ADEQUACY OF CRIMINAL LAW AND PROCEDURE (CYBER)

A "LEGAL FOUNDATIONS" STUDY

Report 7 of 12

Report to the
President's Commission
on Critical Infrastructure Protection
1997

This report was submitted to the President's Commission on Critical Infrastructure Protection, and informed its deliberations and recommendations. This report represents the opinions and conclusions solely of its developers.

Contents

Acknowledgments

The *Legal Foundations* series of reports of the President's Commission on Critical Infrastructure Protection (PCCIP) resulted from the concerted efforts and hard work of several individuals. The Commission gratefully acknowledges Commissioner Stevan D. Mitchell and Assistant General Counsel Elizabeth A. Banker for their leadership and important contributions in developing the *Legal Foundations* series of reports. Their research, writing and analytical contributions were essential to the success of the effort.

The Commission also acknowledges Lee M. Zeichner, Esq. of LegalNet Works Incorporated and his staff, for conceptualizing and maintaining the legal issues database and for providing tireless research support. Finally, the Commission acknowledges the contributions of Senior Consultant Paul Byron Pattak for his deft editing of this compilation.

Preface

Executive Order 13010 established the President's Commission on Critical Infrastructure Protection (PCCIP) and tasked it with assessing the vulnerabilities of, and threats to, eight named critical infrastructures and developing a national strategy for protecting those infrastructures from physical and cyber threats. The Executive Order also required that the PCCIP consider the legal and policy issues raised by efforts to protect the critical infrastructures and propose statutory and regulatory changes necessary to effect any subsequent PCCIP recommendations.

To respond to the legal challenges posed by efforts to protect critical infrastructures, the PCCIP undertook a variety of activities to formulate options and to facilitate eventual implementation of PCCIP recommendations by the Federal government and the private sector. The PCCIP recognized that the process of infrastructure assurance would require cultural and legal change over time. Thus, these activities were undertaken with the expectation that many would continue past the life of the PCCIP itself.

The *Legal Foundations* series of reports attempts to identify and describe many of the legal issues associated with the process of infrastructure assurance. The reports were used by the PCCIP to inform its deliberations. The series consists of 12 reports:

1. *Legal Foundations: Studies and Conclusions*
2. *The Federal Legal Landscape*
3. *The Regulatory Landscape*
4. *Legal Authorities Database*
5. *Infrastructure Protection Solutions Catalog*
6. *Major Federal Legislation*
7. *Adequacy of Criminal Law and Procedure (Cyber)*
8. *Adequacy of Criminal Law and Procedure (Physical)*
9. *Privacy and the Employer-Employee Relationship*
10. *Legal Impediments to Information Sharing*
11. *Federal Government Model Performance*
12. *Approaches to Cyber Intrusion Response*

and two special studies:

- *Information Sharing Models*
- *Private Intrusion Response*

Legal Foundations: Studies and Conclusions is the overall summary report. It describes the other reports, the methodologies used by the researchers to prepare them, and summarizes the

possible approaches and conclusions that were presented to the PCCIP for its consideration. The series has been sequenced to allow interested readers to study in detail a specific area of interest. However, to fully appreciate the scope of the topics studied and their potential interaction, a review of the entire series is recommended.

Part One

Introduction

This paper studies the adequacy of current criminal law to provide adequate protection for the nation's critical infrastructures from cyber attack. It also addresses the adequacy of criminal law to deter or punish cyber attacks on infrastructures and if so, whether applicable laws should be amended, revised, or supplemented to fill the gap.

Research Issues

This paper addresses the following research questions:

- Do existing laws governing criminal procedure unduly hinder investigations of infrastructure threatening behavior?
- To the extent that they may unduly hinder such investigations, how should they be reconsidered or modified?

Research Findings

Upon reviewing various Federal, state and international statutes, the following observations were noted:

- In the United States, substantive computer crime laws (including sentencing laws) have been made by-and-large sufficient owing to recent amendments:

- Federal and state computer crime statutes are now broad enough to cover a wide range of behaviors, including unauthorized computer intrusion and propagation of malicious code.

- The Federal Sentencing Guidelines for these offenses have recently been amended to provide for increased and more comprehensive penalties for computer crime and are currently before Congress for approval.

- Procedural laws governing the investigation of computer-related offenses, however, have traditionally received far less attention, and may, in their current form, unduly hinder the conduct of investigations in electronic environments:

- U.S. law governing search and seizure requires that search warrants be obtained from courts "within a federal district . . . for a search of property . . . within the district." Fed. R. Crim. P. 41(a). This formulation does not apply readily or predictably to evidence stored in networked environments, leading to confusion and delay in the conduct of time-sensitive investigations.

- U.S. law governing the issuance of "trap and trace" orders requires that the government apply for legal process in each of the jurisdictions through which suspect electronic communications pass, thus hampering law enforcement's ability to quickly identify the source of an attack.

- Intrusions emanating from outside the United States compound these legal difficulties and create others—substantive and procedural:

    - In order to enlist assistance from foreign law enforcement services, mutual legal assistance treaties (MLATs) often require "dual criminality," that is, the behavior subject to investigation must also be a crime in the country in which the intruder is physically located. The United States thus has an interest in seeing that other countries also have adequate substantive computer crime laws.

    - In order to obtain timely and effective assistance from foreign law enforcement services, it is desirable for those services to be equipped with adequate procedural laws to foster the quick identification of the source of an attack.

    - In order to obtain evidence from foreign law enforcement services for use in U.S. criminal prosecutions, U.S. investigators currently must appeal to the courts to engage in a formal process (letters rogatory). Streamlined procedures would aid time-sensitive investigations.

- The legal channels necessary for maximally efficient international cooperation are just beginning to develop.

Assumptions

This paper uses certain assumptions in its analyses, and they are as follows:

- Computer crimes will continue to rise in frequency and severity, with (at least) a proportionate increase in the number of intrusions emanating from foreign jurisdictions.
- Although strong domestic enforcement will carry a significant deterrent effect on some classes of computer intruders, maximum deterrence can only be achieved through an effective international computer crime response.
- Enhancing the effectiveness of local, state, Federal and international law enforcement response to computer crime will achieve additional deterrence.
- Enhancing deterrence will reduce the cyber-threat to critical infrastructures.

Part Two

Historical Background: Computer Crime Legislation & International Agreements

As described more completely in the next section, legal reform in the areas of computer crime is underway at the local, state, national and international levels. The states continue to revise and reform their computer crime legislation, and many allocate funds to develop dedicated units of computer crime investigators and prosecutors. States continue to develop the most progressive ways of dealing with juvenile offenders.

On the Federal level, Congress has made frequent revisions to applicable federal law, which now covers virtually all forms of computer fraud and abuse. In late 1996, Congress enacted a federal law to address economic espionage and theft of trade secrets. The U.S. Sentencing Commission recently studied and proposed amendments to their guidelines for computer crimes. The new Guidelines are expected to go into effect in November 1997. Congress and the Administration are also reconsidering the current federal approach to crimes committed by juveniles. Despite its willingness to reconsider and revisit substantive computer crime laws, Congress has not been as receptive to changes in procedural criminal laws, particularly where revisions may be interpreted to impinge upon privacy and civil liberties. (Much of current criminal procedure is dictated not only by Congress, but by the Constitution and the Supreme Court.)

