UIC John Marshall Journal of Information Technology & Privacy Law

Volume 20
Issue 3 *Journal of Computer & Information Law - Spring 2002*

Article 1

Spring 2002

Transnational Evidence Gathering and Local Prosecution of International Cybercrime, 20 J. Marshall J. Computer & Info. L. 347 (2002)

Susan W. Brenner

Joseph J. Schwerha IV

ARTICLES

TRANSNATIONAL EVIDENCE GATHERING AND LOCAL PROSECUTION OF INTERNATIONAL CYBERCRIME

SUSAN W. BRENNER†
& JOSEPH J. SCHWERHA IV††

I. INTRODUCTION: TWO CASES

A variety of legal and procedural issues can arise when the process of investigating cybercrime requires gathering evidence across national borders.[1] These issues, and the different approaches investigators can

† NCR Distinguished Professor of Law & Technology, University of Dayton School of Law, Dayton, OH, <http://www.cybercrimes.net>. E-mail: Susan.Brenner@notes.udayton.edu.

†† Assistant District Attorney, Washington County, Pennsylvania; Co-Chair, Search & Seizure Working Group – International Cybercrime Project of the American Bar Association's Privacy and Computer Law Committee. E-mail: joe@schwerha.com.

1. *See e.g.* Council of Europe, *Convention on Cybercrime (ETS no. 185), Explanatory Report* ¶¶ 132-33 <http://conventions.coe.int/Treaty/EN/cadreprincipal.htm> (Nov. 8, 2001):

> The technological revolution, which encompasses the 'electronic highway' where numerous forms of communication and services are interrelated and interconnected through the sharing of common transmission media and carriers, has altered the sphere of criminal law and criminal procedure. The ever-expanding network of communications opens new doors for criminal activity in respect of both traditional offences and new technological crimes. Not only must substantive criminal law keep abreast of these new abuses, but so must criminal procedural law and investigative techniques. . . .

Id. at ¶ 132.

> One of the major challenges in combating crime in the networked environment is the difficulty in identifying the perpetrator and assessing the extent and impact of the criminal act. A further problem is caused by the volatility of electronic data, which may be altered, moved or deleted in seconds. For example, a user who is in control of the data may use the computer system to erase the data that is the

take toward dealing with them, are illustrated by the investigations conducted in two high-profile cybercrime cases—the "Invita" case and the "Rome Labs" case.

In the Invita case, which is the more recent of the two, the FBI was called in to investigate a series of intrusions "into the computer systems of businesses in the United States" that emanated from Russia.[2] The attacks targeted:

> Internet Service Providers, e-commerce sites, and online banks in the United States. The hackers used their unauthorized access to the victims' computers to steal credit card . . . and other . . . financial information, and . . . tried to extort money from the victims with threats to expose the sensitive data to the public or damage the victims' computers. The hackers also defrauded PayPal through a scheme in which stolen credit cards were used to generate cash and to pay for computer parts purchased from vendors in the United States.[3]

The FBI identified the Russians—Vasiliy Gorshkov and Alexey Ivanov—responsible for the attacks and used a ruse to entice them to the United States: The FBI created a bogus computer security company called "Invita" located in Seattle, Washington, and brought the hackers to Seattle to "interview" with the company.[4] As part of the "interview," the Russians were asked to hack into a network set up by the FBI, the purpose being to demonstrate their computer skills.[5] Using laptops provided by the FBI, they successfully broke into the network and, in so doing, accessed their computer system—"tech.net.ru"—in Russia.[6] The FBI had previously installed a keystroke logger program on the each of the laptops and the program recorded the usernames and passwords Gorshkov and Ivanov used to access their Russian computers.[7]

As soon as the "interview" was over, agents arrested Gorshkov and Ivanov; they then used the information retrieved by the keystroke logger

---

> subject of a criminal investigation, thereby destroying the evidence. Speed and, sometimes, secrecy are often vital for the success of an investigation.

Id. at ¶ 133.

2. *U.S. v. Gorshkov*, 2001 WL 1024026 at *1 (W.D. Wash. May 23, 2001).

3. Dept. of Justice, *Russian Computer Hacker Convicted by Jury* <http://www.usdoj.gov/criminal/cybercrime/gorshkovconvict.htm> (Oct. 10, 2001).

4. *Id.*

> The break . . . came when Ivanov identified himself in an e-mail while attempting to extort money from a victimized company. . . . FBI agents then found his resumé online and, posing as representatives of a fictitious network security company called Invita, contacted him to offer him a job.

ZDNet News, *Judge Okays Hack of Russian Computers* <http://zdnet.com.com/2100-11-529917.html?legacy=zdnn> (May 30, 2001); *see also Gorshkov*, 2001 WL 1024026 at *1.

5. Dept. of Justice, *supra* n. 3.

6. *Gorshkov*, 2001 WL 1024026 at *1.

7. *Id.*

to access the Russian computers and download files they contained.[8] They did all this without obtaining a warrant.[9]

After being indicted for conspiracy, computer crime and fraud,[10] Gorshkov moved to suppress the evidence obtained from the Russian computers, arguing that it was the product of a search and seizure that (a) violated the Fourth Amendment and/or (b) violated Russian law.[11] The district court denied the motion.[12] As to the FBI's using the keystroke logger program to obtain Gorshkov's password, the court found that Gorshkov did not have a cognizable Fourth Amendment expectation of privacy when he used a "foreign" computer to access his files in Russia.[13] As to the FBI's downloading files from the Russian computer without a warrant, the court held: (a) that the Fourth Amendment did not apply because the computer was in Russia and the Fourth Amendment

---

8. *Id.;* ZDNet News, *supra* n. 4 (FBI downloaded "nearly 250 gigabytes" of data):

> The data copied from the Russian computers provided a wealth of evidence of the men's computer hacking and fraud. They had large databases of credit card information that was stolen from Internet Service Providers. . . . More than 56,000 credit cards were found on the two Russian computers. The Russian computers also contained stolen bank account and other personal financial information of customers of online banking at Nara Bank and Central National Bank - Waco.
>
> The data from the Russian computers revealed that the conspirators had gained unauthorized control over numerous computers . . . and then used those compromised computers to commit a massive fraud involving PayPal and the online auction company e-Bay. . . .

Id.; Dept. of Justice, *supra* n. 3. The FBI was forced to act on its own:

> Typically, U.S. law enforcement would wait on their counterparts in Russia to search the servers. Yet, while the United States has more than 25 mutual legal assistance treaties to aid law enforcement in capturing data in other countries, Russia has signed an agreement to help the U.S. in investigating only some crimes—and computer crimes are not among them.
>
> Nevertheless, the Department of Justice did request assistance from Russian authorities, but without answer. After several unsuccessful attempts to get Russian authorities to cooperate, the FBI—with the help of a security expert—used the usernames and passwords to access the two servers.

Id.; Robert Lemos, *CNET News.com, Tech News, FBI "Hack" Raises Global Security Concerns* <http://news.com.com/2100-1001-256811.html?legacy=cnet&tag=tp_pr> (May 1, 2001). Mutual legal assistance treaties are discussed in Section II of accompanying text.

9. Dept. of Justice, *supra* n. 3 (stating that "[T]he FBI copied voluminous data from the accounts . . . and then obtained a search warrant"); *Gorshkov*, 2001 WL 1024026 at *1.

10. Dept. of Justice, *supra* n. 3.

11. *Gorshkov*, 2001 WL 1024026 at **3-4.

12. *Id.* at *5.

13. *Id.* at *2:

> When Defendant sat down at the networked computer at the Invita undercover site, he knew that the systems administrator could and likely would monitor his activities. Indeed, the undercover agents told Defendant that they wanted to watch . . . to see what he was capable of doing. With the agents . . . looking over his shoulder, Defendant . . . logged on to an account at a computer named 'freebsd.tech net.ru.'. Therefore the Defendant had no expectation of privacy in his actions on the Invita computer.

Id.

does not apply to searches and seizures conducted outside the territorial boundaries of the United States;[14] and (b) that if the Fourth Amendment did apply, the agents' actions were "reasonable" because they were justified by the exigent circumstances exception to the warrant requirement.[15] Finally, the court held that Russian search and seizure law did not apply to the agents' conduct.[16]

The second case began when system administrators at the Rome Air Development Center ("Rome Labs") at Griffiss Air Force Base in New York discovered hackers had installed password sniffer programs on all

---

14. *Id.* at *3:

> Under *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990), the Fourth Amendment does not apply to a search or seizure of a non-resident alien's property outside the territory of the United States. . . . [T]he computers accessed by the agents were located in Russia, as was the data contained on those computers that the agents copied. Until the copied data was transmitted to the United States, it was outside the territory of this country and not subject to the protections of the Fourth Amendment.

Id.

15. *Id.* at *4:

> The . . . agents had probable cause to believe that the Russian computers contained evidence of crimes. The agents had good reason to fear that if they did not copy the data, Defendant's coconspirators would destroy the evidence, or make it unavailable before any assistance could be obtained from Russian authorities. The agents made 'reasonable efforts' to reconcile their needs with Defendant's privacy interest by copying the data, without . . . examining its contents until a search warrant could be obtained. . . . Therefore, . . . because the agents were acting under exigent circumstances, the agents' actions in accessing the Russian computers and downloading the data without a warrant were fully legal and the evidence should not be suppressed.

Id. (footnotes omitted)

16. *Id.* at *4 n. 4. The court noted that "even if it were to apply, the agents sufficiently complied with the relevant portions of the Criminal Process Code of Russia." *Id.; but see* Kevin Poulsen, *BusinessWeek Online, California Indictment in Russian Hacks* <http://www.businessweek.com/technology/content/jul2001/tc20010726_774.htm> (June 21, 2001) (stating search of the Russian computers "apparently violate[d] Article 272 of the Russian Criminal Code, which punishes 'Unlawful Access to Computer Information' with up to two years in prison"); *see* American Russian Law Institute, *Penal Code of the Russian Federation* <http://russianlaw.org/res-compl.htm> (June 13, 1996) (stating "[u]nwarranted access to computer information protected by the law that is information on a computer carrier, in a computer, a computer system, or their network, if such actions has resulted in destruction, blocking, modification or copying of information, disruption in the operation of a computer, a computer system or a network thereof, shall be punishable with a fine in the amount of two hundred to five hundred minimum wages or in the amount of wages or other income of the convict during a period from two to five months, or corrective labor for a term from six months to one year, or imprisonment for up to two years"); *see generally* U.S. Dept. of State, *Fact Sheet: Mutual Legal Assistance Treaty Between the Untied States and Russia* <http://usinfo.state.gov/topical/pol/terror/02020108.htm> (Jan. 31, 2002). New U.S. - Russia treaty "replaces the Mutual Legal Assistance Agreement (signed in 1995) and. . . . is an important new tool to pursue . . . offenses such as transnational organized crime, global terrorism, . . . computer crime and money laundering". *Id.*

the Rome Labs networks.[17] In addition to gaining access to information on the Rome Labs computers, the hackers—who called themselves "Datastream Cowboy" and "Kuji"—used Rome Labs' systems to attack other targets around the world.[18] The Air Force's Office of Special Investigations ("AFOSI") used informants to identify "Datastream Cowboy" as Richard Pryce, a 16-year-old citizen of the United Kingdom.[19]

Having previously established a relationship with New Scotland Yard officers, AFOSI agents contacted them; New Scotland Yard had British Telecom monitor Pryce's telephone lines.[20] The monitoring showed, for example, that his path of attack in one venture was

> through systems in multiple countries in South America, multiple countries in Europe, and also through Mexico and Hawaii. . . . From Rome Labs he was able to attack systems via the Internet at NASA'S, Jet Propulsion Laboratory in California and their Goddard Space Flight Center in Greenbelt, MD.[21]

Working together, AFOSI and New Scotland Yard developed probable cause to believe evidence of the intrusions would be found at Pryce's home, and New Scotland Yard used the information to obtain a warrant to search his residence.[22] New Scotland Yard executed the warrant and seized incriminating evidence.[23] Pryce was prosecuted and eventually pled guilty to twelve counts of hacking.[24]

Both cases resulted in the apprehension and prosecution of the perpetrators, but they differ conceptually. Parsing these differences reveals

---

17. Richard Power, *Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace,* 66-67 (QUE 2000). "Rome Lab is the Air Force's premier command and control research facility. Its projects include artificial intelligence system, radar guidance systems, and target detection and tracking systems." U.S. Senate, *Security in Cyberspace,* Appendix B <http://www.fas.org/irp/congress/1996_hr/s960605b.htm> (June 5, 1996).

18. Power, *supra* n. 17; U.S. Senate, *supra* n. 17 (indicating that "[a]fter the attackers had compromised . . . the . . . systems at Rome Labs the intruders used Rome Labs systems a. . . to attack other military, government, commercial, and academic systems world-wide, compromising user accounts, installing sniffer programs, and downloading large volumes of data from penetrated systems").

19. Power, *supra* n. 17, at 67-70; U.S. Senate, *supra* n. 17 (stating that "Datastream [Cowboy] even provided the informant with his home telephone number for his own hacker bulletin board system he had established").

20. Power, *supra* n. 17, at 70-71.

21. U.S. Senate, *supra* n. 17. Datastream Cowboy also attacked other military systems, including a system at SHAPE (NATO Headquarters). *See id.* He also broke into "a system in Korea and . . . obtained . . . data stored on the Korean Atomic Research Institute system." *Id.*

22. Power, *supra* n. 17, at 72.

23. *Id.*

24. *Id. at* 74-75. His colleague Kuji was also apprehended and charged, but the prosecution wound up offering "no evidence" against him, which resulted in his being acquitted of all charges. Mathew Bevan, *Who is the Real Kuji?* <http://www.bogus.net/kuji/kuji_who.htm> (last updated Mar. 28, 2000).

two different modes of approaching the legal issues involved in transborder searches and seizures.

The *Gorshkov* court at least implicitly relied on the premise that the law governing a search and/or seizure is the law of the state where the crime was committed, in this instance, the law of the United States. The court used this premise to justify its applying United States law to uphold the FBI's actions and its refusal to apply Russian law to those actions.[25] In this, it erred: The *Gorshkov* premise cannot provide the conceptual basis for approaching the legal issues involved in transborder searches and seizures because it would inevitably allow the victim state to transgress upon another state's sovereignty by searching and seizing property belonging to that state's citizens, property that is physically located within that state's territorial boundaries.[26]

The agents in the Rome Labs investigation, on the other hand, operated on the premise that the law governing a search and/or seizure is the law of the state where the property to be searched or seized is located. The American agents therefore contacted their counterparts in Britain and cooperated with New Scotland Yard officers, who, in turn, ensured that the evidence in possession of British citizens was collected in accordance with British law. One virtue of this approach is that it protects the rights of citizens by assuring them the protections established by their local law; another virtue is that it maintains comity by ensuring that law enforcement officers from one state do not unilaterally take action against property that is owned by a citizen of another state and that physically resides in that state.[27] The implementation of this premise of

---

25. *See supra* nn. 14-16 and accompanying text. The court applied United States law—in the form of Supreme Court decisions—to hold that the Fourth Amendment did not apply to searches and seizures conducted outside the geographical territory of the United States. *Id.*

26. Dept. of Justice, *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet, A Report of the President's Working Group in Unlawful Conduct on the Internet* <http://www.usdoj.gov/criminal/cybercrime/unlawful.htm#CHALLENGES> (Mar. 9, 2000) [hereinafter *The Electronic Frontier*]:

> If law enforcement agents in the United States access a computer and seize data from a computer, the fact that they have a search warrant makes that action lawful. If, with that same search warrant, they remotely access a Canadian computer (from the United States), might this constitute a criminal act under Canadian law notwithstanding the existence of the U.S. warrant? To the extent that agents know nothing more than an Internet protocol address . . . the physical location of the computer to be searched may not be accurately known. Yet ignorance of physical location may not excuse a transborder search; consider how we would react to a foreign country's 'search' of our defense-related computer systems based upon a warrant from that country's courts.

