Unit 4: Avenues for Prosecution and Government Efforts

4

SUBJECT CODE: PGDCL 104

DIGITAL RECORDS AND CYBER FORENSICS

BLOCK 3 – ROLE AND ANALYSIS OF CYBER FORENSICS

UNIT 4 – AVENUES FOR PROSECUTION AND GOVERNMENT EFFORTS

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- The evolution of computer-specific statutes
- Terrorist surveillance program
- Virtual Global Taskforce

1.2 INTRODUCTION

The advent of computer crime has resulted in a myriad of problems for law enforcement administrators. The lack of resources available to small agencies, the traditional apathy toward nonviolent crime, and the reluctance of legislative action have enabled many computer criminals to act with virtual impunity. While it is anticipated that an increase in technology-specific legislation and the modification of extant statutes are forthcoming, lawmakers should evaluate existing federal and state law for prosecutorial avenues currently available. This would empower local agencies and reduce demands on federal agencies.[105]

Traditionally, state and local officials have been forced to rely exclusively on the expertise of better-trained, better-funded federal agencies. Unfortunately, these agencies are incapable of addressing every call for assistance. In addition, they are often unwilling to expend resources on crimes which do not constitute threats to institutional security, the economic infrastructure, the exploitation of children, individual safety, or violation of federal law. (It is unlikely, for example, that a federal agency would assist law enforcement in cases constituting misdemeanour offenses or those offenses which appear to be minor—e.g., installation of Back Orifice on a personal computer, a currently contained virus which destroyed two computers.) Law enforcement administrators should carefully evaluate state statutes. When used creatively, many can be directly applied to criminal activity involving computers. Remember, the method of execution is not an essential element in criminal law. Intent, action, and illegality are inherent in every case of larceny, for example. The method is irrelevant. Thus, an individual who utilizes a computer to steal money from a bank is just as culpable as the individual who resorts to physical theft. At the

[105] Adams, D (2003, December 16) Police prove a match for electronic foe. The Sydney Morning Herald. Retrieved on 28th January 2015 from <http://www.smh.com.au/articles/2003/12/15/1071336882279.html?from=storyrhs>

same time, criminal mischief or vandalism statutes may be utilized to prosecute an individual who remotely alters data. Investigators and administrators must be encouraged to look for the obvious! While there are a variety of statutes which have been enacted to specifically address technological crime, traditional statutes should be utilized where the former is lacking.

1.3 THE EVOLUTION OF COMPUTER-SPECIFIC STATUTES

While many state legislatures have been slow to enact computer-specific statutes, U.S. Congress has reacted more quickly. Thus, measures enabling the prosecution of electronic fraud, hacking, and the theft of intellectual property may be found at the federal level. Unfortunately, this legislation has been buffeted by a variety of legal challenges, the language characterized by jurists as vague and ambiguous.[106] Such efforts can be traced back to 1977 when Senator Abraham Ribicoff (Connecticut) introduced the Federal Computer Systems Protection Act (FSCPA). Although the bill died in committee, it was responsible for initiating dialogue and communication about the threat and potentiality of computer crime.

1.4 COMPUTER FRAUD AND ABUSE ACT, 1986

Originally known as the Counterfeit Access Device and Computer Fraud and Abuse Act (CFAA), Section 1030 of Title 18 of the U.S. Code quickly became the federal government's main weapon in fighting computer crime. Known as the hacking statute, the act in its original form was very narrow in scope, making it a felony to knowingly

> [a]ccess a computer without authorization, or in excess of authorization, in order to obtain classified United States defense or foreign relations information with the intent or reason to believe that such information would be used to harm the United States or to advantage a foreign nation. Second, the 1984 Act made it a misdemeanor knowingly to access a computer without authorization, in excess of authorization, in order to obtain information contained in a financial record of a financial institution or in a consumer file of a consumer reporting agency. Third, the 1984 Act made it a misdemeanour knowingly

[106] Nicholson, Laura J; Shebar, Tom F.; and Weinberg, Meredith R. (2000). "Computer Crimes: Annual White Collar Crime Survey" American Criminal Law Review, 37(2): 207–210

to access a computer without authorization, or in excess of authorization, in order to use, modify, destroy, or disclose information in, or prevent authorized use of, a computer operated for or on behalf of the United States if such conduct would affect the government's use of the computer. The 1984 Act also made it a crime to attempt or to conspire to commit any of the three acts described above.