Work is also underway in a number of international forums, including the OECD, the Council of Europe, the European Union, and the G-7/P8, to insure the adequacy of criminal laws, procedures and resources among the respective member nations. In addition, the U.S. continues to pursue bilateral treaties and agreements to cement in place predictable and effective international response mechanisms.

The bulk of the items in this paper are premised on the work already undertaken or accomplished by these various bodies.

State Computer Crime Laws

Florida, Arizona and Virginia were at the forefront of state and federal efforts to craft legislation specifically to combat computer crime. As early as 1978, these states had computer crime statutes in place, and by 1979, California, Colorado, Illinois, Michigan, New Mexico, North Carolina, Rhode Island, and Utah had joined their ranks. By 1990, all states except Vermont had enacted some form of computer-related criminal law. Today, these statutes take a variety of forms and are, in some instances, more flexible and responsive to the unique character of computer crime than their federal counterparts. State statutory schemes often address unauthorized access or use, information abuse, and intrusive code (e.g. viruses).

States have also shown flexibility in responding to the challenges of investigating computer crimes. For instance, "Nebraska's computer crime statute provides incentives for potential victims of computer crimes to implement their own security measures. California's computer crime statute encourages victims to come forward by providing a civil cause of action for compensatory damages."[1] Civil actions are growing in popularity among states. A number of states have developed civil provisions either to supplement a criminal prosecution, act as an alternative to criminal prosecution, or fill a void left unfilled by the criminal law.[2] State civil actions not only cover a wider range of computer abuses, they also provide greater relief for the victim through the availability of injunctions, damages, court costs and attorney fees. Civil actions have the added advantages of a lower standard of proof and a higher degree of privacy.[3]

A number of states are also experimenting with novel sentencing provisions that afford the courts flexibility to craft penalties to minimize recidivism and achieve maximum deterrence, while at the same time providing additional monetary relief to the victim. Restitution and forfeiture provisions are becoming increasingly common.[4] Fines may be set in proportion to the loss of the victim or the financial gain of the defendant.[5] Judges may also impose restrictions on a defendant's use of computers following conviction.[6]

---

[1] Project, *Eighth Survey of White Collar Crime*, 30 Am. Crim. L. Rev. 495, 516 (1993).

[2] *See, e.g.*, Cal. Penal Code § 502(e) (permits recovery of compensatory damages, including expenses incurred to verify the extent of damage done by the access, and a reasonable attorney's fee to the prevailing party); Ga. Code Ann. § 16-9-93(g) (victim may recover damages, including lost profits and victim expenditure, plus cost of the suit); Tex. Civ. Prac. & Rem. Code Ann. §§ 143.001-143.002 (requires knowing or intentional violation of criminal provisions); Conn. Gen. Stat. Ann. § 52-570b (civil recovery independent of criminal actions for acts done recklessly, rather than intentionally or knowingly).

[3] Arkansas, Virginia, and Wisconsin provide specifically for some measure of privacy for the victims of computer crime. *See* Ark. Code Ann § 5-41-106(b); Va. Code Ann. § 18.2-152.12; Wis. Stat. § 943.70(5).

[4] *See, e.g.*, N.M. Stat. Ann. § 30-45-7 (Restitution to be paid in addition to incarceration, forfeiture or fine); Cal. Penal Code § 502(g) (Forfeiture of computer equipment used during an offense); Ill. Ann. Stat. Ch. 38 para. 16D-6 (Forfeiture of "monies, profits, or proceeds"). *See also*, N.M. Stat. Ann. § 30-45-7; Ohio Rev. Code Ann. § 2925.44.

[5] *See* Mon. Code Ann. § 45-6-311(c)(2); 1984 Conn. Gen. Stat. Ann. § 53a-257; Del. Code Ann. tit. 11, § 937(f).

[6] *See* Wis. Stat. § 943.70(4); Cal. Penal Code § 502(e)(3).

While there are benefits to state schemes, they do have legal and practical limitations. State investigators are often hampered in investigations of computer crime by jurisdictional boundaries. The nature of the Internet is not only interstate, but also international. States are beginning to develop special venue provisions that allow cases to go forward where any part of the criminal act took place, not only where the computer is located.[7] This is only a small first step. Over the next several years, states can be expected to continue confronting these difficulties as well as to continue refining their substantive statutes.

Federal Computer Crime Legislation

In the early 1980's, there was no specific federal legislation in the area of computer crime. To prosecute a computer-related crime, one had to rely on federal statutes designed for other offenses, such as mail fraud[8] or wire fraud.[9] However, as evidence of computer-related crimes became more abundant, computer crime began to receive the attention of law enforcement personnel, the media, and the general public. Specifically, financial institutions (e.g. MasterCard International, VISA, etc.) reported large losses due to the exploitation of stolen and counterfeited credit cards and account numbers, in which exploitation was intertwined with the use of computers.

As a result, the House Committee on the Judiciary held hearings (Sept. 29 and Nov. 10, 1983; March 28, 1994) documenting society's dependence on credit cards and other financial instruments, many of which involved the use of computers and other electronic devices subject to criminal abuse. It became apparent that traditional theft/larceny statutes were not the proper vehicle to control computer abuse and computer assisted crimes. The Committee concluded that criminal laws needed 1) to be brought up to date, 2) to account for rapidly advancing technology, and 3) to shift attention from concepts such as "tangible property" to concepts of "information" and "access to information." The hearings led to passage of the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (a part of the Comprehensive Crime Control Act).[10] This Act created 18 U.S.C. §§ 1029 and 1030 which made unauthorized access of classified information in a computer a felony and unauthorized access to financial records or credit histories in financial institutions or to trespass into a government computer a misdemeanor.[11]

In 1985, both the House and the Senate introduced legislation to expand the Computer Fraud and Abuse Act, 18 U.S.C. § 1030. Hearings were held before the Committee on the Judiciary to

[7] *See* Ark. Stat. Ann. § 5-41-105; Conn. Gen. Stat. Ann. § 53a-260; Ga. Code Ann. § 16-9-94; Ky. Rev. Stat. Ann. § 434.860; see also Md. Ann. Code art. 27, § 146(e); Miss. Code Ann. § 97-45-11; N.J. Stat. Ann. § 2C:20-34; S.C. Code Ann. § 16-16-30; S.D. Codified Laws Ann. § 43-43B-8; Tenn. Code Ann. § 39-14-603.
[8] 18 U.S.C. § 1341.
[9] 18 U.S.C. § 1343.
[10] Pub. L. No. 98-473 (1984) (codified at 18 U.S.C. § 1030).
[11] S. Rep. No. 357, 104th Cong., 2d Sess. 4 (1996).

introduce variations. The Committee noted that, although financial institutions relied heavily on computer communications and were therefore especially vulnerable to attack, computer crime posed threats outside of the financial realm. After reviewing the American Bar Association Task Force on Computer Crime's Report on Computer Crime ("ABA Report"), which concluded that the most effective means of preventing computer crime was "more comprehensive and effective self-protection" by businesses, the Committee recommended the development of education programs for computer users and the general public to make people aware of the ethical and legal implications of using such technology. The Committee also considered issues of jurisdiction, and decided that, instead of enacting sweeping federal legislation, federal jurisdiction should be limited to cases in which there is a compelling federal interest. The result of the hearings was the Computer Fraud and Abuse Act of 1986 (CFAA).[12]

Congress amended the CFAA again in 1994. The 1994 amendments focused specifically on subsection (a)(5) of section 1030. The intent of the amendment was to expand the prohibition on damage to computers to cover not only "federal interest computers," but any "computer used in interstate commerce." This revision thus technically eliminated federal protection for government and financial institution computers which were not used in interstate commerce.

