.91.IV.2 (1991), and the United Nations published a Manual on the Prevention and Control of Computer-Related Crime in 1994, U.N. Ctr. for Soc. Dev. & Humanitarian Aff., U.N. Manual on the Prevention and Control of Computer Related Crime, U.N. Doc. ST/ESA/SER.M/43-44, U.N. Sales No. E.94.IV.5 (1994).

50. *See* United Nations General Assembly resolution 1997/52 of December 1997.

In addition to these multilateral processes, U.S. law enforcement has actively developed the informal relationships that are essential to effective cooperation and that help breathe life into the formal arrangements. One of the aims of a March 1997 International Computer Crime Conference in New York City, hosted by the Computer Crime Squad in the FBI's New York field office, was to make possible international informal contacts.[51] Twenty-nine foreign nations sent representatives to the conference, which provided an overview of computer crime issues and cases and allowed countries to discuss their various approaches to computer crimes. U.S. law enforcement staff have established relationships with numerous knowledgeable foreign law enforcement personnel.

A. *G-8*

In October 1996, the G-8's Senior Experts' Group on Transnational Organized Crime, meeting in Lyon, France, adopted a proposal to create a subgroup to focus specifically on international electronic crime issues. This subgroup met for the first time in Chantilly, Virginia, in January 1997. The G-8 is an excellent forum for such an effort because it is small enough to make meaningful discussions possible while including representatives from some of the most technologically advanced nations that are most susceptible to electronic crimes.

During 1997, the United States held the presidency of the G-8 and hosted the summit of G-8 heads of state in Denver, Colorado, in June of that year. At that summit, the heads of state jointly asked their countries to work together in addressing electronic crime issues. In an effort to address that request, the Attorney General of the United States convened a meeting of Justice and Interior Ministers from the countries that make up the G-8 in Washington, on December 9-10, 1997. One outgrowth of the meeting and of the Subgroup's work was that the Ministers adopted a communiqué that contained ten principles and ten action items relating to high-tech crime.[52]

The Subgroup worked on numerous issues in 1998, focusing in particular on three items. The first of these items was

---

51. *See, e.g.*, Pat Milton, *FBI Director Calls for Effort to Fight Growing Danger of Computer Crime*, ASSOCIATED PRESS, Mar. 4, 1997.

52. The communiqué can be found in Appendix A.

transborder computer searches in networked systems by law enforcement.[53] Rapid transborder searches may be crucial to protect public safety, privacy, and human rights in stalking, sexual abuse, kidnapping, extortion, terrorism, and other cases. (The fact that a communication is stored in another country has no necessary connection to whether one person is physically close enough to do another harm). Moreover, it is frequently difficult or impossible for law enforcement, acting with proper domestic legal authority, to discern when it has crossed a country's border electronically. Yet to permit such searches on a wholesale basis would undermine those same values of public safety, privacy, and human rights. The Subgroup has been discussing all possibilities, including prohibiting, permitting, or regularizing such searches (such as by restricting them to use in controlled and limited circumstances).

Second, the Subgroup fully implemented a network among the G-8 countries of twenty-four hour emergency contacts for investigating crimes involving electronic evidence, which would include hacker attacks on the nation's critical infrastructure. That network was used repeatedly in 1998 and investigators are becoming familiar with its use. The Subgroup is in the process of inviting other countries to join this emergency network and anticipates its continual expansion.

Third, the Subgroup spent a substantial amount of time talking with telecommunications and Internet service providers to ensure that the governments understand industry trends and provider needs and aims. As an initial response to those discussions, the Subgroup expects to set up an emergency contact network between government and industry. Also, it is standardizing the forms by which governments request information from providers. This government-industry liaison will continue.

In November 1998, the United States organized and hosted the first G-8 training conference. This five-day conference, well-received by the attendees, brought together high-tech investigators from all of the G-8 countries and from the European Union and Council of Europe to discuss, in technical terms, operational aspects of investigating cases in an electronic environment. Because of the conference's success, two technical training sessions will be held in 1999.

---

53. *See* Part II.B.4.

B. *Council of Europe*

A second significant multilateral effort involves the Council of Europe, which has long been an active forum for computer crime issues. In 1989, the COE issued a seminal paper on the substantive law of computer-related crime.[54] This document contained a "Minimal List" describing conduct that COE countries should criminalize and an "Optional List," which included activity that some countries might wish to criminalize. The result of this effort was a spate of new computer crime laws throughout Europe.

Following this effort, the COE convened another group of experts to address procedural issues raised by crimes against information technology. The United States is not a member of the Council of Europe, but participated as an official observer and was represented by the Justice Department. This meeting resulted in sweeping procedural recommendations on such matters as tracing the source and destination of communications, transborder searches in networked systems, mutual legal assistance, and other topics, all geared to providing swifter international cooperation in high-tech cases.[55]

In early 1997, the Council of Europe's European Committee on Crime Problems ("CDPC") established a committee to continue its study of high-tech issues. Under the terms of reference (i.e., the charter), the committee has been charged with drafting a convention focusing on cyberspace offenses, transborder searches, international cooperation, and other issues.

The committee's initial meeting was held in April 1997. Member countries and various observer countries, including the United States, participated in the sessions. The Justice Department represented the United States in this committee as well. Some of the subjects being studied by the committee are acts against the confidentiality, integrity, or availability of information systems that should be criminalized by all signatories; jurisdiction; a limited intellectual property section; a limited child pornography section; transborder searches of networked computers; more rapid exchange of telecommunications source and

54. Council of Europe, Computer-Related Crime, Recommendation No. R (89) 9.

55. Council of Europe, Criminal Procedural Law in Information Technology Cases, Recommendation No. R (95) 13. Recommendation No. (95) 13 can be found in Appendix B.

destination information; undercover operations; wiretaps; a network of emergency contacts; and mutual legal assistance. The committee is expected to complete its draft of a "Cyber-Crime Convention" by the end of 1999.