This legislation proved to be largely ineffective due to the ambiguity of the statutory language and an overemphasis on financial information. (Only one person was successfully prosecuted under the original provisions.) Finally, the 1986 revisions specifically targeted hackers by criminalizing password trafficking.[107]

The act was also used to prosecute early hackers, Herbert Zinn (aka Shadowhawk) and Kevin Mitnick. Shadowhawk was an 18-year-old high school dropout and hacker extraordinaire. Herbert Zinn considered a juvenile at the time of his arrest, was sentenced to nine months and fined $10,000 for breaking into computers of various organizations ranging from NATO to the U.S. Air Force. In addition, Zinn stole 52 AT&T programs valued at over $1 million. Provisions under the act could have resulted in a prison term of 20 years for an adult charged with the same range of offenses. Unlike Zinn, Kevin Mitnick, one of the most infamous hackers in history, had a criminal history the length of which rivals that of many organized crime figures. His successful conviction under this act was a result of his theft of programs valued at more than $1 million from Digital Equipment Corporation and the illegal manipulation of MCI service codes. Since its inception, the act has been modified several times, primarily to clarify terms.

1.5 NATIONAL INFORMATION INFRASTRUCTURE PROTECTION ACT, 1996

While the CFAA was successfully used to prosecute hackers and individuals who exceeded their authorized use, it contained significant limitations in that it only involved those cases in which computer data was a target. It neither included other offenses committed via or in conjunction with computer technology nor included noninterest computers. To remedy this, Congress passed the National Information Infrastructure Protection Act (NIIPA).[108] Originally conceived in 1996,

[107] Pastrikos, Catherine (2004). "Identity Theft Statutes: Which Will Protect Americans the Most?" Albany Law Review, 67(4): 1137–1157

[108] 18 U S C § 1030

NIIPA amended the CFAA to provide for any computer attached to the Internet even if the said computer was not one defined as a federal interest computer or if multiple computers were located in one state. In addition, NIIPA identified broad areas of computer-related crime which involve either accessing computer systems without/or in excess of authorization or causing damage to computers.

These modifications served to close numerous loopholes in the original legislation. By extending protection to all computers connected to the Internet, NIIPA provides for the prosecution of hacker attacks on both intrastate government and financial institution computers. In addition, by removing the trespass requirement and adding an intent or recklessness element, NIIPA provides for the prosecution of insiders who intentionally damage computers. The act further provides for the prosecution of individuals trafficking in passwords or those who attempted to extort money or values from an individual or entity by threatening computer harm. Finally, and perhaps more importantly, NIIPA successfully eliminates several defenses predicated on intent, implied authorization, or value of access. More specifically, NIIPA requires only an intent to access not an intent to cause damage. Thus, individuals attempting to access a protected computer may be prosecuted even if their motivation was not fiduciary.

1.6 EVOLVING CHILD PORNOGRAPHY STATUTES

Although a variety of laws have been enacted to combat the increase in technological crime, none are more emotionally charged than those dealing with child pornography. Beginning in 1977, Congress has attempted to eliminate child pornography. Originally criminalized at the federal level with the Protection of Children against Sexual Exploitation Act of 1977 (PCSE), Congress has periodically revised the legislation to protect children from sexual exploitation in keeping with emerging legal doctrine. However, lower courts have remained divided on new legislation, and the Supreme Court has denied cert on the majority of cases. Traditionally, evaluations of child pornography statutes relied primarily on two Supreme Court decisions, whose interpretation of and application to emerging laws have been diverse.[109]

[109] Stevens, Gina and Doyle, Charles (2003) Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping. Report for Congress: 98-326. Retrieved from <www.epic.org> on March 23, 2012.