The 1996 amendments corrected this oversight in the revision of section 1030(a)(5) and also expanded the definition of damage required to trigger the prohibition. The statute, as amended, makes it a crime to:

- Knowingly access a computer without, or in excess of, authorization to obtain classified information.[13]

- Knowingly access a computer without, or in excess of, authorization to obtain (1) financial information from a credit reporting company or a financial institution, (2) any information in the possession of the government, and (3) any private information where the defendant's conduct involves interstate commerce.[14]

- Access, without authorization, a government computer—even if no damage is done or nothing is stolen.[15]

- Use a computer in a scheme to defraud victims of property.[16]

- Knowingly transmit a program (as well as information, code, or a command) and intentionally cause damage to a protected computer.[17]

- Traffic in passwords or other similar information.[18]

---

[12] Pub. L. No. 99-474 (1984).
[13] 18 U.S.C. 1030(a)(1) (1994).
[14] 18 U.S.C. 1030(a)(2) (1994). Obtaining information includes reading the information. Congress did not require that defendants copy or physically move the information. *Id*.
[15] 18 U.S.C. 1030(a)(3) 1994.
[16] 18 U.S.C. 1030(a)(4) 1994.
[17] 18 U.S.C. 1030(a)(5) 1994. Congress amended only this provision in 1995, clarifying that computer viruses and other similar attack mechanisms were included in the orbit of the statute.

Through the National Information Infrastructure Protection and Economic Espionage Acts of 1996, Congress expanded coverage of 18 U.S.C. § 1030 to:

- Protect civilian, state and local government computers from unauthorized access.
- Prohibit abuse of access privileges by government employees to obtain confidential or sensitive information.
- Include lost computer time within the fraud provision;
- Protect intrastate government computers and computers used in foreign communications and commerce from damage from viruses and other harmful computer programs. (A copy of the current law is attached as Appendix B.)

The 1996 amendments also added a new provision to section 1030. 18 U.S.C. § 1030(a)(7) prohibits the use of computers for blackmail or extortion.[19] The amendments also expanded the civil remedy by making it available for all seven provisions of 18 U.S.C. § 1030(a) and by expanding the definition of damage. "Damage" is either significant financial loss, potential impact on medical treatment, causing physical injury to any person, or threatening the public health or safety.[20]

While the CFAA is the major piece of federal legislation for prosecuting computer crimes, other federal legislation also touches on computer crime. The Electronic Communications Privacy Act of 1986 (ECPA)[21] updates the federal wiretap statute to protect the privacy and security of information transmitted through new computer and telecommunications technologies. The ECPA addresses the interception of wire, oral, and electronic communications, the unauthorized access to stored wire and electronic communications, and the use of pen registers and "trap and trace" devices. The ECPA protects the privacy of personal and proprietary information while at the same time satisfying the Federal government's legitimate law enforcement needs. In 1994, Congress supplemented the government's ability to conduct wiretaps through the Communications Assistance for Law Enforcement Act (CALEA) which sets out requirements and procedures for communications carrier cooperation with court ordered wiretaps.[22] In spite of this step forward, the procedural aspects of computer crime investigation and prosecution have not been as active an area for Congressional initiatives and lag well behind the substantive statutes.

---

[18] 18 U.S.C. 1030(a)(6) 1994.

[19] The legislative history provides an example of the sort of act Congress intended to criminalize in subsection (a)(7)-- "hackers penetrate a system, encrypt a database and then demand money for the decoding key." S. Rep. No. 357, 104th Cong., 2d Sess. 12 (1996).

[20] *See* 18 U.S.C. § 1030(e)(8).

[21] Pub. L. No. 99-508 (1986) (codified at 18 U.S.C. § 2505 *et seq.*).

[22] Pub. L. No. 103-414 (1994) (codified at 18 U.S.C. § 2601 *et seq.*).

Congress additionally passed legislation in 1996 primarily to address foreign government-sponsored economic espionage or theft of trade secrets.[23] The Economic Espionage Act of 1996 (attached as Appendix C) criminalizes various computer-related acts by any person, as well as persons "intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent […]"[24] Prohibited acts to obtain trade secrets include:

- stealing or fraudulently obtaining;
- copying or downloading;
- knowingly purchasing or obtaining; and
- conspiring with others to obtain the trade secret.

The United States Sentencing Commission has recently revised the Sentencing Guidelines for computer crime and economic espionage. The amendments are set to go into effect in November, 1997. Unless the Guidelines are modified by Congress, they will provide for, among other things, an expanded definition of loss. When a defendant is convicted of trespass or theft under 18 U.S.C. § 1030(a)(3) or § 1831-32, upward departures in sentencing may be considered based not only on monetary losses, but also costs to the victim for damage assessments, restoring the system or data, and any lost revenue due to interruption of service. An upward departure may also be warranted in situations where the computer crime does not cause a loss per se, but results in a substantial invasion of privacy. If convicted under 18 U.S.C. § 1030(a)(5), an enhanced sentence will be appropriate if the computer crime caused a delay in medical treatment or disruption of important government, or private, services.

International Computer Crime Initiatives

With the advent of the Internet as a global resource, computer crimes are committed increasingly across national boundaries, potentially invoking different legal systems and traditions. While significant work has been done during the past 25 years by several multilateral organizations on substantive computer-related crimes, international organizations have only recently been devoting significant time and attention to procedural issues raised by the need for cross-jurisdiction investigations. The most pressing issues being considered today include:

[23] Economic Espionage Act of 1996, P.L. 105-15, 18 U.S.C. §§ 1831-1839 (1996).
[24] *Id*. at 18 U.S.C. § 1831(a)(1) - (a)(5).

- mutual legal assistance/"dual criminality" requirements;
- extradition and prosecution;
- "rapid trace" capabilities;
- cross jurisdictional search and seizure; and
- evidence collection and computer forensics.

The United States has been an active participant in many of these efforts and has the potential to act as a leader in bringing many of these organizations' recommendations to fruition.