This Cyber-Crime Convention will have the full effect of a multilateral treaty among the ratifying nations and, as such, will have the force of law. There is a large set of potential signatory nations. First, as with any Council of Europe Convention, all of the member European nations may sign on to the Convention. Moreover, the observer states that have participated in drafting the Cyber-Crime Convention, such as Canada, Japan, and the United States, may also sign on.[56] Eventually, even non-observing nations may be permitted by the Council of Europe to enter into the Cyber-Crime Convention. With such a large pool of potential signatory nations, the reciprocal ramifications of the Cyber-Crime Convention must be carefully considered before they are adopted.

C. *Organization for Economic Co-operation and Development*

The OECD has long been in the forefront of developing policy approaches to address cybercrime. The OECD initiated the first multinational effort to address the flaws in existing criminal laws with regard to computer crimes. In 1986, the OECD suggested a common approach based on an analysis of the substantive law of member states.[57] In 1992, the OECD developed Guidelines for the Security of Information Systems.[58]

More recently, the OECD entered the highly contested area of cryptography policy. This policy area is of great interest to the Justice Department. The Justice Department believes that the use of strong cryptography is critical to the development of the Global Information Infrastructure ("GII"). Communications and data must be protected "both in transit and in storage" if the GII is to be used for personal communications, financial transactions, medical care, the development of new intellectual property, and other applications. The widespread use of unrecover-

56. For the United States, entering into the Cyber-Crime Convention would require Senate ratification.

57. Organization for Economic Co-operation and Dev., Computer-Related Crime: Analysis of Legal Policy (1986).

58. *See* Organization for Economic Co-operation and Dev., Guidelines for the Security of Information Systems (1992).

able encryption by criminals, however, poses a serious risk to public safety. Encryption may be used by terrorist groups, drug cartels, foreign intelligence agents, and other criminals to secure their data and communications, thus nullifying the effectiveness of search warrants and wiretap orders. The Justice Department's goal "and the Clinton Administration's policy" is to promote the development and use of strong encryption that enhances the privacy of communications and stored data, while also preserving law enforcement's current ability to gain access to evidence as part of a legally authorized search or surveillance.[59]

The export of encryption products is currently regulated under U.S. law.[60] The United States does not control the domestic use of encryption products. Because of the growth of international markets for computer software, and the ease with which computer software can be disseminated, it is important for countries concerned about the widespread use of unrecoverable encryption to coordinate national policies. Indeed, export controls of various nations have been coordinated internationally since World War II through an agreement that is now known as the Wassenaar Agreement.[61]

The OECD began work on cryptography policy formally in early 1996. The effort was taken up under the auspices of the OECD's Information, Computers, and Communication Policy, which established an Ad Hoc Group of Experts on Cryptography Policy Guidelines ("Ad Hoc Group"). This group was charged with drafting Guidelines for Cryptography Policy ("Guidelines") to identify the issues that should be taken into consideration in the formulation of cryptography policies at the national and international levels. The Ad Hoc Group was chaired by a member of the Attorney General's Department of Australia. Since the

---

59. *See Preface, Department of Justice Frequently Asked Questions ("FAQ") on Encryption Policy* (visited Apr. 14, 1999) <http://www.usdoj.gov/criminal/cybercrime/crypto.html#IVa> (on file with the *Fordham International Law Journal*).

60. *See* 15 C.F.R. §§ 740, 742, 743, 772, 774 (1999); *see also* Bureau of Export Administration, Department of Commerce, *Encryption Items*, 63 Fed. Reg. 72,156 (Dec. 31, 1998) (Interim Rule).

61. The Wassenaar Agreement is subject to re-negotiation and amendment. Most recently, agreement was reached on encryption standards under the Wassenaar framework in December 1998 at a meeting in Vienna. *See, e.g.*, Elizabeth Corcoran, *Encryption Curbs Backed by 33 Nations*, WASH. POST, Dec. 4, 1998, at D1; John Markoff, *International Group Reaches Agreement on Encryption*, N.Y. TIMES, Dec. 4, 1998, at C3.

OECD is a consensus-based organization, all member nations were invited to participate.

With an active delegation from the United States, including representatives from the Justice Department, the Guidelines were completed in December 1996. These Guidelines included eight principles for member nations to take into account when developing their own cryptography policies. These principles are as follows:

1. Trust in Cryptographic Methods: Cryptographic methods should be trustworthy in order to generate confidence in the use of information and communications systems.
2. Choice of Cryptographic Methods: Users should have a right to choose any cryptographic method, subject to applicable law.
3. Market Driven Development of Cryptographic Methods: Cryptographic methods should be developed in response to the needs, demands, and responsibilities of individuals, businesses, and governments.
4. Standards for Cryptographic Methods: Technical standards, criteria, and protocols for cryptographic methods should be developed and promulgated at the national and international level.
5. Protection of Privacy and Personal Data: The fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national cryptography policies and in the implementation and use of cryptographic methods.
6. Lawful Access: National cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible.
7. Liability: Whether established by contract or legislation, the liability of individuals and entities that offer cryptographic services or hold or access cryptographic keys should be clearly stated.
8. International Cooperation: Governments should cooperate to coordinate cryptography policies. As part of this effort, governments should remove, or avoid creating in

the name of cryptography policy, unjustified obstacles to trade.