In 1982, the Supreme Court evaluated free-speech challenges to child pornography and found them wanting ***(New York v. Ferber).***[110] Uncharacteristically emphatic, the Court ruled that child pornography was outside the scope of the First Amendment, and allowed states to enact blanket prohibitions against visualizations of children engaged in sexual situations. The Child protection act of 1984 (CPA) incorporated this decision. Although the CPA lacked technological specificity, it was widely used against online offenders until the emergence of the Child Protection and Obscenity act of 1988. While both of these acts were designed to protect children from exposure to and inclusion in material deemed to be obscene, these and future acts are continuously challenged by free speech advocates. At the same time, the Supreme Court has remained resolutely silent.

The Congress passed the Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today (PROTECT) Act. Although it sought to reinstate the original provisions housed within the CPPA, it also included a variety of other measures designed to protect children both online and offline. The most important of these included the following:

- Mandatory life sentences for offenders involved in a sex offense against a minor if such offender has had a prior conviction of abuse against a minor;
- The establishment of a program to obtain criminal history/background checks for volunteer organizations;
- Authorization for electronic eavesdropping in cases related to child abuse or kidnapping;
- Prohibition against the pre-trial release of persons charged with specific offenses against children;
- Elimination of the statutes of limitation for child abduction or child abuse;

1.7 IDENTITY THEFT AND ASSUMPTION DETERRENCE ACT, 1998

In October 1998, the Identity Theft and Assumption Deterrence Act (ITADA) was passed by Congress. It was the first act to make the possession of another's personal identifying

[110] *New York v Ferber* 458 U S 747

information a crime, punishable by up to 20 years in prison. More specifically, the act stated that it is unlawful if an individual,[111]

> [k]nowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.

In addition, the law expanded the traditional definition of "means of identification" to include:

- name, social security number, date of birth, official State or government-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer-identification number;
- unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
- unique electronic identification number, address, or routing code; or
- telecommunication identifying information or access device.

1.8 IDENTITY THEFT ENFORCEMENT AND RESTITUTION ACT, 2008

In 2008, Congress formally recognized the financial impact of identity theft by passing the identity theft enforcement and restitution act. Among other provisions, the act broadened the scope of activities which may be prosecuted as identity theft and provided mechanisms for the recovery of direct funds stolen from victims. For example, this act removed the $5,000 threshold for legal action and granted federal jurisdiction in cases involving same state victimization (i.e., it removed the traditional interstate commerce requirement). Perhaps most importantly, the act also provided for the recovery of indirect costs of victimization including lost wages and credit rehabilitation.[112]

1.9 AUTOMATED TARGETING SYSTEM (ATS)

[111] Seifert (2007) Data Mining and Homeland Security

[112] Broadhurst, Roderic (2006) "Developments in the Global Law Enforcement of Cyber-Crime" Policing: An International Journal of Police Strategies and Management, 29(3): 408–433

The Automated Targeting System (ATS) was developed by the Department of Homeland Security within the Treasury Enforcement Communications System. It was designed to screen travellers entering the United States by automobile, aeroplane, or rail. Housed within the Bureau of Customs and Border Protection (CBP), ATS assesses risks for cargo, conveyances, and travellers. There are six categories, or modules, of activity:

- ATS-Inbound—inbound cargo and conveyances (rail, truck, ship, and air);
- ATS-Outbound-outbound cargo and conveyances (rail, truck, ship, and air);
- ATS-Passenger-travelers and conveyances (air, ship, and rail);
- ATS-Land-private vehicles arriving by land;
- ATS-International-cargo targeting for CBP's collaboration with foreign customs authorities; and
- ATS-Trend Analysis and Analytical Selectivity Program (ATS-TAP)-analytical module.