Organization for Economic Development (OECD)

OECD involvement in addressing computer crime and the use and abuse of computer networks began with several peripheral issues. In 1980, the OECD formally adopted its *Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data.* By 1992, the OECD had adopted well-known Guidelines for computer networks in the *Security of Information Systems.* Today, the OECD's focus is primarily on information systems, international telecommunications policy and the Global Information Infrastructure (GII). Currently, an OECD ad hoc Group of Experts is drafting Cryptography Policy Guidelines to assist governments and the private sector in developing guidelines for the use of cryptography technology in order to advance the development of the GII. The OECD hopes to balance these developments with traditional policies covering national security and public safety.

Several members of the OECD hope to focus the organization on the Internet. In particular, France and England are now arguing that the OECD should study, and later pass, international legal standards for the Internet. The French are circulating their own proposal. The OECD is also considering other areas of expansion, including computer crimes, however no specific work has been done to date.

Council of Europe (COE)

The Council of Europe has passed several well-known Recommendations in the area of computer crime. During the past ten years, the COE's European Committee on Crime Problems (CDPC)–a standing committee–commissioned two ad hoc groups to address issues of information technology and criminal law.

The first group focused on substantive criminal issues and produced *Computer-Related Crime,* an extensive report which lead to the well-known COE Recommendation No. R. (89) 9. This

Recommendation, which the whole Council of Ministers adopted in 1989, lists various acts that nations should criminalize as computer crimes.[25]

In 1992, the COE commissioned a second ad hoc Group to focus on procedural issues associated with computer-related crimes. The Committee of Experts on Problems of Criminal Procedure Law Connected with Information Technology produced a second Recommendation.[26] The whole Council of Ministers adopted Recommendation No. R. (95) 13 in September, 1995. The Appendix to Recommendation No. R. (95) 13 recommends that countries create various procedural mechanisms to facilitate investigation and prosecution of crimes involving information technology. The Appendix specifically recommends that rules for search and seizure, technical surveillance, electronic evidence, cooperation with investigators, and international cooperation be reviewed and revised to ensure that they take into adequate account the unique nature of information technology.

Informally, the COE is indicating that it will soon commission a new Group of Experts on Crimes in Cyberspace. The agenda is broad and includes both substantive and procedural issues.

The European Union (EU)

The EU is undertaking several projects that complement the work done by the OECD and the COE. These projects cover topics including:

- Training
- Harmful content on the Internet
- Improving Mutual Legal Assistance Treaties (MLATs) and producing a new European MLAT
- Internet and EU Telecom Issues

G7/P8

Of all the multilateral and international organizations, the G7/P8 is perhaps the most focused in the area of procedural mechanisms to facilitate international cooperation.

The P8 evolved when Russia joined the Group of Seven, or G-7 nations. The P8 then adopted an international agenda that reached beyond the historically economic focus of the G-7, addressing both political and global issues. The Eight—Canada, England, France, Germany, Italy, Japan,

[25] These acts included computer fraud, computer forgery, damage to computer data or programs, computer sabotage, unauthorized access, and unauthorized interception. There were also a number of optional crimes such as alteration of data or programs, computer espionage, and unauthorized computer use.
[26] Recommendation No. R(95)13.

Russia, and the United States—recently embarked on two major initiatives—terrorism and transnational organized crime.

The P8's approach is both aggressive and practical. In the Communiqué from the recent Summit of the Eight in Denver (June 20-22, 1997), aggressive action was called for with regard to two areas of concern:

> *"First, the investigation, prosecution, and punishment of high-tech criminals, such as those tampering with computer and telecommunications technology, across national borders; Second, a system to provide all governments the technical and legal capabilities to respond to high-tech crimes, regardless of where the criminals may be located."*[27]

The High-tech Crime Subgroup of the Senior Experts' Group of the Eight on Transnational Organized Crime are currently working to implement "forty recommendations" relating to transnational organized crime, including computer crime, adopted by the Group in April 1996. The Subgroup is focusing on three areas specifically—(1) locating and identifying the perpetrator of a computer offense ("trap and trace"); (2) gaining access to the content of communications; (3) international cooperation in the collection of evidence (in particular "transborder searches").

The Group has since (in December 1997) issued a communiqué setting forth objectives and an Action Plan for improving response to computer and other high technology crime.

U.S. Involvement/Next Steps

In addition to these multilateral organizations, many foreign nations are working independently to improve the international environment for the investigation and prosecution of computer crime. Neighbors and allies, such as Canada and the United Kingdom, are actively working the problem. The United States government is an active participant and follows the efforts of these international bodies and individual nations closely. The Department of State, Department of Justice, and Federal Bureau of Investigation are just a few of agencies involved in the international battle against computer crime. These agencies and the interest of the Administration and Congress provide conduits for directing and forwarding the efforts of our international partners.

[27] Communiqué, Summit of the Eight, § 40 (June 22, 1997).

Part Three

Legal And Legislative Options

The sheer number of options and permutations offered by bodies studying these issues has necessitated something of a novel approach. Possible approaches identified in this paper are organized by the jurisdiction to which they apply—state and local, Federal, and international—and then further by the aspect of criminal law on which they focus (whether substantive, procedural or pertaining to resources). To present the analysis better, each option has a "Pro" and "Con" element.

State and Local (Substantive)

Pursue Alternatives to Incarceration and Fines in Their Sentencing Schemes

Although a thorough study of state sentencing schemes was beyond the scope of this paper, it may be feasible for states to continue to create novel remedies that would increase deterrence and provide compensation for victims.

- **Pro:** Recognizes efforts by states that have adopted novel sentencing schemes to deal with unique nature of the crime and those who commit it. Restitution and other remedies, if uniformly provided, may increase the deterrent value of prosecutions by minimizing financial gain.
- **Con:** The value of innovative sentencing schemes has not adequately been demonstrated by states enacting them.

Consider Adoption of Computer Crime Laws Specifically Tailored to Juvenile Offenders

While the increased "detention" of juvenile offenders may be unpopular, some recognition of the need to address the problem they present may be warranted. Ethics training in schools or other vehicles may provide a more appropriate sentencing vehicle through which to "refocus" potential computer criminals.

- **Pro:** By drawing attention to volume of computer crimes perpetrated by juveniles and the weaknesses of some criminal schemes to prosecute or deter them, with further study, recommendations may ultimately be made that will be successful in reducing the number of intrusions by "recreational hackers." This would allow law enforcement to focus on truly destructive computer criminals.

- **Con:** Legal planning related to juvenile offenders is arguably best led by the states themselves, as Federal law enforcement is significantly less experienced in dealing with juvenile justice issues than are the states.

State and Local (Resources)

Devote Increased Resources to State and Local Enforcement of Computer Crime

Computer crime investigations place a tremendous drain on the resources of state and local authorities. Violent crimes are currently—and properly—given priority by strapped departments. An increase in resources would allow states and local jurisdictions to train officers or hire experienced computer security experts, to purchase equipment, and to expend additional man-hours on computer crime investigations. It may be prudent to examine increased training for or hiring of computer-literate prosecutors.

- **Pro:** A more effective state and local response may relieve pressure on federal law enforcement.