On March 27, 1997, the OECD adopted the Guidelines as a Recommendation of the Council of the OECD.[62] As countries formulate their cryptography policies, the OECD Guidelines have been carefully analyzed and seriously considered.[63]

CONCLUSION

While the development of cyberspace offers much promise for international interaction and growth, it also facilitates the commission of international crime. By identifying the critical international issues relating to crimes in cyberspace and addressing them, countries can try to maintain the same security for their citizens in the information society that they have traditionally enjoyed.

62. The Guidelines adopted by the Organization for Economic Co-operation and Development can be found in Appendix C.

63. *See, e.g.*, Stewart A. Baker, *Decoding OECD Guidelines for Cryptography Policy*, 31 INT'L L. 729, *passim* (1997); Wayne Madsen et al., *Cryptography and Liberty: An International Survey of Encryption Policy*, JOHN MARSHAL J. COMP. & INFO. L. 475, 522-24 (1998) (discussing OECD Guidelines).

APPENDIX A

MEETING OF JUSTICE AND INTERIOR MINISTERS OF THE EIGHT DECEMBER 9-10, 1997

COMMUNIQUÉ
WASHINGTON, D.C.
DECEMBER 10, 1997

At the Summit of The Eight in Denver, our Heads of State and Government directed us to intensify our efforts to implement the forty recommendations of the Summit of Lyon, in order to combat transnational organized criminal activity posing an ever-greater threat to the individual and collective security of our citizens. With increased international movement by organized criminal groups and their use of new global communications technologies, the protection of our citizens' safety, traditionally a domestic concern, requires unprecedented levels of international cooperation. Our responsibility is not only to react to the activities of organized criminal groups, but also to anticipate and prevent their growth.

We meet today at the Ministerial level to agree upon a program of specific actions designed to accomplish two critical tasks: enhancing our abilities to investigate and prosecute high-tech crimes and strengthening international legal regimes for extradition and mutual legal assistance to ensure that no criminal receives safe haven anywhere in the world.

With regard to high-tech crime, we must start by recognizing that new computer and telecommunications technologies offer unprecedented opportunities for global communication. As nations become increasingly reliant upon these technologies, including wireless communications, their exploitation by high-tech criminals poses an ever-greater threat to public safety. This threat takes at least two forms. First, sophisticated criminals are targeting computer and telecommunications systems to obtain or alter valuable information without authority and may attempt to disrupt critical commercial and public systems. Second, criminals, including members of organized crime groups and terrorists, are using these new technologies to facilitate traditional offenses. Clearly, the misuse of information systems in these ways poses a serious threat to public safety.

National laws apply to the Internet and other global net-

works. But while the enactment and enforcement of criminal laws have been, and remain, a national responsibility, the nature of modern communications networks makes it impossible for any country acting alone to address this emerging high-tech crime problem. A common approach addressing the unique, borderless nature of global networks is needed and must have several distinct components.

Each country must have in place domestic laws that ensure that the improper use of computer networks is appropriately criminalized and that evidence of high-tech crimes can be preserved and collected in a timely fashion. Countries must also ensure that a sufficient number of technically-literate, appropriately-equipped personnel are available to address high-tech crimes.

Such domestic efforts must be complemented by a new level of international cooperation, especially since global networks facilitate the commission of transborder offenses. Therefore, consistent with principles of sovereignty and the protection of human rights, democratic freedoms and privacy, nations must be able to collect and exchange information internationally, especially within the short time frame so often required when investigating international high-tech crimes.

The development of effective solutions will also require unprecedented cooperation between government and industry. It is the industrial sector that is designing, deploying and maintaining these global networks and is primarily responsible for the development of technical standards. Thus, it is incumbent on the industrial sector to play its part in developing and distributing secure systems that, when accompanied by adherence to good computer and personnel security practices, serve to prevent computer abuse. Such systems should also be designed to help detect computer abuse, preserve electronic evidence, and assist in ascertaining the location and identity of criminals.

To meet the challenges of the information age, we have agreed to ten Principles and a ten-point Action Plan, annexed to this Communiqué. We direct our experts to promote these Principles throughout the international community and take forward the Action Plan without delay.

Another core area of concern is mutual legal assistance and extradition. We reiterate the fundamental importance of either

returning our nationals for trial in the country in which the crime was committed or, where that is not possible, conducting effective domestic prosecutions in lieu thereof. Those of us that conduct domestic prosecution of our nationals in lieu of extradition agree to pursue such prosecutions with the same commitment of time, personnel and financial resources as are devoted to the prosecution of serious crimes committed within our own territory.

We recognize that the need for enhanced cooperation in extradition and mutual assistance is particularly acute with respect to high-tech crime and other areas of emerging significance. We commit to remove impediments in existing cooperation regimes by such means as approaching issues of dual criminality with flexibility, and we will ensure that serious computer abuses have criminal penalties sufficient to make them extraditable. We also commit to enhance coordination among States in multi-jurisdictional cases, so as to minimize conflicts and duplications in investigations and prosecutions, consult as to where best to prosecute, and allocate responsibility for gathering and sharing evidence.

We are also convinced that we must further enhance our abilities to obtain testimony from witnesses located abroad for use in criminal proceedings in our States. We agree to intensify our efforts to use video-link technology as a means of securing testimony or statements from a witness located abroad. Where possible, we will locate or establish facilities with technical video-link capability, allow the use of video-link as a form of mutual assistance to other States and provide for the punishment of perjury committed during video-link transmissions.