Like other data-mining practices by law enforcement, ATS has been harshly criticized by privacy advocates. In 2006, a suit was filed to suspend the systems as it applied to individuals, or, in the alternative, fully apply all Privacy Act safeguards to any person subjected to the system. Although it was originally designed to enhance customer service in the private sector through customizing profiles of individual shoppers, it has increasingly been employed by criminals and law enforcement alike.[113]

1.10 TERRORIST SURVEILLANCE PROGRAM

First disclosed to the public in December 2005 via a news report, the Terrorist Surveillance Program has been employed by the National Security Agency (NSA) since 2002. Among other things, the program includes the domestic collection, analysis, and sharing of telephone call information. According to statements issued by the president and the Department of Justice, the program is reserved for international calls with links to al Qaeda or related terrorist groups and requires review and reauthorization every 45 days. Privacy advocates have repeatedly expressed concerns over the potential for abuses. Recently, such concerns were validated when it was

[113] Frost and Sullivan (2003) "U S CALEA Market Insight: 6841–63" Retrieved from <http://www.corp.att.com/stateandlocal/docs/US_ CALEA_Market_Insight.pdf on February 12, 2013>

revealed that the NSA had contracted with AT&T, Verizon, and BellSouth to collect information about domestic telephone calls. Although the content of such disclosures is not entirely clear, the compromise of privacy expectations and subsequent erosion of public trust occurred.

CASE STUDY – PRIVACY IN IRAN

In 2010, Nokia Siemens Network was sued by Iranian dissidents who alleged that Nokia had provided the Iranian regime with devices which monitored, eaves-dropped, filtered, and tracked mobile phones.[114] The suit was filed after Isa Sakarkhiz, a prominent Iranian journalist who was instrumental in illuminating Iran's oppression of the press was arrested by government agents who had tracked his mobile phone using Nokia's Intelligence Solutions tool which had been sold to the state-owned telecommunications provider. This Nokia system, which was sold and specifically modified to the government's needs, was composed of (1) a monitoring area which provided for the centralized deep packet inspection of both voice and data communications, and (2) an intelligence area which provided for real-time data mining. Although Nokia claims to have abandoned the software which provides for monitoring of communications, they have declared themselves immune from responsibility as they are a corporation.[115]

1.11 VIRTUAL GLOBAL TASKFORCE (VGT)

In 2003, the Virtual Global Taskforce was created as a collaborative effort between the Australian High Tech Crime Centre, the Child Exploitation and Online Protection Centre (UK), the Royal Canadian Mounted Police, the U.S. Department of Homeland Security, and Interpol.[116] It is designed to deliver low-cost, high-impact initiatives that deter pedophiles and prevent the online exploitation of children. By reducing the confidence of potential perpetrators through the removal of perceptions of anonymity, the group aims to deter online misconduct. Their most notable initiative is to know as Operation Pin. This program involves a Web site which claims to contain images of child exploitation and pornography. Visitors to the site who attempt to

[114] United Nations (2000) "United Nations Manual on the Prevention and Control of Computer-related Criteria"
[115] Department of Defense (May 20, 2003) Report to Congress Regarding the Terrorism Informational Awareness Program, Detailed Information. Retrieved from <www.epic.org on March 23, 2012>
[116] <http://www.virtualglobaltaskforce.com> the homepage of the Virtual Global Taskforce. The group, dedicated to the prevention and prosecution of online child abuse, provides access to the latest news regarding online predators and law enforcement successes

download images are confronted by an online law enforcement presence and informed that they have committed a criminal offense and that information about them has been forwarded to appropriate authorities.