- **Con:** With the advent of the Internet, exclusively "local" computer crimes are likely to be increasingly rare. Jurisdictional restrictions often prevent state and local law enforcement from investigating cross-jurisdictional offenses on their own, often requiring inter-state cooperation or federal law enforcement assistance. Thus, resources might be better spent on a coordinated federal response.

Conclusions (State and Local)

The Administration, Through the Department Of Justice, Should Sponsor A Comprehensive Study Aimed at Discovering Effective Ways of Deterring And Responding To Computer Crime And Abuse By Juveniles.

The study would focus on the effectiveness of state-level handling of computer crime incidents, state computer crime laws, procedures for handling juvenile offenders, and sentencing regimes. It would determine whether modifications to applicable federal laws might be warranted. Study participants might include representatives of federal, state and local law enforcement; prosecutors offices; criminal defense attorneys; social services/juvenile justice experts; and representatives from the educational community. The study's aim would be to gather statistics on juvenile offenders (ages, recidivism rates, punishments, criminal activity as adults); examine how well juvenile issues are being covered by federal and state law enforcement efforts (i.e., are there jurisdictional gaps allowing juveniles to "slip through the cracks"?); evaluate the effectiveness of sentencing provisions specifically tailored to juveniles (e.g., community service requirements or extraordinary remedies such as expulsion from school); and promote education and awareness (e.g., ethics training, promote awareness of parents and educators). The study panel should be instructed to offer recommendations to state and federal governments for enhancing efforts to discourage hacker activity among juveniles and to promote responsible computer use.

Federal (Substantive)

Expand Sentencing Guidelines Treatment of "Harm" and "Loss" as Used for 18 U.S.C. § 1030 to Other Electronic Crimes

The U.S. Sentencing Commission, in new guidelines for computer crime, has taken the approach of increasing the deterrent effect of prosecutions by expanding the definitions of harm and loss to include interruptions in service; disruptions or delays in delivery of vital services endangering lives; invasions of privacy; and the cost to the victim of damage assessment, restoration of service and data, and loss of business or revenue due to interruption of service. This approach to sentencing could be adopted for other electronic crimes, including violations of the Wiretap statute and the Electronic Communications Privacy Act.

- **Pro:** The new amendments to sentencing guidelines tend to make punishment more proportional to overall damage done which could be an important consideration in deterring cyber attacks that disrupt critical infrastructures.
- **Con:** Amendments generally take time to be studied by the Sentencing Commission and may have to come as a result of Congressional prompting, which has to date caused a considerable backlog. Sentencing as a deterrent is reliant on reporting of an incident, successful investigation and prosecution. This approach may have limited deterrent value on its own.

Increase Attention to the Issue of Juvenile Computer Crime Offenders

Juvenile computer crime may merit study at the Federal level. Advocates can capitalize on existing federal initiatives which could be used to promote studies and recommendations for dealing with the issue (e.g., legislative initiatives, grant programs, education and awareness programs, research and study bodies). Timing of issue may be influenced by the current Federal juvenile justice statute which is set to expire in September, 1997.

- **Pro:** Federal attention may result in greater awareness of parents, media, and educators to the issue of computer abuse by juveniles. Federal attention may result in a more coordinated and well-rounded approach to dealing with juvenile hackers.

- **Con:** The Federal government has a limited role in criminal prosecutions of juveniles. The issue may be more appropriately handled at the state level. If the issue is not framed carefully, it may receive a negative public reaction from quarters already concerned about the treatment of the juveniles under the criminal law.

Federal (Procedural)

Improve Law Enforcement's Ability to Investigate Through Enhanced Cooperation of Victims and Witnesses

Recognizing difficulties inherent in bolstering law enforcement effectiveness through changes in criminal procedure, it may be preferable to encourage measures that would improve victim and witness cooperation and reporting of criminal incidents. Current victim/witness assistance legislation may provide a model to the extent it provides for a right to restitution and a right to be kept abreast of investigation and prosecution efforts. As an incentive for increased reporting, restitution will only work to the extent the defendant is able to pay. Mandatory requirements for reporting intrusions of a certain magnitude would be included in this general category.

- **Pro:** Additional reporting would provide information that law enforcement might otherwise have to acquire through burdensome procedures, and may obviate the need for procedural reform.
- **Con:** Any form of mandatory reporting is likely to be met with equal or greater opposition than would revisions to procedural criminal law. Incentives for reporting or reporting requirements can be costly and difficult to administer.

Identify And Endorse Viable Alternatives To Fortification Of Criminal Enforcement Regime

Due to the relative intransigence of existing criminal procedures and the unlikely accomplishment of meaningful reform, Congress might consider viable alternatives to criminal

enforcement to instill enhanced deterrence. (*See* PCCIP supplemental report *Approaches to Cyber Intrusion Response* for discussion and options).

Identify Procedural Changes

Congress may wish to consider revisions to procedural laws and rules governing how investigations can be performed in electronic environments. Specific recommendations could include new legislation on performing surveillance in an electronic environment (analogous to the current Wiretap Act, but written specifically for the Internet); a national "trap and trace" capability; or increased ability to monitor systems under 18 U.S.C. § 2511(2)(a)(i) (which currently provides for limited monitoring by service providers to operate and maintain their systems).

- **Pro:** Certain to stir immediate and vigorous discussion.
- **Con:** An immediate and vigorous debate will ensue, due to concerted opposition from civil libertarians, privacy advocates, and the web-surfing public. It is unclear whether significant improvements can be obtained without running afoul of constitutional considerations.

Federal (Resources)

Fortify Law Enforcement Resources Under Existing Substantive and Procedural Regime

Recognizing the relative adequacy of federal substantive criminal law and the limited likelihood of achieving meaningful modification to procedural criminal law, additional resources can be directed to overcoming difficulties inherent in the investigation and prosecution of crimes that arise in electronic environments.

- **Pro:** Avoids staking out potentially controversial position between law enforcement and civil liberties concerns, instead resorting to relatively uncontroversial, "more cops on the beat" approach.

- **Con:** Law enforcement response not cost-effective. Advocating enhancement of law enforcement resources to address high technology crime can be controversial, as it carries potential implication that fewer law enforcement resources might be available for other pressing concerns (violent crime, narcotics offenses, etc.).

Conclusions (Federal)

The Administration Should Promote Current Efforts To Develop Specific Procedural Changes To Assist Law Enforcement In The Investigation Of Computer Crime.

The Department of Justice is currently exploring ways to ease undue administrative burdens on law enforcement officers investigating various forms of computer and high technology crimes that cross federal jurisdictional boundaries. There is a need for a national "trap and trace" capability and an analogous national search warrant capability that would allow for process obtained in one jurisdiction to be used in multiple jurisdictions involved in the offense under investigation. The Administration and Congress should also be sensitive to such needs, given the value of a rapid law enforcement response. Where currently law enforcement investigators are required to obtain court orders or warrants for each jurisdiction they will enter, a national capability would allow electronic searches or "trap and trace" efforts to be conducted across jurisdictional boundaries with the authorization of only one judge. This would not constitute an expansion of law enforcement's current ability to perform these vital functions, but would merely increase the speed and efficiency of their efforts in the computer crime investigation arena.