See e.g. supra n. 16.

27. *See e.g.* Henry H. Perritt, Jr., *Jurisdiction in Cyberspace,* 41 Vill. L. Rev. 1, 87 (1996) (indicating that "a foreign search by U.S. officers potentially offends the sovereignty of the foreign state in which it occurred, thus potentially subjecting the United States and

course requires cooperation between law enforcement officials in various states.[28]

While informal cooperation proved effective in the Rome Labs investigation, that investigation only required the cooperation of officers from two culturally compatible nations; informal cooperation can be a less reliable mechanism when multiple states with varying legal systems are involved. In an effort to resolve the uncertainties resulting from informal cooperation, the Council of Europe prepared its Convention on Cybercrime,[29] which requires signatory nations to adopt legislation or do whatever else is required to ensure "international co-operation . . . to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence."[30] The G8 (United States of America, Japan, Germany, Britain, France, It-

---

its citizens to retaliation, and the officials performing the search and seizure to punishment by the foreign country").

28. The FBI agents conducting the Invita operation did try to obtain the cooperation of Russian authorities, but were unsuccessful in doing so. *See supra* n. 8.

29. It took four years and twenty-seven drafts before the final version of the Convention was submitted to the European Committee on Crime Problems at its 50th Plenary Session in June of 2001. Council of Europe, *supra* n. 1, at ¶¶ 7-15 [hereinafter Council of Europe, *Report*]. The Convention was opened for signature by the member states on November 23, 2001. It contains a Preamble and four Chapters: the Preamble explains the goals the Convention was intended to achieve; Chapter I defines terms used in the Convention; Chapter II specifies "measures to be taken at the national level"; Chapter III addresses "international co-operation"; and Chapter IV deals with administrative matters, such as the period during which the Convention will be open for signature and the date on which it will enter into force. Council of Europe, *Convention on Cybercrime,* Article 23 <http://conventions.coe.int/Treaty/EN/cadreprincipal.htm> (Nov. 23, 2001) [hereinafter Council of Europe, *Convention*].

30. Council of Europe, *Convention, supra* n. 29, at Article 23; *see also* Council of Europe, *Convention, supra* n. 29, at Article 25, ¶ 1 (stating that "[T]he Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data or for the collection of evidence in electronic form of a criminal offence"). The principles of cooperation enunciated in the Convention on Cybercrime "requires Parties to provide extensive cooperation to each other, and to minimize impediments to the smooth and rapid flow of information and evidence internationally." Council of Europe, *Report, supra* n. 1, at ¶ 242. The general obligation of cooperation extends "to all criminal offences related to computer systems and data . . . as well as to the collection of evidence in electronic form of a criminal offence." *Id.* This means that either where the crime is committed by use of a computer system, or where an ordinary crime not committed by use of a computer system (e.g., a murder) involves electronic evidence, the terms of the Convention are applicable. *Id.* at ¶ 243. The Convention does provide for "a different scope of application" of its requirements with regard to extradition, mutual assistance involving the real-time collection of traffic data and mutual assistance involving the interception of content data. *See id.; see also* Council of Europe, *Convention, supra* n. 29, at Article 24, 33-34.

aly, Canada and Russia) has recommended similar measures.[31]

II. TRANSNATIONAL EVIDENCE-GATHERING

A. WHERE TO START?

The first thing an investigator should determine is what formal and informal devices are available to search for and/or seize evidence located in another country. As the Rome Labs investigation illustrates, informal methods of cooperation can be very effective; indeed, they are usually the most expeditious means of obtaining evidence.[32] The formal devices include "requests under mutual legal assistance treaties ("MLATs"), letters rogatory in the absence of a treaty or executive agreement, and subpoenas directed to U.S. citizens and permanent residents of the United States located abroad."[33]

---

31. Dept. of Justice, *Meeting of the Justice and Interior Minister of the Eight, Communique* <http://www.cybercrime.gov/communique.htm> (Dec. 9-10, 1997); *see also* Section II(C) of the accompanying text.

32. Dept. of Justice, *270 Type of Assistance Needed* <http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/crm00276.htm> (Oct. 1997) (stating that "some tasks may best be accomplished by informal means while others can only be done by a formal approach"). The most common informal methods are "police-to-police requests (often accomplished through United States law enforcement agents stationed at our embassies abroad)" and requests made "through Interpol for evidence (or . . . information) that can be obtained by foreign police without an official request". Dept. of Justice, *278 Informal Means* <http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/crm00278.htm> (Oct. 1997). This section of the *Criminal Resource Manual* also lists other informal methods. Even informal methods are not always effective, as this example from an Australian Parliament report illustrates:

> Mr Prince. . . gave a detailed account of attempts by his investigators to use alternative international mechanisms, such as Interpol and the International High Tech Crime Contact list, both accessed through the AFP. In one case, a complaint was received by the [Western Australia] Police Service in November 1999 relating to an extortion attempt via email. Police immediately secured evidence and imaged hard drives. The email header information led to a source Internet Protocol registered to an UK ISP. The ISP complied with a request to preserve the relevant logs for evidentiary purposes. However, the local UK police were reluctant to assist until the request came through official channels. The request was made through formal channels, through the Bureau of Criminal Intelligence within the WA Police Service and Interpol. A short response, insufficient to base further action on, was received over six months later, effectively bringing the inquiry to a halt. Mr. Prince noted a second case where no response had been received after three months.

Australian Parliament, Joint Committee on the National Crime Authority, *The Law Enforcement Implications of New Technology* <http://www.aph.gov.au/senate/committee/nca_ctte/law_enforcement/law_enforcement.pdf> (Aug. 2001) [hereinafter Australian Parliament, *Law Enforcement*]. At the time these events occurred, Kevin Prince was the Western Australia Police Minister. *See id.*

33. Perritt, *supra* n. 27, at 84. There are also executive agreements that provide for assistance in certain types of cases. *See* Dept. of Justice, *277 Executive Agreement and*

The investigator should therefore identify the country from which evidence is to be sought and determine whether a mutual legal assistance treaty encompassing the evidence exist between the United States and that country.[34] The procedure for obtaining assistance under an MLAT is "generally faster and more reliable" than the older process of using letters rogatory.[35] If an MLAT is in force that applies to the type

---

Memoranda of Understanding on Mutual Assistance in Criminal Matters <http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/crm00277.htm> (Oct. 1997).

34. *See e.g. Mexico-United States: Mutual Legal Assistance Cooperation Treaty* (Dec. 9, 1987), Sen. Treaty Doc. No. 100-113; *Canada-United States: Treaty on Mutual Legal Assistance in Criminal Matters* (Mar. 18, 1985), 24 I.L.M. 1092; *see also* Dept. Of Justice, *268 Location of the Evidence* <http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/crm00268.htm#268> (Oct. 1997). The investigator will have to demonstrate that evidence is located in that country. *See id.* "Foreign cooperation depends on the existence of articulable facts indicating that evidence is located in a particular jurisdiction." *Id.*

35. *See infra* n. 38.

> The limits of letters rogatory prompted countries to develop other methods of securing evidence in criminal matters. First, countries have entered into a variety of multilateral and bilateral arrangements containing procedures for obtaining and providing legal assistance in criminal matters. The first major legal assistance treaty, the European Convention on Mutual Assistance in Criminal Matters, entered into force in 1962. Its signatories undertook 'to afford each other . . . the widest measure of mutual assistance' in investigating criminal offenses. . . . The European experience spurred the United States to develop bilateral agreements containing similar obligations. . . . The United States currently has MLATs in force with more than forty countries. . . . The treaties generally require the requested state to locate persons believed to be in its territory, to execute requests for searches and seizures, to compel a witness's appearance and production of documents, and to produce records in the government's possession. . . .

Id.; Patricia L. Bellia, *Chasing Bits Across Borders,* 2001 U. Chi. Legal F. 35, 51-53 (footnotes omitted); *see e.g.* Dept. of Justice, *276 Treaty Request* <http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/crm00276.htm> (Oct. 1997) (stating that "The MLAT will define the obligation to provide assistance, the scope of assistance, and the contents of the request"); *see also Testimony of Assistant Attorney General James Robinson Before the Banking and Financial Services Committee, U.S. House of Representatives* <http://usinfo.state.gov/topical/econ/bribes/robinson4.htm> (Sept. 22, 1999):

> Under the MLATs, each party is obliged to assist the other in the investigation, prosecution, and other proceedings related to criminal matters. Assistance may include taking testimony or statements, obtaining documents or items, serving documents, transferring persons in custody, conducting searches and seizures, assistance in forfeiture proceedings . . . and any other assistance not prohibited by the Requested State's laws. MLATs usually provide for assistance without regard to whether the matter under investigation would be a crime in both countries, and are especially helpful in assuring that the evidence produced is in a form that is admissible at trial in the Requesting State.
>
> Typical provisions found in MLATs include: (1) a designation of a 'Central Authority' or implementing official, in each State, permitting direct communication between law enforcement communities for purposes of the MLAT; (2) a limited number of agreed bases for denying assistance (e.g., a request related to a political or military offense or a request that would prejudice the sovereignty, security or similar essential interests of the Requested State); and (3) a description of the form and contents of a request, the manner in which requests shall be executed, and the costs that each side will assume in connection with MLAT matters. The

of evidence being sought,[36] the investigator should prepare a request for assistance pursuant to the treaty.[37] If no treaty is in force, the investigator may have to rely on the letter rogatory procedure, which can be very time-consuming.[38]

MLATs usually specify clearly upon request, the Requesting State may use or reveal the evidence produced pursuant to MLAT requests only for the purpose for which it was requested.

Id.; MLATs are not "the only treaties that provide for legal assistance: some extradition treaties and many tax treaties contain such provisions." Dept. of Justice, *276 Treaty Requests* <http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/crm00276.htm> (Oct. 1997).

36. For an instance in which it did not, *see supra* n. 8.

37. *See* Dept. of Justice, *276 Treaty Requests* <http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/crm00276.htm> (Oct. 1997). Each treaty to which the United States is a party includes a provision requiring the requested country to conduct searches and seizures on behalf of the requesting country if the request includes information justifying such action under the laws of the requested country. *See* Perritt, *supra* n. 27, at 84. Even the Council of Europe's Convention on Cybercrime incorporates the provisions of applicable MLAT's. *See* Council of Europe, *Report, supra* n. 1 (stating that "the obligation to provide mutual assistance is generally to be carried out pursuant to the terms of applicable mutual legal assistance treaties, laws and arrangements").

38. *See e.g.* Bellia, *supra* n. 35, at 50:

> Historically, countries seeking evidence from other states relied on formal 'letters rogatory' in both civil and criminal matters. Letters rogatory are requests for evidence issued by a court in one country, transmitted through diplomatic channels and seeking the assistance of a court in another country. These letters, however, have limited use. Because courts may issue letters rogatory only in pending cases, from the perspective of the United States they cannot be used to obtain foreign evidence before the grand jury stage of a criminal proceeding. In addition, states honor letters rogatory only as a matter of comity and often provide the requested evidence after a substantial delay.

Id. (footnotes omitted); *see also,* Mark K. Gyandoh, *Foreign Evidence-Gathering: What Obstacles Stand in the Way of Justice?,* 15 Temp. Int'l & Comp. L.J. 81, 86-87 (2001):

> The most common of the laws available to gather information abroad is the letter rogatory codified under 28 U.S.C.S. § 1781 et seq. (1999). The letter rogatory is a 'medium, in effect, whereby one country, speaking through one of its courts, requests another country, acting through its own courts and by methods of court procedure peculiar thereto and entirely within the latter's control, to assist the administration of justice in the former country.' Section 1781 pertains to how the United States may execute a letter rogatory to a foreign tribunal, while § 1782 applies to the receipt of letters rogatory requests from foreign nations. Under § 1781, the Department of State is vested with the power to transmit a letter rogatory to a 'foreign or international tribunal, officer, or agency to whom it is addressed and its return in the same manner.'. . . [FN22]
>
> Letters rogatory may be used for 'providing notice, serving summons, locating individuals, examining both voluntary and involuntary witnesses, document inspection,' and producing evidence in general. . . .
>
> If the activity for which a requesting country wants the requested country to perform is not permissible in that country, then the investigation comes to an immediate end. This is because the foreign country can only honor requests which fall within its courts' procedures and control.

Id. (footnotes omitted) (quoting *The Sgine*, 37 F. Supp. 819, 820 (E.D. La. 1941). Dept. of Justice, *275 Letters Rogatory* <http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/crm00275.htm> (Oct. 1997). "A letter rogatory is a request from a judge in the

Another critical issue is determining whether the evidence being sought pertains to conduct that is illegal in the country whose assistance is being requested.[39] Some countries only grant assistance if the conduct is illegal under their own law.[40] This can be a significant impediment.[41]

United States to the judiciary of a foreign country requesting the performance of an act which, if done without the sanction of the foreign court, would constitute a violation of that country's sovereignty." *Id.* The general procedure for obtaining a letter rogatory is outlined in this section of the *Criminal Resource Manual.*

39. Australian Parliament, *Law Enforcement, supra* n. 32:

> 3.53 The deficiencies of the current mutual assistance scheme were addressed in four of the seven submissions received from government/police service representatives of the States and the Northern Territory. The Queensland Minister for Police and Corrective Services, the Hon. Tom Barton, noted:
> Jurisdictional differences in what constitutes a crime inhibits international cooperation at an operational level. While overarching mutual assistance agreements may be in place between jurisdictions, these often require that the grounds on which assistance is sought be defined as a crime both in the requesting country and in the assisting jurisdiction.
> 3.54 The Victorian Government submitted:
> The effectiveness of the traditional means of cooperation through Mutual Assistance applications is already compromised by administrative delays. The situation is aggravated by technology facilitated crime crossing borders instantaneously. The need to develop and maintain consistent legislation.

Id. (footnotes omitted).

40. *See* Dept. of Justice, *269 Intended Use of the Evidence* <http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/crm00269.htm> (Oct. 1997); *see also The Electronic Frontier, supra* n. 26:

> [D]ual criminality . . . is often required (e.g., U.S./Netherlands MLAT). . . . [A] country can refuse a request if the request 'relates to conduct in respect of which powers of search and seizure would not be exercisable in the territory of the Requested Party in similar circumstances' (e.g., U.S./U.K. MLAT). . . . [S]ome MLATs . . . permit assistance only if dual criminality exits and if the offense is extraditable . . . Therefore, if one country does not criminalize computer misuse . . . extradition may be prohibited.

Id.; Some countries also exclude assistance for specific offenses or specific types of cases (such as tax prosecutions) and some "limit assistance to the purpose stated in the request," which means the evidence cannot be used for another purpose without obtaining the express permission of the country that provided it. *See* Dept. of Justice, *269 Intended Use of the Evidence* <http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/crm00269.htm> (Oct. 1997).