We emphasize that these agreed-upon cooperation measures can be used by all countries to enhance international cooperation in combating transnational organized crime. Our experts will review annually our implementation at the national level of these international legal cooperation measures. We also urge all States to adopt the recommendations of the Summit of Lyon pertaining to international legal cooperation and the best practices agreed upon by our experts to implement them.

We direct our experts to focus their future work on the following areas: Continued examination of the use of video-link technology and confiscation and sharing of assets obtained

through criminal activity; identification of additional measures that would enhance cooperation in areas of emerging significance; ways to further promote acceptance by other members of the international community of the principles set forth in the above recommendations and practical actions; and coordination among The Eight on the possible elaboration of a U.N. organized crime convention.

In addition to taking action on high-tech crime and mutual legal assistance, we further direct our experts to pursue their work in implementing comprehensive action against transnational organized crime, as mandated by the Denver Summit. Therefore, we welcome the continued efforts of our experts to develop cooperative strategies and policies to combat major transnational criminal organizations and to implement joint operational projects to target such organizations and their criminal activities. We will continue to work together to combat international firearms trafficking and other forms of cross-border crime and smuggling and to address the financial aspects of organized crime.

In conclusion, we recognize the urgent need to make rapid progress in these areas and will take the steps necessary to ensure protection from the physical and financial predation of transnational organized crime. Our task is daunting, but we expect to report substantial progress in this endeavor to the Birmingham Summit in May of 1998.

COMMUNIQUÉ ANNEX:
PRINCIPLES TO COMBAT HIGH-TECH CRIME

Statement of Principles

I. There must be no safe havens for those who abuse information technologies.

II. Investigation and prosecution of international high-tech crimes must be coordinated among all concerned States, regardless of where harm has occurred.

III. Law enforcement personnel must be trained and equipped to address high-tech crimes.

IV. Legal systems must protect the confidentiality, integrity, and availability of data and systems from unauthorized impairment and ensure that serious abuse is penalized.

V. Legal systems should permit the preservation of and quick access to electronic data, which are often critical to the successful investigation of crime.

VI. Mutual assistance regimes must ensure the timely gathering and exchange of evidence in cases involving international high-tech crime.

VII. Transborder electronic access by law enforcement to publicly available (open source) information does not require authorization from the State where the data resides.

VIII. Forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions must be developed and employed.

IX. To the extent practicable, information and telecommunications systems should be designed to help prevent and detect network abuse, and should also facilitate the tracing of criminals and the collection of evidence.

X. Work in this area should be coordinated with the work of other relevant international fora to ensure against duplication of efforts.

ACTION PLAN

In support of these PRINCIPLES, we are directing our officials to:

1. Use our established network of knowledgeable personnel to ensure a timely, effective response to transnational high-tech cases and designate a point-of-contact who is available on a twenty-four hour basis.

2. Take appropriate steps to ensure that a sufficient number of trained and equipped law enforcement personnel are allocated to the task of combating high-tech crime and assisting law enforcement agencies of other States.

3. Review our legal systems to ensure that they appropriately criminalize abuses of telecommunications and computer systems and promote the investigation of high-tech crimes.

4. Consider issues raised by high-tech crimes, where relevant, when negotiating mutual assistance agreements or arrangements.

5. Continue to examine and develop workable solutions regarding: the preservation of evidence prior to the execution of a request for mutual assistance; transborder searches; and computer searches of data where the location of that data is unknown.

6. Develop expedited procedures for obtaining traffic data from all communications carriers in the chain of a communication and to study ways to expedite the passing of this data internationally.

7. Work jointly with industry to ensure that new technologies facilitate our effort to combat high-tech crime by preserving and collecting critical evidence.

8. Ensure that we can, in urgent and appropriate cases, accept and respond to mutual assistance requests relating to high-tech crime by expedited but reliable means of communications, including voice, fax, or e-mail, with written confirmation to follow where required.

9. Encourage internationally-recognized standards-making bodies in the fields of telecommunications and information technologies to continue providing the public and private sectors with standards for reliable and secure telecommunications and data processing technologies.

10. Develop and employ compatible forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions.

APPENDIX B

RECOMMENDATION NO. R (95) 13 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES CONCERNING PROBLEMS OF CRIMINAL PROCEDURE LAW CONNECTED WITH INFORMATION TECHNOLOGY (ADOPTED BY THE COMMITTEE OF MINISTERS ON 11 SEPTEMBER 1995 AT THE 543 MEETING OF THE MINISTERS' DEPUTIES)

The Committee of Ministers, under the terms of Article 15.b of the Statute of the Council of Europe.

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Having regard to the unprecedented development of information technology and its application in all sectors of modern society;

Realizing that the development of electronic information systems will speed up the transformation of traditional society into an information society by creating a new space for all types of communications and relations;

Aware of the impact of information technology on the manner in which society is organised and on how individuals communications and interrelate;

Conscious that an increasing part of economic and social relations will take place through or by use of electronic information systems;

Concerned at the risk that electronic information systems and electronic information may also be used for committing criminal offenses;

Considering that evidence of criminal offenses may be stored and transferred by these systems;

Noting that criminal procedure laws of members states often do not yet provide for appropriate powers to search and collect evidence in these systems in the course of criminal investigations;

Recalling that the lack of appropriate special powers may impair investigating authorities in the proper fulfillment of their tasks in the face of the ongoing development of information technology;

Recognising the need to adopt the legitimate tools which investigating authorities are afforded under criminal procedure laws

the specific nature of investigations in electronic information systems;

Concerned by the potential risk that member states may not be able to render mutual legal assistance in an appropriate way when requested to collect electronic evidence within their territory from electronic information systems;

Convinced of the necessity of strengthening international co-operation and achieving a greater compatibility of criminal procedural laws in this field;

Recalling Recommendation No. R (81) 20 of the Committee of Ministers on the harmonisation of laws relating to the requirement of written proof and to the admissibility of reproductions of documents and recordings on computers, Recommendation No. R. (85) 10 on letters rogatory for the interception of telecommunications, Recommendations No. R (87) 15 regulating the use of personal data in the police state and Recommendations No. R (89) 9 on computer-relating crime,

Recommends the governments of member states:

i. when reviewing their internal legislation and practice, to be guided by the principles appended to this recommendation; and ii. to ensure publicity for these principles among those investigating authorities and other professional bodies, in particular in the field of information technology, which may have an interest in their application.