International (Procedural)

Clarify and Improve Current Procedures

The United States and other countries could pursue clarifications and improvements to their current procedures for investigating computer crime by, for example, a) clearly delineating and

applying a distinction between searching computer systems and seizing data stored therein and intercepting data in the course of its transmission; b) granting investigators the authority, while executing a computer search, to extend the search to any computer system in their jurisdiction which is connected by a network and to seize the data therein, provided immediate action is necessary; c) enabling interception of telecommunications and collection of traffic data in investigations of serious offenses against the confidentiality, integrity, and availability of telecommunications or computer systems; and d) reviewing legal standards for collection of service data to ensure that they are appropriate to the level of personal intrusion.

- **Pro:** Clarifying procedural rules would benefit law enforcement both domestically and internationally. The U.S. may choose to be the leader and urge other nations to follow.
- **Con:** Many of the improvements and clarifications recommended by international bodies implicate complex statutory, constitutional, and policy questions in the United States.

Work to Create a Network of International Law Enforcement Agencies and Telecommunications Carriers to Draw Upon During Investigations

The creation of such a network of dedicated individuals would facilitate prompt "trap and trace" and identification of foreign sources of intrusions. Network members may also be expected to exchange information, engage in training exercises, and share technological innovations. (Note: P8 working groups have consistently highlighted the importance of cooperative networks for addressing law enforcement issues.)

- **Pro:** A network of trained personnel will provide an in-place capability to respond to computer intrusions quickly and effectively.
- **Con:** Developing a network alone will not facilitate investigations without clarification of procedures for obtaining international cooperation and resolution of dual criminality requirements in advance.

Promote International Agreements to Facilitate Cooperation in Computer Investigations

The U.S. currently has Mutual Legal Assistance Treaties (MLATs) in place with a number of countries to facilitate investigations of computer crimes. Various international organizations are

analyzing alternative legal models to MLATs, which are typically variations on traditional and cumbersome procedures for international law enforcement cooperation. The U.S. could nonetheless encourage widespread adoption of agreements, or other vehicles, to improve international cooperation in computer crime, especially among countries who are not members of the primary international organizations working in this area (e.g., P8, OECD, COE).

- **Pro:** Well-crafted agreements will allow investigations to proceed at the speed necessary for successful identification of intruders and still observe international conventions for cooperation.
- **Con:** It may take a considerable amount of time to put in place all necessary agreements to allow a successful investigation. Hackers may be able to use countries not parties to such agreements to shield themselves from investigations.

International (Resources)

Improve Awareness of Sound Computer Forensic Principles and Applications

Gathering of computer evidence is a time-sensitive process which requires careful attention to procedures in order to assure authenticity of the evidence. Use of foreign investigators to collect evidence in U.S. intrusion investigations greatly forwards investigations and chances for prosecution provided the evidence is properly collected. It may be in the U.S. law enforcement interest to educate the international community of investigators, or even to work together to determine guidelines for proper computer forensic procedures. (Note: This option is based on the considerable work of P. Sommer in computer forensics.[28])

- **Pro:** This approach can be expected to increase the availability of evidence of foreign sources of intrusions to be introduced in U.S. courts and may contribute to successful prosecutions.
- **Con:** May be difficult to harmonize procedures internationally. The U.S. will have to work carefully with other participating countries to ensure that U.S. criminal procedure and evidentiary requirements are met.

[28] *See* P. Sommer, Forensic Computing, Computer Security Research Centre, London School of Economics & Political Science (1995), reprinted at http://csrc.lse.ac.uk/csrc/forncomp.htm.

Improve Technological Tools Available for Locating the Sources of Intrusion

The U.S. may want to stimulate an international effort at developing tools to assist in locating the sources of unauthorized intrusions. (Note: The P8 has noted similar concerns about the tools of law enforcement in its study of computer crime.)

- **Pro:** New detection and location tools may have the capability to be tailored to enhance privacy by being less intrusive into the systems passed through during the course of an investigation. Coordination of research and development would bring the international community together and draw on skills and resources of a variety of countries. International guidelines for using such tools may develop in concert with development of the technology.

- **Con:** Research and development is costly and new tools may bring limited returns. Tools will still have to conform to U.S. laws governing tracking down intruders. Technology is moving so quickly that hackers will likely develop tricks to elude law enforcement as quickly as law enforcement develops new tools.

Create Specialized Computer Crime Units on an International Scale

Units would be specially trained and well-versed in the complexities of international investigations. Units would provide an existing network to carry out international investigations. (Note: This recommendation has been put forward by the Council of Europe.)

- **Pro:** Specialized units could be quickly mobilized for an international investigation. They could receive specialized training and would be expected to develop close working relationships across international borders.

- **Con:** Supporting such operations may detract from resources available domestically. There may be problems associated with close investigatory relationships with foreign investigators surveilling U.S. citizens. It would require resources to establish and maintain excellence.

Conclusions (International)

The Administration and Congress should continue to support the efforts by U.S. delegations to several international bodies to further infrastructure assurance objectives and highlight potential areas for continued or expanded efforts in the international area.

The U.S. has been a forerunner in efforts to clarify and improve current procedures for investigating computer crimes. The Administration and Congress should continue to recognize and support these efforts. This may require, for example, careful review of existing standards and procedures for searching and intercepting electronic data during an investigation, as well as support of internationally focused efforts to assure that other countries have the legal and technical capability to conduct and assist in computer crime investigations. Second, the United States should continue with efforts to establish a sound network of international law enforcement agencies and telecommunications carriers to draw on in investigations. The creation and maintenance of such a network can facilitate prompt "trap and trace" and identification of foreign sources of intrusions. Third, the United States should continue to promote efforts to enhance international cooperation in computer crime investigations whether through new international arrangements or traditional mutual legal assistance treaties. The U.S. should ensure that existing and future efforts are broad enough to cover the broadest range of potential sources of attack (i.e. where possible, agreements should cover more than members of P8, OECD, and COE.)

Part Four

A Unified Approach To Criminal Deterrence

Perhaps the most powerful deterrent to cyber crime is a maximally effective criminal enforcement regime. A maximally effective response to computer crime requires the availability of adequate laws and resources at the state, federal and international level.

The effectiveness of a criminal enforcement regime depends in large part on the adequacy of underlying laws and enforcement resources. Adequate laws and resources should ideally support both the prosecutorial and investigative functions. Substantive criminal law should clearly define the prohibited behavior and set forth appropriate punishment. Procedural law should facilitate the conduct of investigations, within clearly defined legal boundaries, while respecting the rights of the accused and of the public. Investigative and prosecutive resources should be allocated in such a way as they remain balanced—they should grow in proportion to one another to avoid gluts and bottlenecks.

Owing to the unique, multi-jurisdictional nature of computer-related offenses, it is insufficient for any single jurisdiction to maximize the effectiveness of only its own law enforcement regime. Savvy computer criminals can choose targets and the routes to those targets, and can, in this way, take advantage of "weak links." Difficulties in investigating and prosecuting offenses occurring across state lines has fueled a need for a more robust national response. Difficulties in investigating and prosecuting offenses across national boundaries has likewise fueled the need for a more robust international response.