41. *See e.g. The Electronic Frontier, supra* n. 26 (stating that when Swiss hackers attacked the San Diego Supercomputing Center, U.S. officials sought help from the Swiss but the effort failed because the countries did not have similar laws banning hacking). The Council of Europe's Convention on Cybercrime attempts to alleviate this problem somewhat by providing, among other things that when the party whose assistance is being requested "is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominates the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws." Council of Europe, *Convention, supra* n. 29, at Article 25. As the Explanatory Report accompanying the Convention explains:

> This provision is essentially a definition of dual criminality for purposes of mutual assistance under this Chapter. Where the requested Party is permitted to require

Still another problem arises when the conduct at issue is treated as a capital offense in the country seeking assistance, but the country from which assistance is sought does not employ the death penalty and refuses to provide assistance to an investigation that might result in someone's being put to death.[42]

B. What Are the Sources of Guidance?

The U.S. Department of State is an excellent resource: Its website (a) offers general information as to how one goes about obtaining evidence from abroad, including advice on preparing letters rogatory;[43] (b) lists the MLAT's and executive agreements currently in force;[44] and (c) provides specific information as to what is required in a series of different countries.[45]

> dual criminality as a condition to the providing of assistance (for example, where a requested Party has reserved its right to require dual criminality with respect to the preservation of data under Article 29, paragraph 4 'Expedited preservation of stored computer data'), dual criminality shall be deemed present if the conduct underlying the offence for which assistance is sought is also a criminal offence under the requested Party's laws, even if its laws place the offence within a different category of offence or use different terminology in denominating the offence. This provision was believed necessary in order to ensure that requested Parties do not adopt too rigid a test when applying dual criminality. Given differences in national legal systems, variations in terminology and categorization of criminal conduct are bound to arise. If the conduct constitutes a criminal violation under both systems, such technical differences should not impede assistance. Rather, in matters in which the dual criminality standard is applicable, it should be applied in a flexible manner that will facilitate the granting of assistance.

Council of Europe, *Report, supra* n. 1, at ¶ 259.

42. *See e.g.* Australian Parliament, *Law Enforcement, supra* n. 32, at 83:

> The challenges in harmonizing international law enforcement approaches are self-evidently considerable. A simple example relates to capital punishment. Australia does not support the death penalty. It generally refuses to provide mutual assistance to a requesting country in a criminal matter where the person might be subjected to the death penalty if found guilty, and will not extradite such persons. Given that some of our closest South East Asian neighbors impose capital punishment for drug-related offences and those countries are often the source of drugs trafficked into Australia, from whom Australia would wish cooperation in its law enforcement efforts, the issue highlights the potential for difficulties for the international community in readily coming to grips with problems on a global scale.

Id.

43. *See* U.S. Dept. of State, *Obtaining Evidence Abroad* <http://travel.state.gov /obtaining_evidence.html> (assessed Sept. 2002); U.S. Dept. of State, *Preparation of Letters Rogatory* <http://travel.state.gov/letters_rogatory.html> (assessed Sept. 2002).

44. *See* U.S. Dept. of State, *Mutual Legal Assistance in Criminal Matters Treaties (MLATs) and Other Agreements* <http://travel.state.gov/mlat.html> (assessed Sept. 2002).

45. *See id.* The site also lists (a) foreign embassies and consulates in the United States; and (b) U.S. embassies abroad. *See* U.S. Dept. of State, *Foreign Embassies and Consulates in the United States* <http://www.state.gov/www/global/legal_affairs/ca_notification/ca_part6.pdf> (assessed Sept. 2002); U.S. Dept. of State, *supra* n. 44.

The National Institute of Justice's International Center maintains a Web site that provides links to the police and/or justice agencies of a number of countries.[46] Interpol provides links to police-justice Web sites for most, if not all, of its 178 member countries.[47] It is also possible to find such information directly on the Internet.[48]

Interpol is both a source of information and assistance; it provides an international framework for police forces to exchange information, share intelligence and cooperate at an operational level.[49] Under its early warning system, Interpol maintains a list of Central Reference Points for participating police forces; officers can use a standard message form to seek assistance in investigating a cybercrime.[50] Interpol's con-

46. *See* National Institute of Justice International Center, *Global Links Government Departments / Components* <http://www.ojp.usdoj.gov/nij/international/gl_c.html> (assessed Sept. 2002).

47. *See* Interpol, *Police-Justice* <http://www.interpol.int/Public/Links/PolJust.asp> (last updated Aug. 1, 2002).

48. *See e.g.* Australian Transaction Reports and Analysis Centre, *Mutual Assistance and Electronic Crime* <http://www.austrac.gov.au/text/publications/agec/mutual_assistance.htm> (July 2001); Organization of American States, *Mutual Legal Assistance in Criminal Matters* <http://www.oas.org/juridico/MLA/en/> (assessed Sept. 2002); Swiss Federal Office of Justice, *International Mutual Legal Assistance-Fact Sheet* <http://www.ofj.admin.ch/themen/rechtshilfe/intro-e.htm> (assessed Sept. 2002).

49. *See e.g.* Interpol, *The Fundamental Principles of Interpol* <http://www.interpol.int/Public/icpo/Guide/principles.asp> (assessed Sept. 2002) (indicating that Interpol aims to "ensure and promote the widest possible mutual assistance between all criminal police authorities, within the limits of the laws existing in the different countries and in the spirit of the Universal Declaration of Human Rights"); *see also id.* (Principles of co-operation):

> International police co-operation within Interpol has always been conducted in accordance with the following guiding principles:
>
> RESPECT FOR NATIONAL SOVEREIGNTY
>
> Co-operation is based on actions taken by the police forces in the various Member States, operating within their own national boundaries and in accordance with their own national laws.
>
> ENFORCEMENT OF ORDINARY CRIMINAL LAW
>
> (Articles 2 and 3 of the Constitution)
>
> The Organization's field of activity is limited to crime prevention and law enforcement in connection with ordinary criminal offences. This is the only basis on which there can be agreement between all Member States.
>
> UNIVERSALITY
>
> Any Member State may co-operate with any other and co-operation must not be impeded by geographic or linguistic factors.

Id.

50. *See* Interpol, *Regional Working Parties* <http://www.interpol.int/public/TechnologyCrime/WorkingParties/Default.asp> (assessed Aug. 1, 2002). Early warning system consists of "an international 24-hour response system, National Central Reference Points (listing responsible experts within each of the 61 countries currently listed . . . and a formatted Computer Crime message format (to ensure that all the essential information is transmitted)." *Id.*

tact information appears on its Web site.[51]

The G8 has established a hi-tech points of reference initiative, which is intended to supplement existing lines of communication between police agencies. Under the initiative, the participating nations nominate "a point of reference to be the first point of contact when a foreign police force needs urgent assistance in a case that involves electronic evidence. The points of reference are staffed twenty four hours a day, seven days a week."[52] At this writing, sixteen countries, e.g., Australia, Brazil, Canada, Denmark, Finland, France, Germany, Italy, Japan, Luxembourg, Russia, South Korea, Spain, Sweden, the United Kingdom and the United States, were participants in the initiative.[53]

The U.S. Department of Justice's Office of International Affairs, which is part of the Criminal Division, "supports . . . state and local prosecutors regarding questions of foreign and international law, including issues relating to . . . mutual legal assistance treaties."[54] In addition, the Department of Justice's Computer Crime and Intellectual Property Section may be able to provide assistance.[55]

C. Efforts to Improve Cooperation

Several efforts are underway to improve the efficacy and efficiency of law enforcement cooperation in cybercrime investigations.[56] As Section I noted, the most notable achievement to date is the Council of Europe's Convention on Cybercrime, the product of many years of drafting and revising.[57] Parties to the Convention pledge to adopt whatever "legisla-

51. *See* Interpol, *Contact Interpol* <http://www.interpol.int/Public/contact.asp> (assessed Sept. 2002).

52. *See e.g.* Australian Transaction Reports, *supra* n. 50. As of May, 1999, 42 countries participated in the early warning system. *Id.*

53. *See e.g.* Council of Europe, *Council Recommendation of 25 June 2001 on Contact Points Maintaining a 24-Hour Service for Combating High-Tech Crime* <http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/c_187/c_18720010703en00050006.pdf> (assessed Sept. 2002); Council of Europe, *Organized Crime: Contact Points to Combat High-Tech Crime* <http://europa.eu.int/scadplus/leg/en/lvb/l33157.htm> (assessed Sept. 2002).

54. Dept. of Justice, *Office of International Affairs* <http://www.usdoj.gov/criminal/oiatxt.html> (assessed Oct. 2002).

55. *See* Dept. of Justice, *Computer Crime and Intellectual Property Section of the Criminal Division of the U.S. Department of Justice* <http://www.usdoj.gov/criminal/cybercrime/index.html> (assessed Sept. 2002).

56. *See e.g.* U of T G8 Information Centre, *Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime, Annex 1 Principles on Transborder Access to Stored Computer Data* <http://www.g7.utoronto.ca/g7/adhoc/crime99.htm#annex1> (assessed Sept. 2002); *see also* Section I of the accompanying text.

57. In 1997, the Council of Europe's European Committee on Crime Problems (CDPC) created a Committee of Experts on Crime in Cyber-Space (PC-CY). *See* Council of Europe, *583rd Meeting of the Ministers' Deputies* Appendix 13 <http://www.cm.coe.int/dec/1997/583/583.a13.html> (assessed Sept. 2002); *see also* Ulrich Sieber, *Legal Aspects of Computer-*

tive or other measures" are needed to ensure the preservation and collection of evidence and the providing of mutual assistance in cybercrime investigations even when no MLAT is in force between the requesting country and the requested nation.[58] In particular, they agree to "afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence."[59] In an effort to expedite mutual assistance as much as possible, the Convention provides that parties

> may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communications, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.[60]

Related Crime in the Information Society, 183 <http://europa.eu.int/ISPO/legal/en/comcrime/sieber.doc> (Sept. 2002). The Committee of Experts on Crime in Cyberspace was assigned to examine the problems "of criminal law connected with information technology" including, *inter alia*, "cyberspace offenses and other substantive criminal law issues where a common approach may be necessary for the purposes of international co-operation." *Id.; see* Council of Europe, *583rd Meeting of the Ministers' Deputies,* Appendix 13, *supra.* The new Committee was also given the task of drafting "a binding legal instrument" dealing with these issues. *Id.* at § 4(c). This initiated the process that ultimately led to the Convention on Cybercrime. *See* Council of Europe, *Report, supra* n. 1. (describing efforts from 1996 to 2001 that resulted in the final version of the Convention on Cybercrime).

58. *See* Council of Europe, *Convention, supra* n. 29, Article 16-34; *see also* Section I of the accompanying text.

59. *Id.* at Article 25 ¶ 1.

60. *Id.* at Article 25 ¶ 3. The Explanatory Report accompanying the Convention elaborates on the need for such a provision:

> Computer data is highly volatile. By a few keystrokes or by operation of automatic programs, it may be deleted, rendering it impossible to trace a crime to its perpetrator or destroying critical proof of guilt. Some forms of computer data are stored for only short periods of time before being deleted. In other cases, significant harm to persons or property may take place if evidence is not gathered rapidly. In such urgent cases, not only the request, but the response as well should be made in an expedited manner. The objective of Paragraph 3 is therefore to facilitate acceleration of the process of obtaining mutual assistance so that critical information or evidence is not lost because it has been deleted before a request for assistance could be prepared, transmitted and responded to. Paragraph 3 does so by (1) empowering the Parties to make urgent requests for co-operation through expedited means of communications, rather than through traditional, much slower transmission of written, sealed documents through diplomatic pouches or mail delivery systems; and (2) requiring the requested Party to use expedited means to respond to requests in such circumstances. Each Party is required to have the ability to apply this measure if its mutual assistance treaties, laws or arrangement do not already so provide. The listing of fax and e-mail is indicative in nature; any other expedited means of communication may be used as would be appropriate in the particular circumstances at hand. As technology advances, further expedited means of

The Council of Europe is not the only transnational group working on cybercrime. From 1983 to 1985, the Organization for Economic Cooperation and Development conducted a study of the need for consistent national cybercrime laws.[61] The study produced a 1986 report listing a core group of cybercrimes countries should outlaw.[62] In 1992, the OECD adopted a recommendation concerning the security of information systems; *Guidelines for the Security of Information Systems* were appended to the recommendation.[63] Among other things, the *Guidelines* suggested that member states develop procedures to facilitate mutual legal assistance in dealing with cybercrimes.[64] In 1997, the OECD initiated a review of the progress that had been made toward implementing the 1992 *Guidelines*.[65] The review revealed that countries had experienced difficulties in developing laws and procedures relating to information security because of "differences in the various legal systems and how they deal with security matters . . . such as . . . computer crimes."[66] The general consensus was that the *Guidelines* were still adequate and did not need to be revised.[67] However, the OECD issued a new version of the *Guide-*

---

communicating will be developed that may be used to request mutual assistance. With respect to the authenticity and security requirement contained in the paragraph, the Parties may decide among themselves how to ensure the authenticity of the communications and whether there is a need for special security protections (including encryption) that may be necessary in a particularly sensitive case. Finally, the paragraph also permits the requested Party to require a formal confirmation sent through traditional channels to follow the expedited transmission, if it so chooses.

Council of Europe, *Report, supra* n. 1, at ¶ 256.

61. *See* International Review of Criminal Policy, *United Nations Manual on the Prevention and Control of Computer-Related Crime* §II(C)(2), at ¶ 117 <http://www.uncjin.org/Documents/EighthCongress.html> (1995).

62. *See id.*

63. *See* Organization for Economic Cooperation and Development, *Recommendation of the Council Concerning Guidelines For the Security of Information Systems* <http://www.oecd.org/EN/document/0,,EN-document-40-1-no-24-10249-0,00.html> (1992).

64. *See id.*

65. *See* Organization for Economic Cooperation and Development, Directorate For Science, Technology and Industry – Committee for Information, Computer And Communications Policy, *Review of the 1992 Guidelines For the Security of Information Systems* <http://www.meti.go.jp/policy/netsecurity/chairmans%20closing%20statement.htm> (2002); *see also* Organization for Economic Cooperation and Development, *Recommendation of the Council Concerning Guidelines For the Security of Information Systems* <http://www.oecd.org/EN/document/0,,EN-document-40-1-no-24-102490,00.html> (1992). The Recommendation suggested that the Guidelines be reviewed every five years "with a view to improving international co-operation on issues relating to the security of information systems." *See* Organization for Economic Cooperation and Development, Directorate For Science, Technology and Industry – Committee for Information, Computer And Communications Policy, *Review of the 1992 Guidelines For the Security of Information Systems* 5 <http://www.oecd.org/dsti/sti/it/secur/index.htm> (1997).

66. *Id.* at 9.

67. *See id.* at 19.

lines in 2002; the new version was prompted by the changes in technology that had taken place since the original guidelines were issued in 1992.[68]

The United Nations has been working toward resolving the problems raised by cybercrime for more than a decade. In 1990, the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders issued a series of recommendations concerning the adoption of anti-cybercrime legislation, investigative procedures, rules of evidence, forfeiture and mutual legal assistance in cybercrime investigations. In 1995 the United Nations published the *United Nations Manual on the Prevention and Control of Computer-Related Crime*.[69] The *Manual* examines the law governing cybercrime and the need for international cooperation in cybercrime investigations.[70] These efforts were followed up in a workshop on cybercrimes that was held at the Tenth United Nations Congress; it yielded recommendations calling for greater cooperation between governments and the private sector, along with improving cooperation among nations in tracing offenders. Finally, in December of 2000 the United Nations General Assembly adopted Resolution 55/59, the "Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-First Century," that committed member nations to work towards enhancing their ability to prevent, investigate and prosecute computer-related crime.[71] The resolution pointed out the need to eliminate safe havens for offenders, increase the effectiveness of cooperation among law enforcement agencies, and improve the training and equipping of law enforcement agencies while keeping in mind the need to protect individual freedom and privacy.[72]

Interpol held its First International Conference on Computer Crime

68. *See* Organization for Economic Cooperation and Development, *OECD Guidelines for the Security of Information Networks and Systems: Toward a Culture of Security* <http://www.oecd.org/pdf/M00034000/M00034292.pdf> (2002).

69. *See* International Review of Criminal Policy, *United Nations Manual on the Prevention and Control of Computer-Related Crime* <http://www.uncjin.org/Documents/Eighth Congress.html> (1995).