APPENDIX TO RECOMMENDATION NO R. (95) 13 CONCERNING PROBLEMS OF CRIMINAL PROCEDURE LAW CONNECTED WITH INFORMATION TECHNOLOGY

I. SEARCH AND SEIZURE

1. The legal distinction between searching computers systems and seizing data stored therein and intercepting data in the course of transmission should be clearly delineated and applied.

2. Criminal procedure laws should permit investigating authorities to search computer systems and seize data under similar conditions as under traditional powers of search and seizure. The person in charge of the system should be informed that the system has been searched and of the kind of data that has been seized. The legal remedies that are provided for in general

against search and seizure should be equally applicable in case of search in computer systems and in case of seizure of data therein.

3. During execution of a search, investigating authorities should have the power, subject to appropriate safeguards, to extend the search of other computer systems within their jurisdiction which are connected by means of a network and seize the data therein, provided immediate action is required.

4. Where automatically processed data is functionally equivalent to a traditional document, provisions in the criminal procedure law relating to search and seizure of documents should apply equally to it.

II. Technical Surveillance

5. In view of the convergence of information technology and telecommunications, law pertaining to technical surveillance for the purpose of criminal investigations, such as interception of telecommunications, should be reviewed and amended, where necessary, to ensure their applicability.

6. The law should permit investigating authorities to avail themselves of all necessary technical measures that enable the collection of traffic data in the investigation of crimes.

7. When collected in the course of a criminal investigation and in particular when obtained by means of intercepting telecommunications, data which is the object of legal protection and processed by a computer system should be secured in an appropriate manner.

8. Criminal procedure laws should be reviewed with a view to making possible the interception of telecommunications and the collection of traffic data in the investigation of serious offenses against the confidentiality, integrity and availability of telecommunications or computer systems.

III. Obligations to co-operate with the investigating authorities

9. Subject to legal privileges or protection, most legal systems permit investigating authorities to order persons to hand over objects under their control that are required to serve as evidence. In a parallel fashion, provisions should be made for the

power to order persons to submit any specified data under their control in a computer system in the form required by the investigating authority.

10. Subject to legal privileges or protection, investigating authorities should have the power to order persons who have data in a computer system under their control to provide all necessary information to enable access to a computer system and the data therein. Criminal procedure law should ensure that a similar order can be given to other persons who have knowledge about the functioning of the computer system or measures applied to secure the data therein.

11. Specific obligations should be imposed on operators of public and private networks that offer telecommunications services to the public to avail themselves of all necessary technical measures that enable the interception of telecommunications by the investigating authorities.

12. Specific obligations should be imposed on service providers who offer telecommunications services to the public, either through public or private networks, to provide information to identify the user, when so ordered by the competent investigating authority.

IV. Electronic Evidence

13. The common need to collect, preserve, and present electronic evidence in ways that best ensure and reflect their integrity and irrefutable authenticity, both for the purposes of domestic prosecution and international co-operation, should be recognized. Therefore, procedures and technical methods for handling electronic evidence should be further developed, and particularly in such a way as to ensure their compatibility between states. Criminal procedural law provisions on evidence relating to tradition documents should similarly apply to data stored in a computer system.

V. Use of Encryption

14. Measures should be considered to minimise the negative effects of the use of cryptography on the investigation of criminal offenses, without affecting its legitimate use more than is strictly necessary.

VI. RESEARCH, STATISTICS AND TRAINING

15. The risks involved in the development and application of information technology with regard to the commission of criminal offenses should be assured continuously. In order to enable the competent authorities to keep abreast of new phenomena in the field of computer related offenses and to develop appropriate counter-measures, the collection and analysis of data on these offenses, including modus operandi and technical aspects, should be furthered.

16. The establishment of specialised units for the investigation of offenses, the combating of which requires special expertise in information technology, should be considered. Training programmes enabling criminal justice personnel to avail themselves of expertise in this field should be furthered.

VII. INTERNATIONAL COOPERATION

17. The power to extend a search to other computer systems should also be applicable when the system is located in a foreign jurisdiction, provided that immediate action is required. In order to avoid possible violations of state sovereignty or international law, an unambiguous legal basis for such extended search and seizure should be established. Therefore, there is an urgent need for negotiating international agreements as to how, when and to what extent such search and seizure should be permitted.

18. Expedited and adequate procedures as well as a system of liaison should be available according to which the investigating authorities may request the foreign authorities to promptly collect evidence. For that purpose the requested authorities should be authorized to search a computer system and seize data with a view to its subsequent transfer. The requested authorities should also be authorized to provide trafficking data related to a specific telecommunication, intercept a specific telecommunication or identify its source. For that purpose, the existing mutual legal assistance instruments need to be supplemented.