1.12 LET'S SUM UP

Although recognition of the insidious nature of computer crime is increasing, much work remains to be completed on all levels of government. Legislation and the codification of computer criminality must keep abreast of emerging technology. Until such a time, investigators should look to traditional statutes to prosecute individuals committing traditional crimes via electronic means.

Even in areas where state, local, and federal government agencies have enacted regulations to specifically address online criminal behavior, some activity is sure to be over-looked. Thus, law enforcement officials must continue to evaluate the applicability of traditional legislation. The Federal Wire Fraud Act, for example, enables prosecutors to pursue individuals illegally transferring funds, accessing bank computers, and the like. While most computer-specific legislation has tended to be enacted on the federal level, state and local agencies may be able to implement generic statutes of enforcement. For example, although many states have not formally encoded electronic vandalism statutes, innovative departments may still pursue individuals responsible for computer worms or viruses through criminal mischief and destruction of property codes. Local and state law enforcement officials should carefully evaluate local regulations and identify applicable statutes.

1.13 FURTHER READING

- Seifert, Jeffrey W. (2007). Data Mining and Homeland Security: An Overview. CRS Report for Congress. Order Code RL 31798. January 18, 2007.
- International Review of Criminal Policy—United Nations Manual on the Prevention and Control of Computer-Related Crime. Retrieved from http://www.uncjin.org/Documents/EighthCongress.html on February 12, 2013.

- Nicholson, Laura J.; Shebar, Tom F.; and Weinberg, Meredith R. (2000). "Computer Crimes: Annual White Collar Crime Survey." American Criminal Law Review, 37(2): 207–210.
- Stevens, Gina and Doyle, Charles (2003). Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping. Report for Congress: #98-326. Retrieved from www.epic.org on March 23, 2012.
- Seifert, Jeffrey W. (2007). Data Mining and Homeland Security: An Overview. CRS Report for Congress. Order Code RL 31798.
- Poulsen, Kevn (2005). "FBI Retires Its Carnivore." Security Focus. Retrieved from www.securityfocus.com on March 23, 2012.

1.14 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) What is the main aim/objective of the National Information Infrastructure Protection Act, 1996?

NIIPA provides for the prosecution of hacker attacks on both intrastate government and financial institution computers.

2) What are the six categories of Automated Targeting System?

- ATS-Inbound—inbound cargo and conveyances (rail, truck, ship, and air);
- ATS-Outbound-outbound cargo and conveyances (rail, truck, ship, and air);
- ATS-Passenger-travelers and conveyances (air, ship, and rail);
- ATS-Land-private vehicles arriving by land;
- ATS-International-cargo targeting for CBP's collaboration with foreign customs authorities; and
- ATS-Trend Analysis and Analytical Selectivity Program (ATS-TAP)-analytical module.

3) What was the reason behind the enactment of Identity Theft Enforcement and Restitution Act, 2008?

The act broadened the scope of activities which may be prosecuted as identity theft and provided mechanisms for the recovery of direct funds stolen from victims. For example, this act removed the $5,000 threshold for legal action and granted federal jurisdiction in cases involving same state victimization (i.e., it removed the traditional interstate commerce requirement). Perhaps most importantly, the act also provided for the recovery of indirect costs of victimization, including lost wages and credit rehabilitation.

4) **Short notes on the evolution of child pornography?**

- Mandatory life sentences for offenders involved in a sex offense against a minor if such offender has had a prior conviction of abuse against a minor;
- The establishment of a program to obtain criminal history/background checks for volunteer organizations;
- Authorization for electronic eavesdropping in cases related to child abuse or kidnapping;
- Prohibition against the pre-trial release of persons charged with specific offenses against children;
- Elimination of the statutes of limitation for child abduction or child abuse;

1.15 ACTIVITY

Explain briefly the evolution of different statutes that was brought to light with respect to computer-based crimes and the after-effects with respect it? Also, How may traditional statutes be applied to the contemporary phenomenon of computer crime? (1000 words)