70. *See id.*

71. *See* United Nations General Assembly, *55/59 Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first Century* <http://www.un.org/documents/ga/res/55/a55r059.pdf> (Jan. 17, 2001). "We decide to develop action-oriented policy recommendations on the prevention and control of computer-related crime, and we invite the Commission on Crime Prevention and Criminal Justice to undertake work in this regard, taking into account the ongoing work in other forums. We also commit ourselves to working towards enhancing our ability to prevent, investigate and prosecute high-technology and computer-related crime." *Id.*

72. *See id.* at ¶¶ 2-7; *see also* United Nations General Assembly, *55/64* <http://www.un.org/documents/ga/res/55/a55r064.pdf> (Jan. 26, 2001); United Nations General Assembly, *56/123* <http://www.undcp.org/adhoc/crime/a_res_56/123e.pdf> (Jan. 23, 2002).

in 1995.[73] Those who attended expressed a great deal of concern over the spread of computer crime and the lack of any global procedures to facilitate effective, efficient responses to such crime.[74] Interpol held subsequent Conferences on Computer Crime in 1996, 1998 and 2000.[75] Its approach to cybercrime has been to harness the expertise of its members "through the vehicle of a 'working party' or a group of experts. . .these working parties have been designed to reflect regional expertise and exist in Europe, Asia, the Americas and in Africa."[76] The first Interpol working party—the European Working Party on Information Technology Crime—was created in 1990;[77] three others were created later.[78] Interpol has also established a Steering Committee for Information Technology Crime, which coordinates and harmonizes the initiatives of the various working parties.[79]

In May of 2000, the G8 held a conference on cybercrime that produced an agenda for a summit to be held in July.[80] At the July, 2000 summit, the G8 issued a communiqué declaring that it would "take a concerted approach to . . . cyber-crime."[81] The approach was set out in

---

73. *See e.g.* Sieber, *supra* n. 57, at 188-89. In 1981, Interpol held its First Interpol Training Seminar for Investigators of Computer Crime. *See e.g.* Stein Schjolberg, *The Legal Framework – Unauthorized Access to Computer Systems* § I <http://www.mossbyrett.of.no/info/legal.html> (assessed Sept. 2002).

74. *See* Interpol, *Regional Working Parties* <http://www.interpol.int/Public/TechnologyCrime/WorkingParties/Default.asp#europa> (assessed Sept. 2002):

> The Steering Committee (SC) was formed to co-ordinate and harmonize the various regional working party initiatives. It is represented by the Chairperson, Vice-Chairperson and a third member from each regional WP and is co-ordinated by the representative from the General Secretariat. The idea was to streamline the individual efforts of the member countries by avoiding unnecessary duplication and the resultant waste of human and financial resources. The SC has now gone a step further by contacting organizations outside of Interpol and involving them in our initiatives. . .to date we have thus achieved success most notably with the High Tech Crime Sub-group of the G8, the International Chamber of Commerce, UNAFEI (the United Nations Asia Institute for the Prevention of Crime and the Treatment of Offenders), as well as with several academic institutions.

Id.

75. *See e.g.* Schjolberg, *supra* n. 73.

76. Interpol, *Interpol's Contribution to Combating Information Technology Crime* <http://www.interpol.int/Public/TechnologyCrime/default.asp> (assessed Sept. 2002).

77. Interpol, *European Working Party on Information Technology Crime* <http://www.interpol.int/Public/TechnologyCrime/default.asp> (assessed Sept 2002).

78. *See* Interpol, *supra* n. 74.

79. *Id.*

80. Adlaw, *Group of Eight Meets to Discuss International Cooperation on Cybercrime* <http://adlawbyrequest.com/international/G8Cybercrime.shtml> (May 22, 2000); Wired News, *G8 Hems and Haws on Cybercrime* <http://www.wired.com/news/politics/0,1283,36398,00.html> (May 17, 2000).

81. G8 Information Centre, *G8 Communique Okinawa 2000* ¶ 44 <http://www.g7.utoronto.ca/g7/summit/2000okinawa/finalcom.htm> (July 23, 2000).

paragraph eight of an accompanying document, the Okinawa Charter on Global Information Society:

> International efforts to develop a global information society must be accompanied by coordinated action to foster a crime-free and secure cyberspace. We must ensure that effective measures, as set out in the OECD Guidelines for Security of Information Systems, are put in place to fight cyber-crime. G8 co-operation within the framework of the Lyon Group on Transnational Organised Crime will be enhanced. . . . [82]

The G8 established a "Digital Opportunity Taskforce" to explore how to integrate the efforts of the G8 members into "a broader international approach."[83] After meeting in 2000 and 2001, the Taskforce submitted a report containing a Proposed Plan of Action that did not address cybercrime.[84] However, at the G8 Justice and Interior Ministers' Meeting in May of 2002, the ministers directly focused on cybercrime, "reaffirming" their "commitment expressed in previous meetings to combat high-tech crime."[85] The ministers also (a) emphasized law enforcement's need for traffic data in cybercrime investigations; (b) confirmed the value of the 24/7 network created by the G8 and expressed the intention to continue to expand and strengthen it; and (c) expressed approval for the Council of Europe's Convention on Cybercrime and the progress it represented toward achieving consistent national efforts in this area.[86]

The Council for Security Cooperation in the Asia Pacific ("CSCAP") was established in 1993 to provide a "regularised, focused and inclusive non-governmental process on Asia Pacific security matters."[87] It established a Working Group on Transnational Crime in 1997.[88] Designed to "address the increasing importance of transnational crime as a threat to regional security," the Working Group focuses on cybercrime and on the need for law enforcement cooperation in the region.[89]

All of these efforts are being taken at the international level in an attempt to improve the effectiveness of local law enforcement's efforts against transnational cybercrime. The next section examines the diffi-

---

82. G8 Information Centre, *Okinawa Charter on Global Information Society* ¶ 8 <http://www.g7.utoronto.ca/g7/summit/2000okinawa/gis.htm> (July 22, 2000).

83. *Id.* at ¶ 16.

84. *See* The Ministry of Foreign Affairs of Japan, *The Current State and Perspective of the Digital Opportunity Taskforce* <http://www.mofa.go.jp/policy/economy/it/df0106.html> (June 1, 2001).

85. G8 Information Centre, *G8 Justice and Interior Ministries' Meeting* ¶ 5 <http://www.g8.utoronto.ca/g7/adhoc/justice2002chair.htm> (May 13-14, 2002).

86. *Id.* at ¶¶ 6,7,9.

87. Council for Security Cooperation in the Asia Pacific, *About CSCAP* <http://www.cscap.org/about.htm> (assessed Sept. 2002).

88. *See* Council for Security Cooperation in the Asia Pacific, *Transnational Crime* <http://www.cscap.org/crime.htm> (assessed Sept. 2002).

89. *See id.*

culties that still plague the local prosecutor who has to deal with this new phenomenon.

III. INTERNATIONAL CYBERCRIME AND LOCAL PROSECUTION

A. INTRODUCTION

Not so long ago, one would never associate the phrase "transnational cybercrime" with "district attorney" or "local prosecutor." However, times have changed. The world of Mayberry is long gone and transnational cybercrime cases have become almost commonplace;[90] as the world becomes more technologically advanced, there is a corresponding increase in crimes involving computers.[91] Computer intrusion cases originating from overseas perpetrators are increasing;[92] simultaneously,

90. *See e.g.* Richard H. Ward, *The Internationalization of Criminal Justice,* Criminal Justice 2000 Vol. II, 281 <http://www.ojp.usdoj.gov/nij/international/internat.pdf> (assessed Sept. 2002). "Cybercrime has virtually eliminated borders. Today it is possible to plan a crime in one country, carry it out in another, and move funds to one or more other countries, all from a personal computer." *Id.*

91. *See e.g.* National Institute of Justice, *Annual Report to Congress: 2000* 12 <http://www.ncjrs.org/pdffiles1/nij/189105.pdf> (assessed Sept. 2002). "By one estimate, cybercrime increased fivefold in a recent 3-year period. The monetary toll is staggering. According to the FBI, cybercrime costs about $10 billion a year." *Id.* Private surveys of cybercrime consistently show that by far the largest percentage of computer crime comes from outside, via the Internet. *2002 CSI/FBI Computer Crime and Security Survey* <http://www.gosci.com/press/20020407.html> (assessed Sept. 2002). They reported that of the 503 computer security professionals responding, 90% had detected computer attacks in the last year and 74% cited the Internet as the most common source of attacks. The *2002 Australian Computer Crime and Security Survey* conducted by Deloitte Touche Tohmatsu and AusCERT and based on responses from "a wide cross section of Australian organizations" found that 67% of those responding had suffered attacks in the last year and 35% had experienced six or more attacks. As in the CSI survey, most attacks (89%) came from the Internet. AusCert, *2002 Australian Computer Crime and Security Survey* <http://www.auscert.org> (assessed Sept. 2002). In a survey released in August, 2001, the Confederation of British Industry (CBI) reported that two-thirds of the 148 companies responding suffered "a serious cybercrime attack" within the last year. *See* CBI, *Business Leaders Warn of Cybercrime Threat to Internet Development* <http://www.cbi.org.uk/80256716004baae5/33a87f2eee41b54e80256803004f04e4/eff1596523e1653f80256aaf00338dac?OpenDocument> (assessed Sept. 2002). A 2002 Price Waterhouse Coopers survey of British businesses found that 44% had suffered at least one attack in the past year and that 65% of the attacks came from the Internet. *See* Price Waterhouse Coopers, *Information Breaches Security Survey 2002* <http://www.pwcglobal.com/Extweb/ncsurvres.nsf/0cc1191c627d157d8525650600609c03/845a49566045759e80256b9d003a4773/$FILE/ATT7PG80/DTI%20Security%20Survey%202002.pdf> (assessed Sept. 2002).

92. *See e.g.* Louis Freeh, Congressional Statement Federal Bureau of Investigation, *Statement for the Record of Louis J. Freeh, Director Federal Bureau of Investigation on Cybercrime* (Washington, D.C. Feb. 16, 2000) <http://www.fbi.gov/congress/congress00/cyber021600.htm> (assessed Feb. 3, 2003):

> In 1996 and 1997, the National Oceanic and Atmospheric Administration . . .suffered a series of computer intrusions. . . . [I]t was determined that the

the federal government resources available to prosecute computer crime have been stretched very thin.[93] Even the Federal Bureau of Investigation believes the international protocols relating to cybercrime investiga-

---

subject resided in Canada. In April 1999, Jason G. Mewhiney was indicted by Canadian authorities. In January 2000, he pled guilty to 12 counts of computer intrusions. . . . Peter Iliev Pentchev, a Princeton University student, was identified as an intruder on an e-commerce system. An estimated 1800 credit card numbers, customer names, and user passwords were stolen. The company had to shut down its web servers for five days to repair the damages estimated at $100,000. Pentchev has fled to his native Bulgaria. . . .

In 1994-95, an organized crime group headquartered in St. Petersburg, Russia, transferred $10.4 million from Citibank into accounts all over the world. After investigation by the FBI's New York field office, all but $400,000 of the funds were recovered. Cooperation with Russian authorities helped bring Vladimir Levin, the perpetrator, to justice. In another case, the FBI investigated Julio Cesar Ardita, an Argentine computer science student who gained unauthorized access to Navy and NASA computer systems. He committed these intrusions from Argentina. . . .

Id.; see also Mike Brunker, *E-Business vs. The Perfect Cybercrime* (March 3, 2002) <http://www.msnbc.com/news/376973.asp> (assessed Sept. 2002):

The Internet has revolutionized commerce by allowing businesses to sell globally, but it also has created what so far appears to be the perfect cybercrime — borderless credit card fraud. An investigation by MSNBC has learned that . . . criminals based overseas now account for up to a third of all online fraud directed at U.S. e-businesses. . . .

It has been known for sometime that organized crime groups and overseas freelancers were responsible for some of the credit card fraud aimed at Internet merchants in the United States. But after more than a dozen interviews with industry insiders and e-business owners, it is clear that a much larger percentage of the fraud than previously known originates overseas.

Id.; see generally Yang Sung-jin, *Hackers Exploit Korea to Attack Global Systems,* <http://www.koreaherald.co.kr/SITE/data/html_dir/2002/04/26/200204260031.asp> (Apr. 26, 2002) (stating that hackers "are increasingly using South Korea as an entry point to attack computer systems in other countries" because while the country's broadband capacity has dramatically increased, security remains low).

93. *See e.g.* Louis J. Freeh, Congressional Statement Federal Bureau of Investigation, *Statement for the Record of Louis J. Freeh, Director Federal Bureau of Investigation on Cybercrime* (Washington, D.C., Feb. 16, 2000) <http://www.fbi.gov/congress/congress00/cyber021600.htm> (assessed Feb. 3, 2003):

Our current resources are stretched paper thin. We only have 193 agents assigned . . . nationwide. Major cases . . . draw a tremendous amount of personnel resources. Most of our technical analysts will have to be pulled from other work to examine the log files received from the victim companies. Tracking down hundreds of leads will absorb the energy of a dozen field offices. . . .

The technical challenges of fighting crime in this arena are equally vast. We can start just by looking at the size of the Internet and its exponential growth. Today it is estimated that more than 60,000 individual networks with 40 million users are connected to the Internet. Thousands of more sites and people are coming on line every month. In addition, the power of personal computers is vastly increasing. The FBI's Computer Analysis Response Team (CART) examiners conducted 1,260 forensic examinations in 1998 and 1,900 in 1999. With the anticipated increase in high technology crime and the growth of private sector technologies, the FBI expects 50 percent of its caseload to require at least one computer forensic examination. By 2001, the FBI anticipates the number of required CART examinations to rise to 6,000. . . .

Id.

tions are "inadequate."[94] The end result is that local prosecutors must deal with transborder issues now and into the future.[95] Are they prepared? Definitely not.

The sheer amount of criminal prosecution that takes place at the local level means local prosecutors must become adept at dealing with transnational issues. It is axiomatic that the majority of all law enforcement in the United States takes place at the state and local level.[96] There are 2,341 local/appointed chief prosecutors in the fifty states; each heads a separate prosecuting agency, which usually has jurisdiction over one or more counties.[97] These chief prosecutors, and the agencies they

---

94. *See* Reuters, *FBI Overwhelmed by Cybercrime* <http://zdnet.com.com/2100-1105-864453.html> (Mar. 20, 2002):

> Technology permits cyber crimes to occur at the speed of light and law enforcement must become more sophisticated in uncovering them,' FBI assistant director Ronald Eldon told a conference on fighting organized crime in Hong Kong.
> Eldon said international protocols and procedures relating to cybercrime investigations was [*sic*] inadequate. . . .
> 'Legal procedure varies from jurisdiction to jurisdiction and the availability of resources and equipment to deal with encryption is another issue,' he said.
> Mark Pollitt, chief of the FBI computer analysis response team, told Reuters . . the volume of digital evidence which the FBI has to ferret through has ballooned.
> 'In the past two years, we have looked at ten times more digital evidence,' he said.
> As information crosses borders with the increased use of handheld devices and Web-enabled mobile phones, enforcement agencies and governments need to find quicker ways of working with each other to take care of legal requirements and diplomacy.

Id.

95. *See e.g.* National Institute of Justice, *Electronic Crime Needs Assessment for State and Local Law Enforcement* IX <http://www.ncjrs.org/pdffiles1/nij/186276.pdf> (2001):

> Not long ago, the incidence of crimes that involved computers or electronic media was negligible. Currently, State and local law enforcement agencies routinely encounter evidence of electronic crimes, including online fraud, child pornography, embezzlement, economic espionage, and cyberstalking. Law enforcement also encounters crimes classified as cyberterrorism. These incidents have included attempts to penetrate electronic systems that control critical infrastructures. The task of investigating and prosecuting electronic crimes and cyberterrorism is complicated by the anonymity afforded perpetrators through the Internet, by a 'borderless' environment, and by the variables in State and foreign laws.

Id.