APPENDIX C

RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES FOR CRYPTOGRAPHY POLICY 27 MARCH 1997

THE COUNCIL, HAVING REGARD TO:

—the Convention on the Organisation for Economic Co-operation and Development of 14 December 1960, in particular, articles 1 b), 1 c), 3 a) and 5 b) thereof;

—the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980 [C(80)58(Final)];

—the Declaration on Transborder Data Flows adopted by the Governments of OECD Member countries on 11 April 1985 [Annex to C(85)139];

—the Recommendation of the Council concerning Guidelines for the Security of Information Systems of 26-27 November 1992 [C(92)188/FINAL];

—the Directive [95/46/EC] of the European Parliament and of the Council of the European Union of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

—the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-use Goods and Technologies agreed on 13 July 1996;

—the Regulation [(EC) 3381/94] and the Decision [94/942/PESC] of the Council of the European Union of 19 December 1994 concerning the control of the export of dual-use goods;

—and the Recommendation [R(95)13] of the Council of Europe of 11 September 1995 concerning problems of criminal procedural law connected with information technology;

CONSIDERING:

—that national and global information infrastructures are developing rapidly to provide a seamless network for world-wide communications and access to data;

—that this emerging information and communications net-

work is likely to have an important impact on economic development and world trade;

—that the users of information technology must have trust in the security of information and communications infrastructures, networks and systems; in the confidentiality, integrity, and availability of data on them; and in the ability to prove the origin and receipt of data;

—that data is increasingly vulnerable to sophisticated threats to its security, and ensuring the security of data through legal, procedural and technical means is fundamentally important in order for national and international information infrastructures to reach their full potential;

RECOGNISING:

—that, as cryptography can be an effective tool for the secure use of information technology by ensuring confidentiality, integrity and availability of data and by providing authentication and non-repudiation mechanisms for that data, it is an important component of secure information and communications networks and systems;

—that cryptography has a variety of applications related to the protection of privacy, intellectual property, business and financial information, public safety and national security, and the operation of electronic commerce, including secure anonymous payments and transactions;

—that the failure to utilise cryptographic methods can adversely affect the protection of privacy, intellectual property, business and financial information, public safety and national security and the operation of electronic commerce because data and communications may be inadequately protected from unauthorised access, alteration, and improper use, and, therefore, users may not trust information and communications systems, networks and infrastructures;

—that the use of cryptography to ensure integrity of data, including authentication and non-repudiation mechanisms, is distinct from its use to ensure confidentiality of data, and that each of these uses presents different issues;

—that the quality of information protection afforded by

cryptography depends not only on the selected technical means, but also on good managerial, organisational and operational procedures;

AND FURTHER RECOGNISING:

—that governments have wide-ranging responsibilities, several of which are specifically implicated in the use of cryptography, including protection of privacy and facilitating information and communications systems security; encouraging economic well-being by, in part, promoting commerce; maintaining public safety; and enabling the enforcement of laws and the protection of national security;

—that although there are legitimate governmental, commercial and individual needs and uses for cryptography, it may also be used by individuals or entities for illegal activities, which can affect public safety, national security, the enforcement of laws, business interests, consumer interests or privacy; therefore governments, together with industry and the general public, are challenged to develop balanced policies;

—that due to the inherently global nature of information and communications networks, implementation of incompatible national policies will not meet the needs of individuals, business and governments and may create obstacles to economic co-operation and development; and, therefore, national policies may require international co-ordination;

—that this Recommendation of the Council does not affect the sovereign rights of national governments and that the Guidelines contained in the Annex to this Recommendation are always subject to the requirements of national law;

On the proposal of the Committee for Information, Computer and Communications Policy;

RECOMMENDS THAT MEMBER COUNTRIES:

—establish new, or amend existing, policies, methods, measures, practices and procedures to reflect and take into account the Principles concerning cryptography policy set forth in the Guidelines contained in the Annex to this Recommendation (hereinafter "the Guidelines"), which is an integral part hereof; in so doing, also take into account the Recommendation of the Council concerning Guidelines Governing the Protection of Pri-

vacy and Transborder Flows of Personal Data of 23 September 1980 [C(80)58(Final)] and the Recommendation of the Council concerning Guidelines for the Security of Information Systems of 26-27 November 1992 [C(92)188/FINAL];

—consult, co-ordinate and co-operate at the national and international level in the implementation of the Guidelines;

—act on the need for practical and operational solutions in the area of international cryptography policy by using the Guidelines as a basis for agreements on specific issues related to international cryptography policy;

—disseminate the Guidelines throughout the public and private sectors to promote awareness of the issues and policies related to cryptography;

—remove, or avoid creating in the name of cryptography policy, unjustified obstacles to international trade and the development of information and communications networks;

—state clearly and make publicly available, any national controls imposed by governments relating to the use of cryptography;

—review the Guidelines at least every five years, with a view to improving international co-operation on issues relating to cryptography policy.

ANNEX
GUIDELINES FOR CRYPTOGRAPHY POLICY

I. AIMS

The Guidelines are intended:

—to promote the use of cryptography;

—to foster confidence in information and communications infrastructures, networks and systems and the manner in which they are used;

—to help ensure the security of data, and to protect privacy, in national and global information and communications infrastructures, networks and systems;

—to promote this use of cryptography without unduly jeopardising public safety, law enforcement, and national security;

—to raise awareness of the need for compatible cryptography policies and laws, as well as the need for interoperable, portable and mobile cryptographic methods in national and global information and communications networks;

—to assist decision-makers in the public and private sectors in developing and implementing coherent national and international policies, methods, measures, practices and procedures for the effective use of cryptography;

—to promote co-operation between the public and private sectors in the development and implementation of national and international cryptography policies, methods, measures, practices and procedures;

—to facilitate international trade by promoting cost-effective, interoperable, portable and mobile cryptographic systems;

—to promote international co-operation among governments, business and research communities, and standards-making bodies in achieving co-ordinated use of cryptographic methods.