It is not enough to strengthen any one of the areas discussed in this paper without seeking to strengthen the others. The enhancement of procedural elements must be done in parallel with enhancement of substantive elements. If one is left with the status quo, improvements in the other will lose their effectiveness. Likewise, focusing on any one of the three major levels of government shown here without the other two will simply permit criminals to focus their activities at the level which provides the least amount of risk for them. Thus, a unified approach is the only one with a high probability of success.

To help understand the scope and complexity of the options, the following chart summarizes them. The reader should note that none of them are mutually exclusive.

Components of Criminal Deterrence

State & Local	LAWS	RESOURCES
INVESTIGATION	procedural	$$, personnel, training, equipment, etc…
PROSECUTION	substantive	$$, personnel, training, etc…

Federal	LAWS	RESOURCES
INVESTIGATION	procedural	$$, personnel, training, equipment, etc…
PROSECUTION	substantive	$$, personnel, training, etc…

International	LAWS	RESOURCES
INVESTIGATION	procedural	$$, personnel, training, equipment, etc…
PROSECUTION	substantive	$$, personnel, training, etc…

APPENDIX A

UNITED STATES CODE ANNOTATED
TITLE 18. CRIMES AND CRIMINAL PROCEDURE
PART I--CRIMES
CHAPTER 47--FRAUD AND FALSE STATEMENTS

Current through P.L. 105-15, approved 5-15-97

§ 1030. Fraud and related activity in connection with computers

(a) Whoever--

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

(5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage;

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if--

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States;

(7) with intent to extort from any person, firm, association, educational institution, financial institution, government entity, or other legal entity, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;

shall be punished as provided in subsection (c) of this section.

(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is--

(1)(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another

offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(2)(A) a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(C), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), if--

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds $5,000;

(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A), (a)(5)(B), or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A), (a)(5)(B), (a)(5)(C), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

[(4) Repealed. Pub.L. 104-294, Title II, § 201(2)(D), Oct. 11, 1996, 110 Stat. 3493]

(d) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under subsections (a)(2)(A), (a)(2)(B), (a)(3), (a)(4), (a)(5), and (a)(6) of this section. Such authority of the United States Secret Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section--

(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2) the term "protected computer" means a computer--

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(B) which is used in interstate or foreign commerce or communication;

(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

(4) the term "financial institution" means--

(A) an institution with deposits insured by the Federal Deposit Insurance Corporation;

(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

(C) a credit union with accounts insured by the National Credit Union Administration;

(D) a member of the Federal home loan bank system and any home loan bank;

(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;

(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;

(G) the Securities Investor Protection Corporation;

(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and

(I) an organization operating under section 25 or section 25(a) of the Federal Reserve Act.

(5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;

(6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter;

(7) the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5; and

(8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information, that--

(A) causes loss aggregating at least $5,000 in value during any 1-year period to one or more individuals;

(B) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment, or care of one or more individuals;

(C) causes physical injury to any person; or

(D) threatens public health or safety; and

(9) the term "government entity" includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. Damages for violations involving damage as defined in subsection (e)(8)(A) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage.

(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5).

APPENDIX B

UNITED STATES PUBLIC LAWS
104th Congress - Second Session
Convening January 3, 1996

PL 104-294 (HR 3723)
October 11, 1996
ECONOMIC ESPIONAGE ACT OF 1996

An Act to amend title 18, United States Code, to protect proprietary economic information, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

<< 18 USCA § 1 NOTE >>

SECTION 1. SHORT TITLE.

This Act may be cited as the "Economic Espionage Act of 1996".

TITLE I--PROTECTION OF TRADE SECRETS

SEC. 101. PROTECTION OF TRADE SECRETS.

<< 18 USCA Ch. 90 >>

(a) IN GENERAL.--Title 18, United States Code, is amended by inserting after chapter 89 the following:

"CHAPTER 90--PROTECTION OF TRADE SECRETS

"Sec.

"1831. Economic espionage.

"1832. Theft of trade secrets.

"1833. Exceptions to prohibitions.

"1834. Criminal forfeiture.

"1835. Orders to preserve confidentiality.

"1836. Civil proceedings to enjoin violations.

"1837. Conduct outside the United States.

"1838. Construction with other laws.

"1839. Definitions.

<< 18 USCA § 1831 >>

"§ 1831. Economic espionage

"(a) IN GENERAL.--Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly--

"(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;

"(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;

"(3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

"(4) attempts to commit any offense described in any of paragraphs (1) through (3); or

"(5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,

shall, except as provided in subsection (b), be fined not more than $500,000 or imprisoned not more than 15 years, or both.

"(b) ORGANIZATIONS.--Any organization that commits any offense described in subsection (a) shall be fined not more than $10,000,000.

<< 18 USCA § 1832 >>

"§ 1832. Theft of trade secrets

"(a) Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly--

"(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;

"(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;

"(3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

"(4) attempts to commit any offense described in paragraphs (1) through (3); or

"(5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,

shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

"(b) Any organization that commits any offense described in subsection (a) shall be fined not more than $5,000,000.

<< 18 USCA § 1833 >>

"§ 1833. Exceptions to prohibitions

"This chapter does not prohibit--

"(1) any otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State; or

"(2) the reporting of a suspected violation of law to any governmental entity of the United States, a State, or a political subdivision of a State, if such entity has lawful authority with respect to that violation.

<< 18 USCA § 1834 >>

"§ 1834. Criminal forfeiture

"(a) The court, in imposing sentence on a person for a violation of this chapter, shall order, in addition to any other sentence imposed, that the person forfeit to the United States--

"(1) any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; and

"(2) any of the person's property used, or intended to be used, in any manner or part, to commit or facilitate the commission of such violation, if the court in its discretion so determines, taking into consideration the nature, scope, and proportionality of the use of the property in the offense.

"(b) Property subject to forfeiture under this section, any seizure and disposition thereof, and any administrative or judicial proceeding in relation thereto, shall be governed by section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except for subsections (d) and (j) of such section, which shall not apply to forfeitures under this section.

<< 18 USCA § 1835 >>

"§ 1835. Orders to preserve confidentiality

"In any prosecution or other proceeding under this chapter, the court shall enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws. An interlocutory appeal by the United States shall lie from a decision or order of a district court authorizing or directing the disclosure of any trade secret.

<< 18 USCA § 1836 >>

"§ 1836. Civil proceedings to enjoin violations

"(a) The Attorney General may, in a civil action, obtain appropriate injunctive relief against any violation of this section.

"(b) The district courts of the United States shall have exclusive original jurisdiction of civil actions under this subsection.

<< 18 USCA § 1837 >>

"§ 1837. Applicability to conduct outside the United States

This chapter also applies to conduct occurring outside the United States if--

"(1) the offender is a natural person who is a citizen or permanent resident alien of the United States, or an organization organized under the laws of the United States or a State or political subdivision thereof; or

"(2) an act in furtherance of the offense was committed in the United States.