96. *See e.g.* American Bar Association, *The Federalization of Criminal Law* Preface 4 <http://www.abanet.org/crimjust/fedreport.html> (1998). "[F]ederal efforts account for only five percent of all prosecutions nationwide. State law enforcement is still the critical component in dealing with the crime which threatens most people." *Id.* Simple statistics demonstrate this: There is one federal system, but there are fifty state systems, each of which encompasses hundreds of municipal and other local systems; there are 2,341 local elected/appointed prosecutors. *See* Carol J. DeFrances, *Prosecutors in State Courts 2001,* Bureau of Justice Statistics Bulletin 1 <http://www.ojp.usdoj.gov/bjs/pub/pdf/psc01.pdf> (May 2002). Indeed, the original "constitutional vision" was that "the federal government should play a narrowly circumscribed role in defining and investigating criminal conduct." American Bar Assoc., *supra.* n. 96.

97. *See* Carol J. DeFrances, *Prosecutors in State Courts 2001,* Bureau of Justice Statistics Bulletin 1, 2 <http://www.ojp.usdoj.gov/bjs/pub/pdf/psc01.pdf> (May 2002). The agen-

head, are responsible for all local prosecution, from petty retail thefts to homicides. In 2000, local prosecutors closed "[o]ver 2.3 million felony cases and almost 7 million misdemeanor cases."[98] A study of prosecution at the local level found that 42% of the 2,341 local prosecutorial agencies had prosecuted computer-related crimes under their state law in 2001.[99] "Three in ten offices nationwide reported prosecuting computer related crimes dealing with the transmittal of child pornography. A quarter of all offices prosecuted credit card fraud (27%) and bankcard fraud (22%). Computer sabotage was prosecuted by 5% of the offices and theft of intellectual property by 3%."[100]

B. The Evolving World (How did this happen?)

Over the last decade, the Internet has become an integral part of everyday life for many people in the United States and elsewhere. According to one estimate, there are currently 533 million Internet users around the globe, a number that will rise to 945 million by 2004.[101] Not so long ago, local prosecutors were much more likely to encounter harassing communications in handwritten, letterform than as e-mail.[102] But this is changing; many of the crimes local prosecutors now deal with are completely electronic.[103] And while someone must physically enter a local business in order to steal a filing cabinet, a hacker in another coun-

---

cies employ "over 79,000 attorneys, investigators, victim advocates, and support staff." *Id.* at 1. This study found that between 1992 and 2001 the total number of staff in these prosecutors' offices increased by 39%, and that the number of assistant prosecutors increased by 26% during the same period. *See id.* at 4.

98. *Id.*

99. *Id.* at 5.

100. *Id.*:

> Data on prosecution of any computer related crime under their State's computer statutes were available for 2,151 prosecutors' offices. Data were available on credit card fraud for 1,995 prosecutors' offices, bank card fraud 1,956 offices, forgery 1,894 offices, sabotage 1,853 offices, unauthorized access to computer system 1,878 offices, unauthorized copying or distribution of computer programs 1,883 offices, cyberstalking 1,927 offices, theft of intellectual property 1,839 offices, transmitting child pornography 2,029 offices, and identity theft 1,927 offices.

Id. For a detailed breakdown of the cases by category. *Id.*

101. *See* CyberAtlas, *The World's Online Populations* <http://cyberatlas.internet.com/big_picture/geographics/article/0,,5911_151151,00.html> (assessed Sept. 2002). According to another source, eMarketer, there are currently 445.9 million people online globally, and the number will increase to 709.1 million by 2004. *See id.* For a country-by-country breakdown. *Id.*

102. Indeed, combating cybercrime became a top-ten priority for the Federal Bureau of Investigation until the middle of 2002. *See e.g. Robert S. Muller,* Congressional Statement Federal Bureau of Investigation, *Statement for the Record of Robert S. Muller, III Director Federal Bureau of Investigation* (Washington, D.C., June 6, 2000) <http://www.fbi.gov/congress/congress02/mueller060602.htm> (assessed Feb. 3, 2003).

103. *See supra* nn 99 - 100 and the accompanying text.

try can "break in" to a computer system and spirit away data without ever leaving his or her desk.[104]

Certainly, efforts have been made at the federal level to address the issues raised by the proliferation of this evolving technology. The *2001 USA Patriot Act*, for example, gave law enforcement increased powers to investigate cybercrime;[105] it also required the creation of a national network of cybercrime task forces which will combine state and federal resources.[106] And the Federal Bureau of Investigation announced it would create a "Cyber Division" as part of the reorganization it undertook in 2002.[107] State and local prosecutors, however are just beginning to ad-

---

104. *See e.g.* National Institute of Justice, *Electronic Crime Needs Assessment for State and Local Law Enforcement* 13 <http://www.ncjrs.org/pdffiles1/nij/186276.pdf> (2001):

> A hypothetical example to illustrate this point is a telecommunications system that is attacked in Florida. A hacker or cyberterrorist breaks into and steals a student's account at the University of California and uses that account to conduct the hack into the telecommunications system in Florida. The hacker, however, is located in Sweden. Although the telecommunications system is the intended victim, the student's computer in California was exploited and used as a launch pad to mask the intrusion in Florida, making it harder for authorities to trace where the attack originated.

Id.; *see also* Louis J. Freeh, Congressional Statement Federal Bureau of Investigation, *Statement Of Louis J. Freeh, Director, Federal Bureau Of Investigation Before The Committee On International Relations House Of Representatives, The Threat From International Organized Crime And Global Terrorism* (Washington, D.C., Oct. 1, 1997) <http://commdocs.house.gov/committees/intlrel/hfa44990.000/hfa44990_0.HTM> (assessed Feb. 3, 2003):

> One recent case was a case we worked with the Russians where an individual sitting in St. Petersburg using a laptop computer broke into a Citibank account in New York and moved about $10 million. The bank ultimately suffered a loss of approximately $400,000. The individual never left his apartment during the course of that crime.

Id.

105. *See* 107 H.R. 3162, *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism* (2000); *see also* Dept. of Justice, Computer Crime and Intellectual Property Section, *Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001* <http://www.cybercrime.gov/PatriotAct.htm> (assessed Sept. 2002).

106. *See e.g.* 107 H.R. 3162, *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism* (stating that "[t]he Director of the United States Secret Service shall take appropriate actions to develop a national network of electronic crime task forces, based on the New York Electronic Crimes Task Force model, throughout the United States, for the purpose of preventing, detecting, and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems"). The New York Electronic Crimes Task Force combines federal, state and local law enforcement with representatives from industry and academic to combat cybercrime. *See e.g.* Brian L. Stafford, *Secret Service's Little-Known Role: Protecting Citizens as Well as Leaders* <http://www.ectaskforce.org/About_Us.htm> (July 23, 2001).

107. *See e.g.* Robert S. Muller, *supra* n. 102:

> Last December, the Administration and Congress approved the establishment of a Cyber Division at FBI Headquarters. The Cyber Division will coordinate, oversee, and facilitate FBI investigations in which the Internet, on-line services, and com-

dress cybercrime issues, and the challenges they raise.[108] Virtually none of the nation's state and local prosecutors are familiar with the challenges involved in prosecuting a case that requires the collection of evidence from abroad.

Local prosecutors are the last resort with regard to all crimes, including those involving computers. Those familiar with the criminal justice system in the United States realize that local prosecutors necessarily assume responsibility for prosecuting cybercrimes that are not damaging[109] or otherwise important enough to be picked up at the state[110] or federal level.[111] For example, assume a hacker breaks into a

---

puter systems and networks are the principal instruments or targets of foreign intelligence or terrorists and for criminal violations where the use of such systems is essential to the illegal activity. The FBI will consolidate under a single national program manager headquarters and field resources associated with the National Infrastructure Protection Center (NIPC), the Internet Fraud Complaint Center, and cyber-related criminal investigations delegated to the FBI for investigation, such as intellectual property rights-related investigations involving theft of trade secrets and signals; copyright infringement investigations involving computer software; and Innocent Images National Initiative investigations and training. . . . . .In large FBI Field Offices, I envision the FBI maintaining existing stand-alone . . . squads to handle computer intrusions, critical infrastructure protection issues, and the INFRAGARD program. Complementary Cyber Crime Squads will be established to consolidate management and investigation of cyber-related violations currently handled under the White-Collar and Violent Crime programs, as well as investigate non-terrorist and non-intelligence computer hacking and intrusion cases. In small or medium FBI Field Offices, the FBI will either use the above model or create hybrid cyber squads that consolidate NIPC and criminal resources into a single squad. . . .

Id.

108. A study released in 2001 found that local prosecutors identified a number of issues that impeded their prosecution of cybercrimes, including insufficient evidence, insufficient prosecutor knowledge and experience, the fact that cybercrime is not a priority, a lack of judicial interest in cybercrime cases, a lack of responding officer training in dealing with cybercrime cases and a lack of cooperation in extradition requests. *See* National Institute of Justice, *supra* n. 104, at 13.

109. For example, the basic federal cybercrime statute, 18 U.S.C.S. § 1030, requires that the government must prove loss exceeding $5,000 to establish the elements of a violation. *See* 18 USCS § 1030(a)(4); *see also* Dept. of Justice, Computer Crime and Intellectual Property Section, *Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001* <http://www.cybercrime.gov/PatriotAct.htm> (assessed Sept. 2002) (discussing § 814 of the Act).

110. Attorney General's offices in a number of states have established cybercrime units. *See e.g.* Arizona Attorney General, *Cybercrime* <http://www.attorneygeneral.state.az.us/cybercrime/index.html> (assessed Sept. 2002). The Office of Massachusetts Attorney General Tom Reilly, *Technological Advancements* <http://www.ago.state.ma.us/hightech/index.asp?head1=High%20Tech&section=14> (assessed Sept. 2002). These offices may not, however, have jurisdiction to prosecute all computer crimes.

111. This is illustrated by a May, 2001 denial of service attack perpetrated by a 13-year-old Wisconsin boy ("Wicked") against a California computer security company. *See* Steve Gibson, *The Strange Tale of the Denial of Service Attacks Against GRC.COM* 12 <http://grc.com/dos/grcdos.htm> (Mar. 5, 2002). Having traced the perpetrator, Steve Gibson,

computer owned by a private individual. The hacker causes some damage, perhaps even makes the computer completely unusable; let us assume it will take several hundred dollars to restore the computer to its working state. This intrusion will not be prosecuted federally because it does not meet the criteria that must be satisfied for the initiation of a federal prosecution.[112] This means that thousands of "small" cyber-

---

CEO of the victim company, went to two different FBI agents in hopes of having "Wicked" prosecuted. Both said the same thing:

> They explained that until $5,000 of damage had been done, no crime had even been committed. That's the law. And due to the peculiar nature of GRC.COM's business model . . . these attacks were stirring up interest in my forthcoming research and it wasn't even clear that we were going to be economically damaged in any way.
>
> Secondly, they said . . . their staffs were overloaded and swamped with cases involving companies that had lost huge sums of money to Internet crime. Furthermore, since the cost of an FBI prosecution was in the neighborhood of $200,000, they needed to prioritize their cases based upon prosecuting criminals who were responsible for causing large dollar losses. 'Wicked's' attacks, no matter how annoying, failed to qualify.
>
> And finally, they said that since 'Wicked' was only 13 years old, nothing much would happen to him, even if the preponderance of evidence demonstrated that he was behind these attacks. They said that a couple of agents might go out to his home and have a talk with his parents, but in this country his youth was an impenetrable shield. This, of course, further discouraged the costs which would be incurred through any investigation.

Id.; *see also* National Institute of Justice, *supra* n. 104, at 25:

> For example, Missouri could have 20 victims who complain to their State attorney general about a 'failure to render' Internet scam that took their money, $250 each for a complete personal computer system, a total loss of $5,000. The Web site they ordered from and sent money to is located in Florida. But the FBI in St. Louis does not want to pursue fraud cases unless they meet the prosecution guidelines threshold of $25,000.

Id.

112. *Id.*; *see also U.S. Attorney's Manual*, Principles of Federal Prosecution §§ 9-27.220 & 9-27.230 <http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/27mcrm.htm#9-27.220> (assessed Sept. 2002). An inquiry conducted by *Criminal Justice Weekly* found that while federal referrals for "prosecutions of computer crime have increased substantially over the past several years, . . . actual prosecutions are fairly rare." David Banisar, *Computer Hacker's Sentence Spotlights High-Tech Crime Prosecutions,* Criminal Justice Weekly <http://www.epic.org/epic/staff/banisar/hacker.html> (Aug. 3, 1999). Based on information obtained under the *Freedom of Information Act*, the article reported that although referrals had more than tripled during the period between 1992 and 1998, "the DOJ has declined to prosecute between 64 and 78 percent of these cases." *Id.* The *U.S. Attorney's Manual* advises prosecutors that they should recommend federal prosecution if they believe "that the person's conduct constitutes a Federal offense and that the admissible evidence will probably be sufficient to obtain and sustain a conviction" unless the prosecutor believes prosecution should be declined because (a) no substantial federal interest would be served by prosecution; (b) the person is subject to effective prosecution in another jurisdiction; and/or (c) there exists an adequate non-criminal alternative to prosecution. *U.S. Attorney's Manual*, Principles of Federal Prosecution § 9-27.220(A) <http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/27mcrm.htm#9-27.220> (assessed Sept. 2002). In determining whether prosecution should be declined because no substantial Fed-

eral interest would be served by prosecution, the *U.S. Attorney's Manual* advises federal prosecutors to weigh all relevant considerations, including the following: federal law enforcement priorities; the nature and seriousness of the offense; the deterrent effect of prosecution; the person's culpability in connection with the offense; the person's history with respect to criminal activity; the person's willingness to cooperate in the investigation and prosecution of others and the probable sentence or other consequences if the person is convicted. *U.S. Attorney's Manual*, Principles of Federal Prosecution § 9-27.230(A) <http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/27mcrm.htm#9-27.230> (assessed Sept. 2002). As to the nature and seriousness of the offense, the *U.S. Attorney's Manual* explains:

> That federal resources should not be wasted in prosecuting inconsequential cases or cases in which the violation is only technical. Thus, in determining whether a substantial Federal interest exists that requires prosecution, the attorney for the government should consider the nature and seriousness of the offense involved. A number of factors may be relevant. One factor that is obviously of primary importance is the actual or potential impact of the offense on the community and on the victim.
>
> The impact of an offense on the community in which it is committed can be measured in several ways: in terms of economic harm done to community interests; in terms of physical danger to the citizens or damage to public property; and in terms of erosion of the inhabitants' peace of mind and sense of security. In assessing the seriousness of the offense in these terms, the prosecutor may properly weigh such questions as whether the violation is technical or relatively inconsequential in nature and what the public attitude is toward prosecution under the circumstances of the case. The public may be indifferent, or even opposed, to enforcement of the controlling statute whether on substantive grounds, or because of a history of nonenforcement, or because the offense involves essentially a minor matter of private concern and the victim is not interested in having it pursued. On the other hand, the nature and circumstances of the offense, the identity of the offender or the victim, or t he attendant publicity, may be such as to create strong public sentiment in favor of prosecution. While public interest, or lack thereof, deserves the prosecutor's careful attention, it should not be used to justify a decision to prosecute, or to take other action, that cannot be supported on other grounds. Public and professional responsibility sometimes will require the choosing of a particularly unpopular course.
>
> Economic, physical, and psychological considerations are also important in assessing the impact of the offense on the victim. In this connection, it is appropriate for the prosecutor to take into account such matters as the victim's age or health, and whether full or partial restitution has been made. Care should be taken in weighing the matter of restitution, however, to ensure against contributing to an impression that an offender can escape prosecution merely by returning the spoils of his/her crime.