II. SCOPE

The Guidelines are primarily aimed at governments, in terms of the policy recommendations herein, but with anticipation that they will be widely read and followed by both the private and public sectors.

It is recognised that governments have separable and distinct responsibilities for the protection of information that requires security in the national interest; the Guidelines are not intended for application in these matters.

III. DEFINITIONS

For the purposes of the Guidelines:

—"Authentication" means a function for establishing the validity of a claimed identity of a user, device or another entity in an information or communications system.

—"Availability" means the property that data, information, and information and communications systems are accessible and usable on a timely basis in the required manner.

—"Confidentiality" means the property that data or infor-

mation is not made available or disclosed to unauthorised individuals, entities, or processes.

—"Cryptography" means the discipline that embodies principles, means, and methods for the transformation of data in order to hide its information content, establish its authenticity, prevent its undetected modification, prevent its repudiation, and/or prevent its unauthorised use.

—"Cryptographic key" means a parameter used with a cryptographic algorithm to transform, validate, authenticate, encrypt or decrypt data.

—"Cryptographic methods" means cryptographic techniques, services, systems, products and key management systems.

—"Data" means the representation of information in a manner suitable for communication, interpretation, storage, or processing.

—"Decryption" means the inverse function of encryption.

—"Encryption" means the transformation of data by the use of cryptography to produce unintelligible data (encrypted data) to ensure its confidentiality.

—"Integrity" means the property that data or information has not been modified or altered in an unauthorised manner.

—"Interoperability" of cryptographic methods means the technical ability of multiple cryptographic methods to function together.

—"Key management system" means a system for generation, storage, distribution, revocation, deletion, archiving, certification or application of cryptographic keys.

—"Keyholder" means an individual or entity in possession or control of cryptographic keys. A keyholder is not necessarily a user of the key.

—"Law enforcement" or "enforcement of laws" refers to the enforcement of all laws, without regard to subject matter.

—"Lawful access" means access by third party individuals or entities, including governments, to plaintext, or cryptographic keys, of encrypted data, in accordance with law.

—"Mobility" of cryptographic methods only means the tech-

nical ability to function in multiple countries or information and communications infrastructures.

—"Non-repudiation" means a property achieved through cryptographic methods, which prevents an individual or entity from denying having performed a particular action related to data (such as mechanisms for non-rejection of authority (origin); for proof of obligation, intent, or commitment; or for proof of ownership).

—"Personal data" means any information relating to an identified or identifiable individual.

—"Plaintext" means intelligible data.

—"Portability" of cryptographic methods means the technical ability to be adapted and function in multiple systems.

IV. INTEGRATION

The principles in Section V of this Annex, each of which addresses an important policy concern, are interdependent and should be implemented as a whole so as to balance the various interests at stake. No principle should be implemented in isolation from the rest.

V. PRINCIPLES

1. TRUST IN CRYPTOGRAPHIC METHODS

CRYPTOGRAPHIC METHODS SHOULD BE TRUSTWORTHY IN ORDER TO GENERATE CONFIDENCE IN THE USE OF INFORMATION AND COMMUNICATIONS SYSTEMS.

Market forces should serve to build trust in reliable systems, and government regulation, licensing, and use of cryptographic methods may also encourage user trust. Evaluation of cryptographic methods, especially against market-accepted criteria, could also generate user trust.

In the interests of user trust, a contract dealing with the use of a key management system should indicate the jurisdiction whose laws apply to that system.

2. CHOICE OF CRYPTOGRAPHIC METHODS

USERS SHOULD HAVE A RIGHT TO CHOOSE ANY CRYPTOGRAPHIC METHOD, SUBJECT TO APPLICABLE LAW.

Users should have access to cryptography that meets their needs, so that they can trust in the security of information and communications systems, and the confidentiality and integrity of data on those systems. Individuals or entities who own, control, access, use or store data may have a responsibility to protect the confidentiality and integrity of such data, and may therefore be responsible for using appropriate cryptographic methods. It is expected that a variety of cryptographic methods may be needed to fulfil different data security requirements. Users of cryptography should be free, subject to applicable law, to determine the type and level of data security needed, and to select and implement appropriate cryptographic methods, including a key management system that suits their needs.

In order to protect an identified public interest, such as the protection of personal data or electronic commerce, governments may implement policies requiring cryptographic methods to achieve a sufficient level of protection.

Government controls on cryptographic methods should be no more than are essential to the discharge of government responsibilities and should respect user choice to the greatest extent possible. This principle should not be interpreted as implying that governments should initiate legislation that limits user choice.

3. MARKET DRIVEN DEVELOPMENT OF CRYPTOGRAPHIC METHODS

CRYPTOGRAPHIC METHODS SHOULD BE DEVELOPED IN RESPONSE TO THE NEEDS, DEMANDS AND RESPONSIBILITIES OF INDIVIDUALS, BUSINESSES AND GOVERNMENTS.

The development and provision of cryptographic methods should be determined by the market in an open and competitive environment. Such an approach would best ensure that solutions keep pace with changing technology, the demands of users and evolving threats to information and communications systems security. The development of international technical standards, criteria and protocols related to cryptographic methods should also be market driven. Governments should encourage and co-operate with business and the research community in the development of cryptographic methods.