<< 18 USCA § 1838 >>

"§ 1838. Construction with other laws

"This chapter shall not be construed to preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret, or to affect the otherwise lawful disclosure of information by any Government employee under section 552 of title 5 (commonly known as the Freedom of Information Act).

<< 18 USCA § 1839 >>

"§ 1839. Definitions

"As used in this chapter--

"(1) the term 'foreign instrumentality' means any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government;

"(2) the term 'foreign agent' means any officer, employee, proxy, servant, delegate, or representative of a foreign government;

"(3) the term 'trade secret' means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes,

whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if--

"(A) the owner thereof has taken reasonable measures to keep such information secret; and

"(B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public; and

"(4) the term 'owner', with respect to a trade secret, means the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed.".

<< 18 USCA Ch. 1 >>

(b) CLERICAL AMENDMENT.--The table of chapters at the beginning part I of title 18, United States Code, is amended by inserting after the item relating to chapter 89 the following:

"90. Protection of trade secrets ..... 1831".

<< 42 USCA § 10604 NOTE >>

(c) REPORTS.--Not later than 2 years and 4 years after the date of the enactment of this Act, the Attorney General shall report to Congress on the amounts received and distributed from fines for offenses under this chapter deposited in the Crime Victims Fund established by section 1402 of the Victims of Crime Act of 1984 (42 U.S.C. 10601).

<< 18 USCA § 2516 >>

SEC. 102. WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS.

Section 2516(1)(c) of title 18, United States Code, is amended by inserting "chapter 90 (relating to protection of trade secrets)," after "chapter 37 (relating to espionage),".

TITLE II--NATIONAL INFORMATION INFRASTRUCTURE PROTECTION ACT OF 1996.

<< 18 USCA § 1030 >>

SEC. 201. COMPUTER CRIME.

Section 1030 of title 18, United States Code, is amended--

(1) in subsection (a)--

(A) in paragraph (1)--

(i) by striking "knowingly accesses" and inserting "having knowingly accessed";

(ii) by striking "exceeds" and inserting "exceeding";

(iii) by striking "obtains information" and inserting "having obtained information";

(iv) by striking "the intent or";

(v) by striking "is to be used" and inserting "could be used"; and

(vi) by inserting before the semicolon at the end the following: "willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it";

(B) in paragraph (2)--

(i) by striking "obtains information" and inserting "obtains--

"(A) information"; and

(ii) by adding at the end the following new subparagraphs:

"(B) information from any department or agency of the United States; or

"(C) information from any protected computer if the conduct involved an interstate or foreign communication;";

(C) in paragraph (3)--

(i) by inserting "nonpublic" before "computer of a department or agency";

(ii) by striking "adversely"; and

(iii) by striking "the use of the Government's operation of such computer" and inserting "that use by or for the Government of the United States";

(D) in paragraph (4)--

(i) by striking "Federal interest" and inserting "protected"; and

(ii) by inserting before the semicolon the following: "and the value of such use is not more than $5,000 in any 1-year period";

(E) by striking paragraph (5) and inserting the following:

"(5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

"(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

"(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage;"; and

(F) by inserting after paragraph (6) the following new paragraph:

"(7) with intent to extort from any person, firm, association, educational institution, financial institution, government entity, or other legal entity, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;";

(2) in subsection (c)--

(A) in paragraph (1), by striking "such subsection" each place that term appears and inserting "this section";

(B) in paragraph (2)--

(i) in subparagraph (A)--

(I) by inserting ", (a)(5)(C)," after "(a)(3)"; and

(II) by striking "such subsection" and inserting "this section";

(ii) by redesignating subparagraph (B) as subparagraph (C);

(iii) by inserting immediately after subparagraph (A) the following:

"(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), if--

"(i) the offense was committed for purposes of commercial advantage or private financial gain;

"(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

"(iii) the value of the information obtained exceeds $5,000;"; and

(iv) in subparagraph (C) (as redesignated)--

(I) by striking "such subsection" and inserting "this section"; and

(II) by adding "and" at the end;

(C) in paragraph (3)--

(i) in subparagraph (A)--

(I) by striking "(a)(4) or (a)(5)(A)" and inserting "(a)(4), (a)(5)(A), (a)(5)(B), or (a)(7)"; and

(II) by striking "such subsection" and inserting "this section"; and

(ii) in subparagraph (B)--

(I) by striking "(a)(4) or (a)(5)" and inserting "(a)(4), (a)(5)(A), (a)(5)(B), (a)(5)(C), or (a)(7)"; and

(II) by striking "such subsection" and inserting "this section"; and

(D) by striking paragraph (4);

(3) in subsection (d), by inserting "subsections (a)(2)(A), (a)(2)(B), (a)(3), (a)(4), (a)(5), and (a)(6) of" before "this section.";

(4) in subsection (e)--

(A) in paragraph (2)--

(i) by striking "Federal interest" and inserting "protected";

(ii) in subparagraph (A), by striking "the use of the financial institution's operation or the Government's operation of such computer" and inserting "that use by or for the financial institution or the Government"; and

(iii) by striking subparagraph (B) and inserting the following:

"(B) which is used in interstate or foreign commerce or communication;";

(B) in paragraph (6), by striking "and" at the end;

(C) in paragraph (7), by striking the period at the end and inserting "; and"; and

(D) by adding at the end the following new paragraphs:

"(8) the term 'damage' means any impairment to the integrity or availability of data, a program, a system, or information, that--

"(A) causes loss aggregating at least $5,000 in value during any 1-year period to one or more individuals;

"(B) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment, or care of one or more individuals;

"(C) causes physical injury to any person; or

"(D) threatens public health or safety; and

"(9) the term 'government entity' includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country."; and

(5) in subsection (g)--

(A) by striking ", other than a violation of subsection (a)(5)(B),"; and

(B) by striking "of any subsection other than subsection (a)(5)(A)(ii)(II)(bb) or (a)(5)(B)(ii)(II)(bb)" and inserting "involving damage as defined in subsection (e)(8)(A)".

TITLE V--USE OF CERTAIN TECHNOLOGY TO FACILITATE CRIMINAL CONDUCT

<< 18 USCA § 3552 NOTE >>

SEC. 501. USE OF CERTAIN TECHNOLOGY TO FACILITATE CRIMINAL CONDUCT.

(a) INFORMATION.--The Administrative Office of the United States courts shall establish policies and procedures for the inclusion in all presentence reports of information that specifically identifies and describes any use of encryption or scrambling technology that would be relevant to an enhancement under section 3C1.1 (dealing with Obstructing or Impeding the Administration of Justice) of the Sentencing Guidelines or to offense conduct under the Sentencing Guidelines.

(b) COMPILING AND REPORT.--The United States Sentencing Commission shall--

(1) compile and analyze any information contained in documentation described in subsection (a) relating to the use of encryption or scrambling technology to facilitate or conceal criminal conduct; and

(2) based on the information compiled and analyzed under paragraph (1), annually report to the Congress on the nature and extent of the use of encryption or scrambling technology to facilitate or conceal criminal conduct.