U.S. Attorney's Manual, Principles of Federal Prosecution § 9-27.230(B)(2) <http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/27mcrm.htm#9-27.230> (assessed Sept. 2002). The general threshold for initiating a federal cybercrime prosecution is $5,000 in "damage" or "loss", a figure that comes from 18 U.S.C.S. § 1030, which is the basic federal cybercrime provision. *See* 18 USCS §§ 1030(a)(4) & 1030(a)(5). "Damage" is defined as "any impairment to the integrity or availability of data, a program, a system or information." 18 USCS § 1030(e)(8). "Loss" is defined as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 USCS § 1030(e)(11); The *Patriot Act of 2001* clarified the meaning of "loss" as used in the statute. *See* 107 H.R. 3162, *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism* (stating that "the term 'loss' means

crimes will by default expand the computer crime docket for local prosecutors.

Can a local prosecutor obtain assistance from federal authorities who have more expertise in dealing with computer crime? Unfortunately, this often depends on the relationship between the local and federal authorities; there needs to be a more effective way of providing for local-federal cooperation with regard to the investigation and prosecution of computer crime. Various federal agencies have made significant efforts to increase their abilities to prosecute all sorts of cybercrime, including those involving international issues.[113] However, if the crime does not fall within federal jurisdiction, the only way a local prosecutor can obtain the assistance of federal authorities is by virtue of a pre-existing cooperative arrangement between them.[114] If such an arrangement is not in place, federal agencies will likely be unable to assist with local prosecutions due to the time constraints imposed by state law. In those cases, prosecution of a crime that involves acquisition of evidence from another sovereignty will prove incredibly difficult. This is especially so given *Speedy Trial Act* requirements in local prosecutions.[115]

As is explained below, the proliferation of transborder issues with regard to cybercrime prosecutions requires the creation of a proactive

---

any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service"). Prior to this amendment, the statute did not define "loss". *See e.g.* Dept. of Justice, Computer Crime and Intellectual Property Section, *Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001* <http://www.cybercrime.gov/PatriotAct.htm> (assessed Sept. 2002). The definition incorporated into the statute was based on the holding in *United States v. Middleton,* 231 F.3d 1207, 1210-11 (9th Cir. 2001). *See id.* The *Patriot Act* also made it clear that the government can aggregate the loss an individual causes to different protected computers to meet the jurisdictional threshold of $5,000 in loss. *See* Dept. of Justice, Computer Crime and Intellectual Property Section, *Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001, supra.* One author criticizes the criteria set forth above for providing little meaningful guidance to federal prosecutors. *See* Michael A. Simons, *Prosecutorial Discretion And Prosecution Guidelines: A Case Study In Controlling Federalization,* 75 N.Y.U.L. Rev. 893, 934 (2000) (stating that "at bottom the Principles of Federal Prosecution are so vague as to be meaningless"). This author also points out that the section in the *U.S. Attorney's Manual* dealing with provides no criteria for federal prosecutors to use in deciding whether a case should be brought. *See id.* at 935; *see also* U.S. Attorney's Manual, *Computer Fraud* § 9-48.000 <http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/48mcrm.htm> (assessed Sept. 2002).

113. *See supra* n. 108 and the accompanying text for one example of such an effort.

114. *See generally* Remarks of Attorney General Janet Reno to the Online Summit <http://www.cybercrime.gov/reno-sp.htm> (Dec. 3, 1997).

115. For example, in Pennsylvania, a defendant must be tried within 365 days of a criminal complaint being filed.

plan designed to facilitate cooperation between local prosecutors and federal agencies.[116] These issues can only be addressed successfully if such a plan is in place.

C. Issues Unique to Local Prosecutors

Some of the issues that are presented by transborder cybercrime cases pose unique problems for local prosecutors. The sections below examine some of these issues.

1. *Skills and Experience*

The prosecution of crimes involving digital evidence takes specialized skills.[117] Therefore, one of the first issues that must be addressed with regard to preparing local prosecutors to deal with transborder cybercrime cases is giving them the means and the opportunities they need to acquire the requisite knowledge with regard to computer forensics and cybercrime. Because of their relative maturity and, perhaps, their career paths, most of the chief prosecutors and most of their senior assistants will have concentrated their careers in areas other than computers and information technology.[118] If the chief prosecutor is not fa-

116. *See* Section II(D) of the accompanying text. *See e.g.* David McGuire, *International Cyber-Police Urge Increased Cooperation* <http://www.infowar.com> (July 26, 2000).

117. *See e.g.* Michael Chertoff, Dept. of Justice, *Statement of Michael Chertoff Assistant Attorney General Criminal Division U.S. Department of Justice Before the Subcommittee on Crime Committee on the Judiciary U.S. House of Representatives* (Washington, D.C., June 12, 2001) <http://www.cybercrime.gov/cybercrime61201_MChertoff.htm> (assessed Sept. 2002):

> Combating computer crime requires a team of professionals, including investigators, forensic experts, and prosecutors, all of whom have technical expertise. In addition to traditional investigative skills, cybercrime investigators must be well versed in the intricacies of technology to insure that evidence is not lost or overlooked. Forensic experts must know how to handle electronic evidence to protect its integrity for later use at trial, as well as how to recover and analyze digital evidence from computers with hard drives that store gigabytes of data. And prosecutors must understand the jargon and complexities of high-technology crimes and be able to translate technical evidence into a form understandable to a judge and jury.

Id.

118. A National Institute of Justice study of local law enforcement documented concerns about this lack of technological sophistication at the management level:

> One of the most frequently heard complaints . . . pertained to awareness and support from upper level managers and policymakers. Although not the case universally, individuals holding upper management positions generally are older and usually have worked with computers at a basic level. Many of the respondents believed this in part explains why many senior officials do not fully appreciate the seriousness of the rapidly growing problem of electronic crime or what law enforcement needs to keep pace with these criminals. Of 122 responses, 84 indicated that managers are either unaware or only somewhat aware of computer crime issues.

National Institute of Justice, *supra* n. 104, at 16.

miliar and comfortable with computer crime issues, it will be very difficult for her to comprehend the issues involved as to the acquisition and use of evidence from an international prospective.[119] As an analogy, it would be very difficult for a local prosecutor to prosecute gun crimes without understanding the issues involved in proving that a particular gun was used in a crime and how that gun was used. Of course, as the science of forensic firearms identification has evolved,[120] local prosecutors accepted the challenge it presented and have developed the expertise they need to become adept at prosecuting cases involving ballistics and other firearms issues. Unfortunately, those same prosecutors most likely would admit to their lack of knowledge as to the intricacies of computers, computer systems and software.

In addition to acquiring the basic technical knowledge he or she will need to approach a cybercrime case, the local prosecutor will also have to learn how to obtain admissible evidence from other jurisdictions, which can be other states or other countries. And while the process of obtaining evidence from other states can be quite difficult in cybercrime prosecutions, these difficulties are only compounded when the evidence must be obtained from another country or countries. The first section of this article gives an overview of what is involved when a United States prosecutor must obtain evidence from abroad.[121] It is a very difficult process, especially for the uninitiated, and it is highly unlikely that a local prosecutor will ever have had to undertake this endeavor; very few local prosecutors, for example, have ever had occasion to contact the Office of International Affairs.[122] Local prosecutors must, however, gain these skills if they are to prosecute transborder cybercrime, a phenomenon which they are going to encounter with ever-increasing frequency.[123] Local prosecutors need to know in advance how to obtain evidence from abroad by using both formal and informal methods; if they wait until a case arises and they need to implement these skills, the learning curve involved in mastering them dramatically decreases the prosecutor's chances of obtaining the evidence she needs within the timelines imposed by the law of that jurisdiction. And if a prosecutor cannot obtain the evidence she needs, she might as well not even attempt to prosecute the crime.

---

119. This knowledge on the chief prosecutor's part will also be needed if she is effectively to cooperate with the local community, who will be looking to her for help in dealing with these types of cases. *See e.g.* Ronald L. Mendell, *Incident Management with Law Enforcement* <http://www.securityfocus.com/infocus/1523> (Dec. 12, 2001).

120. *See generally* An Introduction to Forensic Firearms Identification, *Fundamentals of Firearms ID* <http://www.firearmsid.com/A_FirearmsID.htm> (assessed Sept. 2002).

121. *See* Section I of the accompanying text.

122. *See supra* n. 54 and the accompanying text.

123. *See* Sections III(A) & III(B) of the accompanying text.

The time and money needed to develop these skills will be a central issue for most local prosecutors. After all, although cybercrime is infiltrating all aspects of our society, it certainly will not overtake "Driving Under the Influence" with regard to the raw number of cases filed at any time in the near future. As a result, some local prosecutors may feel, not unjustifiably, that it is not worth the time and effort to develop these skills, at least not for the time being. As a result, some compelling cases may go unprosecuted.

2. *Time*

Of the prosecutors working at all levels of law enforcement, local prosecutors are no doubt the most stressed for time.[124] It is not unusual for an assistant district attorney to deal with the disposition of ten to twenty cases in a single day.[125] And since cybercrime cases, like homicide cases, present difficult legal, scientific and technical issues, this pace simply does not allow local prosecutors to dedicate the time and energy they need to prosecute crimes involving the acquisition and use of digital evidence.[126]

In order to deal effectively with a case involving transnational issues, the prosecutor must be involved from the outset. The first step in a cybercrime case is often determining where the perpetrator is located and how the evidence needed to prosecute the case can be acquired. If it is determined that the perpetrator's activities crossed national boundaries at any stage, a whole new dimension will be added to the investigation. Local, state and federal officials will have to cooperate, which necessitates an investigation that far exceeds the scope of most other criminal investigations.[127] Having an adequate amount of time to deal with these issues will be a central problem from the local prosecutor's prospective. While local prosecutors will certainly not be willing to let murderers go free so they can pursue minor hacks, they must recognize

124. *See* NDAA for statistic.

125. A survey of local prosecution conducted found that local prosecutors' offices closed "[o]ver 2.3 million felony cases and almost 7 million misdemeanor cases" in 2001. Carol J. DeFrances, *Prosecutors in State Courts 2001,* Bureau of Justice Statistics Bulletin 6 <http://www.ojp.usdoj.gov/bjs/pub/pdf/psc01.pdf> (May 2002). For the results of a study examining the burden on local prosecutors, *see* M. Elaine Nugent & Jane Nady Sigmon, *Assessing Prosecutor Workload: The Tennessee Experience* <http://www.ndaa.org/pdf/Oct%2099%20Pros.%20PDF%20Nugent%20Sigmon.pdf> (Sept./Oct. 1999).

126. As Mr. Schwerha's personal experience attests, prosecutors handling cybercrime cases need to be involved in the cases from the beginning of the initial investigation to the resolution of the final appeals. Every cybercrime case presents difficult legal issues and therefore requires the participation of a prosecutor who is knowledgeable in this area.

127. *See generally* William Matthews, *Reno: Law Enforcement Ill-Prepared for Cybercrime* <http://www.fcw.com/fcw/articles/2000/0306/web-1reno-03-10-00.asp> (May 10, 2000).

that this, too, is an area for which they are responsible. Management within the local prosecutor's office must allocate to the individuals responsible a realistic amount of time to pursue these cases.

3. *Homeland Security*

As local prosecutors become adept at dealing with the issues presented by cybercrime cases, especially the transborder aspects of these cases, they may be able to contribute to the nation's counter-terrorism efforts, which will have to encompass the threat of cyberterrorism as well as "real world" terrorism.[128] The staffs of the local prosecuting agencies in this country comprise thousands of local prosecutors,[129] many of whom can be recruited to assist with these efforts once they acquire the skills needed to deal with cybercrime and cyberterrorism.[130]

After the September 11 attacks on New York and on the Pentagon, President Bush created the Office of Homeland Security.[131] Appointed to head the new Office of Homeland Security, ex-Pennsylvania Governor Thomas Ridge outlined the goals of his office as both preventing terrorist attacks and educating the public about the risk of such attack.[132] In 2002, the FBI revised its strategic goals; combating terrorism and cyber-

128. *See e.g.* Diane Frank, *Cybersecurity Called Key to Homeland Defense* <http://www.fcw.com/fcw/articles/2001/1001/news-cyber-10-01-01.asp> (Oct. 1, 2001).

129. *See* Carol J. DeFrances, *supra* n. 97.

130. *See e.g.* Tech Law Journal, *Advisory Panel Reports on Cyber Terrorism, Gov. Gilmore's Comments on Cyber Terrorism* <http://www.techlawjournal.com/security/20001214.asp> (Dec. 14, 2000):

> Our preparedness for cyber terrorism must be broader, to include all levels of private and public activity. Critical local, state, regional and national systems are computer controlled . . . Power grids, communications, airlines, hazardous materials, hospital life support, the nation's economy, and our national defense.
>
> For years terrorism has been viewed as the exclusive domain of national security. That view requires a reality check. The federal government must recognize that states, communities, governors, mayors, and citizens all have responsibilities, and important vital roles in dealing with the terrorist threat.

Id.; Governor Gilmore of Virginia chaired the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. *Id.; see also Second Annual Report of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction* 41 <http://www.rand.org/nsrd/terrpanel/terror2.pdf> (Dec. 15, 2000).

131. *See e.g.* Dawn House, *Bennett Predicts Cyber Terrorism,* Salt Lake Tribune <http://www.sltrib.com/2002/jun/06102002/utah/744211.htm> (June 10, 2002); Paul Quinn-Judge, *Cracks in the System,* Time Magazine <http://www.time.com/time/europe/magazine/article/0,13005,901020617-260664,00.html> (June 17, 2002); *see also* Diane Frank, *supra* n.128.

132. *See* The White House President George W. Bush, *President Establishes Office of Homeland Security* <http://www.whitehouse.gov/news/releases/2001/10/20011008.html> (Oct. 2001); *see also* The White House President George W. Bush, *Homeland Security Briefing with Gov. Ridge and Security Abraham* <http://www.whitehouse.gov/news/releases/2001/11/20011115-5.html> (Nov. 15, 2001).

crime are now among its highest priorities.[133] On June 6, 2002, President Bush proposed the creation of a Cabinet-level Department of Homeland Security that would be given four essential tasks:

This new agency will control our borders and prevent terrorists and explosives from entering our country. It will work with state and local authorities to respond quickly and effectively to emergencies. It will bring together our best scientists to develop technologies that detect biological, chemical, and nuclear weapons, and to discover the drugs and treatments to best protect our citizens. And this new department will review intelligence and law enforcement information from all agencies of government, and produce a single daily picture of threats against our homeland. . . . [134]

By June of 2002, it had become apparent that the agency in charge of Homeland Security needs to gather evidence of trends, as well as specific acts that may give rise to intelligence of terrorist activities.[135] There certainly is a need for better information gathering and sharing.[136]

Simultaneously, local prosecutors are the people most familiar with the criminal activities within their jurisdictions because they are primarily responsible for prosecuting those crimes.[137] However, there is no

133. Under Director Robert Mueller's proposed reorganization, the FBI's top ten priorities would become as follows:

1. Protect the United States from terrorist attack
2. Protect the United States against foreign intelligence operations and espionage
3. Protect the United States against cyber-based attacks and high-technology crimes
4. Combat public corruption at all levels
5. Protect civil rights
6. Combat transnational and national criminal organizations and enterprises
7. Combat major white-collar crime
8. Combat significant violent crime
9. Support federal, state, local and international partners
10. Upgrade technology to successfully perform the FBI's mission

See FBI Strategic Focus, *FBI Priorities* <http://www.fbi.gov/page2/52902.htm> (assessed Sept. 2002); *see also* Robert S. Mueller III, *supra* n. 102.

134. George W. Bush, *Remarks by the President in Address to the Nation* (Washington, D.C., June 6, 2002) <http://www.whitehouse.gov/news/releases/2002/06/20020606-8.html> (assessed Sept. 2002) [hereinafter Bush, *Remarks*]. *See e.g.* President George W. Bush, *The Department of Homeland Security* 2-3 [hereinafter Bush, *Homeland Security*] <http://www.whitehouse.gov/deptofhomeland/book.pdf> (June 2002).