4. STANDARDS FOR CRYPTOGRAPHIC METHODS

TECHNICAL STANDARDS, CRITERIA AND PROTOCOLS FOR CRYPTOGRAPHIC METHODS SHOULD BE DEVELOPED AND PROMULGATED AT THE NATIONAL AND INTERNATIONAL LEVEL.

In response to the needs of the market, internationally-recognised standards-making bodies, governments, business and other relevant experts should share information and collaborate to develop and promulgate interoperable technical standards, criteria and protocols for cryptographic methods. National standards for cryptographic methods, if any, should be consistent with international standards to facilitate global interoperability, portability and mobility. Mechanisms to evaluate conformity to such technical standards, criteria and protocols for interoperability, portability and mobility of cryptographic methods should be developed. To the extent that testing of conformity to, or evaluation of, standards may occur, the broad acceptance of such results should be encouraged.

5. PROTECTION OF PRIVACY AND PERSONAL DATA

THE FUNDAMENTAL RIGHTS OF INDIVIDUALS TO PRIVACY, INCLUDING SECRECY OF COMMUNICATIONS AND PROTECTION OF PERSONAL DATA, SHOULD BE RESPECTED IN NATIONAL CRYPTOGRAPHY POLICIES AND IN THE IMPLEMENTATION AND USE OF CRYPTOGRAPHIC METHODS.

Cryptographic methods can be a valuable tool for the protection of privacy, including both the confidentiality of data and communications and the protection of the identity of individuals. Cryptographic methods also offer new opportunities to minimise the collection of personal data, by enabling secure but anonymous payments, transactions and interactions. At the same time, cryptographic methods to ensure the integrity of data in electronic transactions raise privacy implications. These implications, which include the collection of personal data and the creation of systems for personal identification, should be considered and explained, and, where appropriate, privacy safeguards should be established.

The OECD Guidelines for the Protection of Privacy and Transborder Flows of Personal Data provide general guidance concerning the collection and management of personal information, and should be applied in concert with relevant national law when implementing cryptographic methods.

6. LAWFUL ACCESS

NATIONAL CRYPTOGRAPHY POLICIES MAY ALLOW LAWFUL ACCESS TO PLAINTEXT, OR CRYPTOGRAPHIC KEYS, OF ENCRYPTED DATA. THESE POLICIES MUST RESPECT THE OTHER PRINCIPLES CONTAINED IN THE GUIDELINES TO THE GREATEST EXTENT POSSIBLE.

If considering policies on cryptographic methods that provide for lawful access, governments should carefully weigh the benefits, including the benefits for public safety, law enforcement and national security, as well as the risks of misuse, the additional expense of any supporting infrastructure, the prospects of technical failure, and other costs. This principle should not be interpreted as implying that governments should, or should not, initiate legislation that would allow lawful access.

Where access to the plaintext, or cryptographic keys, of encrypted data is requested under lawful process, the individual or entity requesting access must have a legal right to possession of the plaintext, and once obtained the data must only be used for lawful purposes. The process through which lawful access is obtained should be recorded, so that the disclosure of the cryptographic keys or the data can be audited or reviewed in accordance with national law. Where lawful access is requested and obtained, such access should be granted within designated time limits appropriate to the circumstances. The conditions of lawful access should be stated clearly and published in a way that they are easily available to users, keyholders and providers of cryptographic methods.

Key management systems could provide a basis for a possible solution that could balance the interest of users and law enforcement authorities; these techniques could also be used to recover data, when keys are lost. Processes for lawful access to cryptographic keys must recognise the distinction between keys that are used to protect confidentiality and keys that are used for other purposes only. A cryptographic key that provides for identity or integrity only (as distinct from a cryptographic key that verifies identity or integrity only) should not be made available without the consent of the individual or entity in lawful possession of that key.

7. LIABILITY

WHETHER ESTABLISHED BY CONTRACT OR LEGISLATION, THE LIABILITY OF INDIVIDUALS AND ENTITIES THAT OFFER CRYPTOGRAPHIC SERVICES OR HOLD OR ACCESS CRYPTOGRAPHIC KEYS SHOULD BE CLEARLY STATED.

The liability of any individual or entity, including a government entity, that offers cryptographic services or holds or has access to cryptographic keys, should be made clear by contract or where appropriate by national legislation or international agreement. The liability of users for misuse of their own keys should also be made clear. A keyholder should not be held liable for providing cryptographic keys or plaintext of encrypted data in accordance with lawful access. The party that obtains lawful access should be liable for misuse of cryptographic keys or plaintext that it has obtained.

8. INTERNATIONAL CO-OPERATION

GOVERNMENTS SHOULD CO-OPERATE TO CO-ORDINATE CRYPTOGRAPHY POLICIES. AS PART OF THIS EFFORT, GOVERNMENTS SHOULD REMOVE, OR AVOID CREATING IN THE NAME OF CRYPTOGRAPHY POLICY, UNJUSTIFIED OBSTACLES TO TRADE.

In order to promote the broad international acceptance of cryptography and enable the full potential of the national and global information and communications networks, cryptography policies adopted by a country should be co-ordinated as much as possible with similar policies of other countries. To that end, the Guidelines should be used for national policy formulation.

If developed, national key management systems must, where appropriate, allow for international use of cryptography.

Lawful access across national borders may be achieved through bilateral and multilateral co-operation and agreement.

No government should impede the free flow of encrypted data passing through its jurisdiction merely on the basis of cryptography policy.

In order to promote international trade, governments should avoid developing cryptography policies and practices that create unjustified obstacles to global electronic commerce. Governments should avoid creating unjustified obstacles to international availability of cryptographic methods.