135. *See e.g.* Bush, *Homeland Security*, *supra* n. 134; *see also* Bush, *Remarks*, *supra* n. 134.

136. *See e.g.* Bush, *Homeland Security*, *supra* n. 134.

137. A terrorist group might, for example, decide to acquire the funds they need to carry out a terrorist attack by defrauding a series of people for relatively small amounts, perhaps using eBay auctions, operating on the premise that the small frauds are less likely to attract law enforcement attention. And it is quite true that a series of crimes such as this might not be noticed by federal anti-terrorism authorities. But the local prosecutors who

mechanism to effectively track cybercrime prosecution at the local level. Correspondingly, there is no support network which a local prosecutor can use to determine if the eBay fraud he is investigating is linked in any way to any larger criminal network. It is, therefore, apparent that the effort at combating terrorism would benefit from the establishment of some network facilitating interaction and the exchange of information between the FBI, the Office/Department of Homeland Security Office and local prosecutors with regard to activity that may constitute terrorism, especially cyberterrorism.[138]

The basic point is that there should be some way for information to be effectively gathered and disseminated at the local level. Consequentially, that same entity could help local prosecutors effectively deal with transnational evidence gathering, and prioritizing criminal investigations within their office. If the Federal government executes a plan of intelligence gathering, the money would be better spent utilizing the resources we have to a greater extent, than to bring on totally new departments whose functions somewhat cross over with local prosecutors at the present time. This is especially true in the present case, where that same entity could assist local prosecutors pursuit of international cybercrime in an efficient fashion.

4. *Lack of Funding*

Lack of funding for costs associated with prosecution is a central problem for local prosecutors who want to become competent in dealing with transborder cybercrime issues. While the problem crosses over various areas, lack of funding certainly will be one of the greatest hindrances for the ability of local jurisdictions to prosecute transborder crime. There

---

would deal with the victims' complaints are in the perfect position to notice what might be a pattern of activity and bring it to the attention of counter-terrorism agencies. This type of operation is not unprecedented; the Internet Fraud Complaint Center, which provides a mechanism for reporting fraud committed via the Internet, regularly submits results of complaints to local agencies, while at the same time tracking trends at the national level. *See e.g.* National White Collar Crime Center, *IFCC 2001 Internet Fraud Report* <http://www1.ifccfbi.gov/strategy/IFCC_001_AnnualReport.pdf> (assessed Sept. 2002). Indeed, the Internet Fraud Complaint Center is currently the primary mechanism for reporting terrorist activity to federal authorities. *See* Dept. of Justice, Federal Bureau of Investigation, *FBI Tips and Public Leads* <https://www.ifccfbi.gov/complaint/terrorist.asp> (assessed Sept. 2002).

138. Critics might argue that such a network would decrease security, on the assumption that the more people there are who know about information, the less likely it is that the information will be kept confidential. This argument, however, ignores the realities of how this information sharing could occur. For example, local prosecutors could submit their information based upon guidelines set at the state or federal level; they would, in turn, only receive receiving evidence from other jurisdictions that was relevant to specific investigations they had already initiated.

are several particular problems that combine to make this area worthy of discussion.

There are virtually no local prosecutors who have the expertise with regard to computer forensics and transborder evidence-gathering needed to prosecute transborder cybercrime. And to make matters worse, there is no funding to provide the training that will be needed to bring local prosecutors up to speed in these areas.[139] It may cost a local municipality $5,000—a substantial sum—to send a prosecutor to a two week course on network intrusions. Thus, the amount an area is willing to spend will greatly effect its ability to prosecute cybercriminals.

Even if a municipality is willing and able to underwrite training expenses, the other costs involved in prosecuting a cybercrime case can be cost-prohibitive. Assume, for example, that a local prosecutor has a case in which a hacker used an Internet Service Provider based in India to attack a computer in the prosecutor's local community. To win his case, the prosecutor must prove that the hacker used the Indian ISP, but how is he to afford the $10,000 it will cost to bring in a representative from the Indian ISP to testify at trial? The likelihood of obtaining funding for expenses such as these can appropriately be analogized to the "chicken or the egg" query: It is unlikely that adequate funding for transborder evidence collection will be allocated until the number of cases involving these issues is significant enough to draw the attention of legislators. Unfortunately, without the training and resources needed to prosecute these crimes, they will not be charged and will, like many cybercrimes, simply never be reported.[140] One can only hope that legislators will real-

139. A National Institute of Justice study released in 2001 found that the need for training is critical:

> Both entry-level and advanced training are needed for law enforcement officers and investigators, prosecutors . . . and judges. First-line officers who secure the initial crime scene need training on basic forensic evidence recognition and collection techniques. National standards should be developed and applied toward a certification program that ensures uniform skill levels. Prosecutors and judges require awareness training and case histories on electronic crime incidents.
>
> State and local law enforcement representatives noted repeatedly that advanced computer and forensics related classes are difficult to find. Another concern was that the level of sophistication of the equipment, software tools, and training needed far exceeds the budgets of most departments. This is especially problematic for courses offered out of State. Attendance is expensive in terms of both personnel time and tuition, travel, and per diem costs.

National Institute of Justice, *supra* n. 104, at 32.

140. *See e.g.* National Institute of Justice, *supra* n. 104, at 17:

> Most participants in the study believe that the vast majority of computer-related crimes are not reported to authorities as a criminal matter. For example, companies may choose to write off a loss, handle it internally, or pursue the case as a civil matter, according to the view of many participants. Since budget makers and policymakers rely heavily on numbers and on the priorities voiced by voters, the dearth of hard data and general awareness hurts most efforts to build stronger State and local crime control measures against electronic crime. Anecdotal infor-

ize that this is a problem that will not go away, that will only become worse as Internet usage increases and American borders become more "virtually" permeable to the depredations of hackers located around the globe.

Funding is, and will continue to be, a problem in this arena. It will always be difficult to acquire the funds needed to prosecute transborder crime.

---

mation often is the only available evidence that can be used to capture management's attention. Many of those who participated in the assessment noted that if the actual losses and impact of computer-related crime could be studied and documented, the public and, by extension, public officials would begin to understand how serious this component of crime has become.

Id.; Everyone concedes that cybercrime statistics are unreliable. One is that law enforcement agencies, at least in the United States, do not break cybercrimes out into a different category. This means, therefore, that if someone uses a computer to commit fraud, the conduct will simply be reported as fraud. Another problem is that many cybercrimes go undetected. *See e.g.* U.N. Commission on Crime Prevention and Criminal Justice, *Conclusions of the Study on Effective Measures to Prevent and Control High-Technology and Computer-Related Crime: Report of the Secretary-General* U.N. Doc. E/CN.15/2201/4 <http://www.odccp.org/adhoc/crime/10_commission/4e.pdf> (assessed Sept. 2002). And yet another problem is, as the passage quoted at the beginning of this note illustrates, that cybercrimes are often not reported to authorities. The 2002 *CSI/FBI Computer Crime and Security Survey* <http://www.gosci.com/press/20020407.html> (assessed Sept. 2002), found, for example, that only 34% of the respondents reported attacks to law enforcement. Only 31% of those responding to the AusCert, *2002 Australian Computer Crime and Security Survey* <http://www.auscert.org> (assessed Sept. 2002), reported attacks to law enforcement. And both the Confederation of British Industry (CBI), <http://www.cbi.org.uk> (assessed Sept.2002). for a description of the survey and its findings go to the CBI, *Business Leaders Warn of Cybercrime Threat to Internet Development* <http://www.cbi.org.uk/8025671600 4baae5/33a87f2eee41b54e80256803004f04e4/eff1596523e1653f80256aaf00390135?Open Document> (Aug. 29, 2001) and Price Waterhouse Coopers <http://www.pwcglobal.com> (assessed Sept. 2002). And Price Waterhouse Coopers, *Information Security Breachers Survey 2002* <https://www.security-survey.gov.uk/> (assessed Sept. 2002), which found that UK businesses seldom reported attacks to law enforcement because they were more worried about damage to their reputation resulting from publicity about an attack than about financial damage from attacks. There are, finally, jurisdictional and doctrinal impediments to the compilation of accurate cybercrime statistics:

> Further problems arise with the mass victimization caused by offences such as virus propagation, because the numbers of victims are simply too large to identify and count, and because such programs can continue creating new victims long after the offenders have been caught and punished. A further factor complicating the gathering and comparison of national crime statistics will be the fact that transnational computer-related crimes are, by definition, committed in or have effects in at least two States, and, in some cases, in many States, risking multiple reporting or no reporting at all.

U.N. Commission on Crime Prevention and Criminal Justice, *Conclusions of the Study on Effective Measures to Prevent and Control High-Technology and Computer-Related Crime: Report of the Secretary-General* 10-11, U.N. Doc. E/CN.15/2201/4 <http://www.odccp.org/adhoc/crime/10_commission/4e.pdf> (2001).

5. *Succession Issues*

Aside from acquiring knowledge in the first place, keeping people with that knowledge within the office should be a priority. This will be dealt with in part by formulation and execution of a plan dealing with succession issues, as discussed later herein. Simply put, once a local prosecutor proceeds down the road to try to prosecute cases involving transborder evidence gathering, that office must assure that someone within it always has the expertise to proceed with those cases. If several of these types of cases are started, and the prosecutor responsible therefore decides to leave to pursue a job in the private sector,[141] an obvious and significant problem arises. An example of the havoc this would cause is easy to illustrate. If a local prosecutor's office merely assigns one young prosecutor to acquire evidence from abroad, no one will be able to understand or explain to judges how this evidence was obtained after that prosecutor leaves. This could lead to suppression of evidence because the prosecutor then in charge of the case would not have a clear understanding of the issues involved.

It is similarly easy to understand how having only one prosecutor involved would leave an office paralyzed if they did not have routinely kept accurate records indicating the status of the investigations. As you can imagine, if you send several requests out to the Office of International Affairs and the prosecutor in charge leaves, the next person in line likely may have no idea what is going on. More importantly, if that next prosecutor in line does not have the basic cybercrime prosecution skills necessary to function in this arena, you may not be able to prosecute those cases in the pipeline without significant and immediate efforts with regard to education of that prosecutor. Therefore, succession issues become incredibly important with regard to prosecution of these cases.

The prosecution of transnational cases at the local level requires a type of expertise that heretofore has not been necessary; until recently, prosecutors, especially local prosecutors, did not need to be conversant with technology and the ways in which it can be put to criminal ends. Consequently, those who are the most likely to have at least some familiarity with computers and computer forensics will be the younger mem-

141. A National Institute of Justice study issued in 2001 found that the loss of trained personnel was a major problem:

> Often, a jurisdiction's promotion policies undermine the retention of uniquely trained and experienced personnel. The loss is felt most keenly in special operations units in which there has been a heavy investment in training. New personnel must be 'trained up," which is time consuming and expensive. . . .
>
> Expertise is lost, not only to promotions and transfers but to the private sector, where the appeal of higher pay and, often, shorter hours attracts many specially qualified personnel. . . .

National Institute of Justice, *supra* n. 104.

bers of local prosecutor's offices throughout our nation. These prosecutors, however, are likely to move into the private sector after only a few years, as their trial expertise and familiarity with high-tech cases make them attractive candidates for employment in the private sector. This is an issue that must be addressed, since local prosecutors' offices will require a stable, experienced staff to deal with transnational issues and cybercrime prosecutions.

Succession issues will be addressed head-on in development of a plan for dealing with these types of cases. A central theme is, and will continue to be, the devotion of management to the idea that their office must be equipped with the intellectual capital to deal with these issues.

6. *Evidence, Evidence, Where's the Evidence?*

While local prosecutors are increasingly faced with prosecuting and investigating crimes having transborder issues, they are not devoting enough resources to allow for acquisition and use of evidence from abroad. This, of course, makes the transnational cybercrime prosecution very difficult. Anyone who has actually gone through the process of gathering evidence that could be usable at trial knows of the difficulties inherent therein. Not only must you obtain logically relevant evidence[142], but it must also be legally relevant. One must also be able to use the evidence once they obtain it. Most likely this involves authentication of any documentary evidence by virtue of non-hearsay testimonial evidence.[143]

If you contemplate this process within the international context, one may clearly understand how difficult producing that evidence would be. Many examples abound. If a local prosecutor wants to obtain Internet records pertaining to the use of a particular IP number on a particular date and time in Brussels, Belgium, that local prosecutor most probably will be making a request to the Office of International Affairs and Department of Justice. That office will then engage the procedures of the Mutual Legal Assistance Treaty between the United States and Belgium in order to ascertain what may be done and in what time frame. Several

142. What I mean by logically relevant is that it would be relevant to the normal person. This differs from legally relevant in that something may not be legally relevant even though you would think it would be more likely to prove something to be true. A prime example of this is prior bad acts. One may not be able to use prior bad acts in the prosecution of a defendant because it would be unduly prejudicial under the law. However, it is commonly held that someone is more likely to recommit a crime that they have already committed in the past.

143. Under the Federal Rules of Evidence, hearsay is a statement not a court statement offered for the truth of the matter asserted. It is roundly misconstrued by the courts; however, prosecutors are responsible for offering admissible evidence at trial, and thereby we must adapt to the overly broad view of hearsay pursuant to presiding judges.

months or more may pass before acquisition of the requisite evidence, if it is acquired at all. During this time, presumably the alleged criminal is either out of jail because charges have not been filed, or is in jail, with the clock running, hoping each and every day leads closer to the mandatory dismissal of his charges for not being timely tried. Local prosecutors cannot obtain the evidence any faster, and therefore must incorporate these slow timelines into their process.

The local prosecutor will also have to deal with the evidence, if and when it is obtained. He may, for example, have to bring in witnesses to authenticate the evidence.[144] The idea of spending several thousands of dollars to bring in a custodian of records from an ISP in Belgium to prosecute what is most likely a computer related offense costing less than that in restitution (since the more damaging cases may be taken to the federal level) is not at all appealing to a local prosecutor. Of course, neither is the idea of letting a criminal escape prosecution. This type of Hopsons Choice is not exclusively limited to transactional cybercrime prosecution and will not be going away anytime in the near future.

7. *Search and Seizure Laws Must Be Changed*

As the Invita investigation illustrates,[145] transborder searches and seizures present very difficult issues for law enforcement officers.[146] If a cybercriminal in Oman hacks into an Arkansas computer system, can the Arkansas investigator search for and seize all related evidence that can be obtained via connections to that local computer?[147] That is, can the Arkansas investigator follow the connection back to the hacker's

144. *See* USCS Fed. Rules Evid. R 901(a). Under this rule, the party attempting to utilize computer records must prove these are what they are proposed to be. Most of the time, this is done by stipulation, or through the testimony of the custodian of records. Thus, we may be faced with flying in the custodian of records from India, which is, of course, very expensive. *See also* Orin S. Kerr, *Computer Records and the Federal Rules of Evidence* <http://www.cybercrime.gov/usamarch2001_4.htm> (Mar. 2001).

145. *See* Section I of the accompanying text.

146. Indeed, as the drafters of the Council of Europe's Convention on Cybercrime noted, even the applicability of traditional terminology may become problematic:

> In adapting traditional procedural laws to the new technological environment, the question of appropriate terminology arises in the provisions of this section. The options included maintaining traditional language ('search' and 'seize'), using new and more technologically oriented computer terms ('access' and 'copy'), as adopted in texts of other international for a on the subject (such as the G8 High Tech Crime Subgroup), or employing a compromise of mixed language ('search or similarly access', and 'seize or similarly secure'). As there is a need to reflect the evolution of concepts in the electronic environment, as well as identify and maintain their traditional roots, the flexible approach of allowing States to use either the old notions of 'search and seizure' or the new notions of 'access and copying' is employed.

See Council of Europe, *Report, supra* n. 1, at ¶ 137.

147. *See* Sandra Underhill, *Cybercrime Prosecution is a Nightmare* <http://www.InfiniSource.com/features/cybercrime-pf.html> (Nov. 2, 2000).

computer in Oman, searching the computer and seizing evidence on it? This scenario illustrates two key search and seizure issues that arise in this context, both of which are discussed below.

a) Transnational Evidence-Gathering

It is simply not clear whether an investigator can lawfully use a computer located in his jurisdiction to "seize" evidence located in another country. Under the Fourth Amendment to the United States Constitution, and most of its state counterparts, no search of a residence or of a business can take place unless it is authorized by a search warrant or by a valid exception to the warrant requirement.[148] Also, under most state law, a search warrant is only valid for searches that are executed within the territorial jurisdiction of the court that issued the warrant, which is usually a county or municipality.

Using the example given above, assume the Arkansas investigator obtains a warrant to search the local computer system that was broken into by the Omani hacker; the officer is allowed to search the local computer system for evidence pertaining to the hacker's breaking into it and to the damage the hacker caused to the system. For the purposes of this discussion, let us assume that the Omani hacker copied files containing valuable, proprietary information from the local computer system. In the course of searching the victimized computer system, the officer discovers that he can "track back" to the hacker's computer, which the officer clearly has reason to believe is located in another country (though he may not know precisely which country). He also believes he can access valuable evidence that is located on the hacker's computer, evidence he can copy and retrieve, evidence that could be used to convict the hacker. For purposes of this discussion, we will assume that the officer's act of gaining access to the Omani computer constitutes a "search" under

148. *See e.g.* Susan W. Brenner & Barbara A. Frederiksen, *Computer Searches and Seizures, Some Unresolved Issues,* 8 Mich. Telecomm. Tech. L. Rev. 39 (2002) <http://www.mttlr.org/html/voleight/BrennerTYPE_HTML.htm> (assessed Sept. 2002):

> The Fourth Amendment guarantees citizens the right to be free from 'unreasonable searches and seizures'. A 'search' or a 'seizure' is reasonable if it meets certain requirements. Officers may conduct a search and/or seizure pursuant to a search warrant that is based on probable cause. The warrant must be issued by a neutral and detached Magistrate Judge and certain other requirements. The officers' conduct will be 'reasonable,' not in violation of the Fourth Amendment, as long as they stay within the scope of that warrant, or, in other words, as long as their actions are calculated to locate evidence for which the warrant authorizes them to search and seize. There are also a number of exceptions to the warrant requirement; if officers carry out a search and/or seizure pursuant to one of these exceptions, their conduct will be deemed to be reasonable even though they acted without a warrant. If officers carry out a search or seizure that is not authorized by a warrant or by an exception to the warrant requirement, their conduct will be deemed unreasonable, and in violation of the Fourth Amendment.

Id. (footnotes omitted).

the Fourth Amendment and that his act of copying whatever pertinent evidence he finds on that computer constitutes a "seizure" of it.[149]

The officer now faces a quandary: If he proceeds through formal channels, he will have to submit a request using an MLAT, if he is lucky; and even the MLAT procedure can take days or even months to obtain the evidence.[150] If the officer is not lucky and there is no MLAT in effect between the United States and Oman, he will have to initiate the letter rogatory procedure, which will take months or even years.[151] If he wants to proceed informally, he will have to be able to contact local law enforcement officers in the country in which the computer is located;[152] even if the officer can identify the physical location of the computer, it is unlikely that he will have personal contacts he—like the Air Force agents in the Rome labs case[153]—can call upon to monitor the Omani computer and obtain an Omani warrant authorizing them to seize and search it. The officer's final option is self-help, i.e., to "track back" to the hacker's computer and download any evidence he may be able to access there;[154] if he does this, he can cite the district court's ruling in the Invita case and argue that the Fourth Amendment did not apply to his actions because the "search" was conducted outside the physical boundaries of the United States, i.e., in Oman.[155] Of course, that ruling is being appealed, and may not stand. As a final alternative, the officer can argue that while his actions were not authorized by a search warrant, they

149. *See* Section I of the accompanying text. When one deals with computer searches and seizures, it can be difficult to tell precisely where the "search" or a "seizure" occurred. *See id.* "[T]he parameters used to implement Fourth Amendment guarantees in the context of real world searches and seizures are well-established. The cyber world lacks the real world's unambiguous physical boundaries, therefore it is often difficult to translate these guarantees into the context of computer searches where simply determining when a 'search' or 'seizure' occurs can be a complicated endeavor, as can differentiating a 'search' from a 'seizure'." *Id.; see also* Council of Europe, *Report, supra* n. 1, at ¶ 137 (stating that "[I]n adapting traditional procedural laws to the new technological environment, the question of appropriate terminology arises. . . . The options included maintaining traditional language ('search' and 'seize'), using new and more technologically oriented computer terms ('access' and 'copy') . . . or employing a compromise of mixed language ('search or similarly access', and 'seize or similarly secure'"). For an argument that copying data is a "seizure," *see* Brenner & Barbara A. Frederiksen, *Computer Searches and Seizures, Some Unresolved Issues, supra,* at Section IV of the accompanying text.

150. *See* Section II(A) of the accompanying text.

151. *See* Section II(A) of the accompanying text.

152. *See* Section I of the accompanying text.

153. *See* Section I of the accompanying text.

154. *See* Section I of the accompanying text.

155. *See* Section I of the accompanying text. Of course, the hacker could argue that the "seizure" of the evidence occurred, at least in part, in the United States; and the subsequent analysis of the copied evidence after it was "brought" to the United States would constitute a "search," which would also have to be justified either by a warrant or by an exception to the warrant requirement. *Id.*

were justified under the Fourth Amendment's exigent circumstances exception to the warrant requirement;[156] he can claim he was justified in proceeding without obtaining a search warrant because of the very real possibility that the evidence would be destroyed had he taken the time to do so.[157]

Law enforcement deal with this dilemma in different ways; the basic approaches are illustrated by the Rome labs and Invita cases described earlier in this article.[158] At the very least, both scenarios illustrate that law enforcement is very much in an *ad hoc* mode in dealing with these issues and that some solution—presumably an approach such as that outlined in the Council of Europe's Convention on Cybercrime[159]—is absolutely essential when the process of acquiring evidence crosses national boundaries.

b) Trans-state Evidence-Gathering

In the scenario analyzed above, the investigator used computer technology to search for and "seize" evidence from a computer located outside the United States. Unfortunately, Fourth Amendment issues do not arise only in the context of transnational evidence-gathering, as is illustrated by a recent decision from a Minnesota district court.

In *United States v. Bach,*[160] Dale Robert Bach was charged with the "possession, transmission, receipt, and manufacturing of child pornography" in violation of federal law.[161] The evidence used to prosecute Bach was gathered in three ways:

> (1) an October 11, 2000, letter sent by Sgt. Brook Thomas Schaub of the City of Saint Paul police department to Yahoo requesting that Yahoo refrain from deleting any incoming or outgoing e-mail messages from Bach's e-mail account; (2) a search warrant from a Ramsey County District Court that was faxed to Yahoo requiring Yahoo to send Schaub information about Bach's Yahoo account; and (3) a search warrant from Hennepin County District Court allowing Schaub to search Bach's residence.[162]

Bach moved to suppress the evidence obtained by the letter and by the two warrants.[163] He argued (a) that the letter to Yahoo! was a seizure that was effected in violation of the *Electronic Communications*

156. *See supra* n. 16 and the accompanying text.
157. *See supra* n. 16 and the accompanying text.
158. *See* Section I of the accompanying text.
159. *See supra* n. 30-31 and the accompanying text.
160. *U.S. v. Bach*, 2001 WL 1690055 (D. Minn. Dec. 14, 2001).
161. *See Bach*, 2001 WL 1690055 at *1. For a detailed statement of facts as to how the prosecution arose, *see U.S. v. Bach*, (Eighth Circuit – No. 02-1238, Criminal), Brief of Appellant 1-7 <http://www.ca8.uscourts.gov/tmp/021238.html> (assessed Sept. 2002).
162. *Bach*, 2001 WL 1690055 at *1.
163. *See id.* at **1-6.

Privacy Act; (b) that the faxed Ramsey County warrant violated the Fourth Amendment and federal statutory law; and (c) that the Hennepin County warrant should be suppressed as the "fruit of the poisonous tree," i.e., as the product of the illegal search and seizure effected by Ramsey County warrant.[164]

The district court rejected Bach's claims as to the letter and the Hennepin County warrant,[165] but suppressed the evidence obtained as a result of the warrant issued by the Ramsey County District Court.[166] The district court found, that probable cause had existed for the issuance of the warrant.[167] It also rejected Bach's contentions that the search warrant lacked the particularity required by the Fourth Amendment.[168] The district court, however, held that Bach's motion to suppress the evidence obtained pursuant to the Ramsey County warrant must be suppressed because it was improperly executed.[169]

The court found that while the execution of the warrant was "not rendered unreasonable by the mere assistance"[170] Yahoo! employees provided in its execution, the execution was unreasonable because a federal statute, 18 U.S. Code § 3105, requires

> an authorized officer be present and acting in the warrant's execution when a third party assists in a search. In this case, [Officer] Schaub was not present and acting in the warrant's execution when the Yahoo employees searched and seized information from Bach's Yahoo account. Schaub's absence rendered this search and seizure unreasonable.[171]

The district court rejected the government's argument that the statute "does not apply to state officers executing state warrants when there was no federal involvement."[172] It found that "[w]hile state officers executing a state warrant without any assistance from federal authorities may not be required to comply with § 3105, protections analogous to those provided for by § 3105 exist under the Fourth Amendment."[173] The court explained that in reaching this conclusion it was

> recognized '[a]lthough adequate police supervision ensures that the warrant is properly executed and its scope is not exceeded, the required level of supervision varies depending on the circumstances.' *Common-*

164. *See id.*
165. *See id.*
166. *See id.* at *6.
167. *See id.* at *2.
168. The court also rejected Bach's claims that the federal statute under which the officers conducting the investigation had proceeded, e.g. 18 USCS § 2703, was unconstitutional under the First, Fourth and Fifth Amendments. *See id.*
169. *See id.*
170. *Id.*
171. *Id.*
172. *See id.* at *3.
173. *Id.*

> *wealth v. Sbordone,* 678 N.E.2d 1184, 1189 (Mass. 1997). The circumstances of this case, however, do not justify Schaub's choice to fax the warrant to Yahoo and allow Yahoo employees to conduct the search and seizure without any supervision or instruction. Police officers have taken an oath to uphold federal and state Constitutions and are trained to conduct a search lawfully and in accordance with the provisions of a warrant. . . . Civilians, on the other hand, are not subject to any sort of discipline for failure to adhere to the law. In fact, an Internet service provider is immune from suit so long as it is providing assistance in accordance with the terms of a warrant. 18 U.S. Code § 2703(e). Without an officer present, this conditional grant of immunity may become an irrefutable protection for Internet service providers to conduct searches that traverse the clearly defined limits of a warrant. In the particular context of this case, there were no safeguards ensuring that the Yahoo employees conducting the search and seizure of information in Bach's e-mail account were cautiously abiding by the terms of the Ramsey County warrant. Accordingly, the execution of the Ramsey County warrant does not pass constitutional muster.[174]

The court also found that the evidence must be suppressed

> under the rule established in *United States v. Moore,* 956 F.2d 843, 848 (8th Cir. 1992). In *Moore,* the Eighth Circuit determined that when state officials, acting without federal involvement, seize evidence that is eventually used in a federal prosecution, the state officials must comply with both state law and Fourth Amendment search and seizure requirements. *Id.* Like federal law, Minn. Stat. §§ 626.13 and 626A.06 require that a law enforcement officer be present at the execution of a warrant. Accordingly, Schaub's absence during the execution of the warrant violates Minnesota law.[175]

Not surprisingly, the *Bach* decision is being appealed.[176] Both the government and a group of Internet Service Providers, who have appeared as amicus curiae, are arguing that the district court erred in holding that the Fourth Amendment requires the physical presence of a police officer while an Internet Service Provider executes a search warrant requiring the ISP to produce certain evidence.[177] The government is arguing (a) that § 3105 does not apply to state officers when there is no Fourth Amendment violation;[178] and (b) that the Fourth Amendment

174. *Id.*

175. *Id.* at *4.

176. *See Bach,* 2001 WL 1690055.

177. *See U.S. v. Bach,* (Eighth Circuit – No. 02-1238, Criminal), Brief of Appellant <http://www.ca8.uscourts.gov/tmp/021238.html> (assessed Sept. 2002); *U.S. v. Bach,* (Eighth Circuit – No. 02-1238, Criminal), Brief of Amici Curiae Yahoo!, Inc., the Computer & Communications Industry Association, Net Coalition and the United States Internet Service Providers Association (on file with the authors).

178. *See U.S. v. Bach,* (Eighth Circuit – No. 02-1238, Criminal), Brief of Appellant 10-13 <http://www.ca8.uscourts.gov/tmp/021238.html> (assessed Sept. 2002).

"does not require an officer to be present while an email provider renders technical assistance in the execution of a valid search warrant."[179] In effect, the government argues that it would be "unreasonable" to require the officer's presence:

> . . . Law enforcement must move quickly to collect and preserve electronic evidence in Internet cases. The difficulty of this task is compounded by the fact that such evidence can be voluminous, intermingled with irrelevant data, and 'vulnerable to tampering or destruction. . . . Requiring an officer to be present at all phases of email searches would make investigations impossible and impractical, slow and expensive, and overly intrusive. Such a requirement would hamper not only investigations into child exploitation, as alleged in this case, but also investigations into other types of crime that commonly involve the use of computers, including Internet fraud, hacking, software piracy, cyberstalking, threats against the President, and international terrorism.
>
> In many cases it would be literally *impossible* for a law enforcement officer to be physically present within a service provider's facility for all aspects of a search, especially if he/she is seeking different types of account information. The contents of an email message may be accessible only by a few high-level administrators at headquarters, while Internet Protocol numbers and other types of connection information may be available only through systems managers at several remote locations, and subscriber or billing information may only be stored at the customer service center. Where, then, are officers supposed to go in order to be "present" for purposes of§ 3105?
>
> Trying to coordinate the identification and collection of each piece of email data, so that it occurs in the officer's "presence" would require an enormous amount of time and money. Even assuming that an email provider could access all of its account information from one location at one time, a rigid application of § 3105 would impose significant costs for training, travel and time on law enforcement, especially state or local police. An officer like Sgt. Schaub would have to find a State law enforcement officer in California to serve and "be present" for the execution of the warrant, or Schaub would have to travel to Silicon Valley whenever he needed evidence related to a Yahoo email address.
>
> Besides increasing the time and expense for law enforcement, the District Court's ruling would impose unreasonable burdens on private third parties – service providers like Yahoo and their customers or subscribers. Yahoo would have to endure five to ten disruptions by law enforcement every week. . . . An ever-present officer would also trigger new "privacy issues and legal concerns" for the company. . . .
>
> Thus, a strict application of the "presence" requirement in § 3105 would undermine the very privacy rights that the District Court hoped to preserve. Not only would a rigid "presence" requirement be impractical and burdensome, it would be invasive and constitutionally

179. *See U.S. v. Bach*, (Eighth Circuit – No. 02-1238, Criminal), Brief of Appellant 13-29 <http://www.ca8.uscourts.gov/tmp/021238.html>.(assessed Sept 2002).

unreasonable. . . . [180]

The *Bach* case raises difficult Fourth Amendment issues because it illustrates how problematic the traditional law of search and seizure, which evolved to address actions taken in the "real," physical world, becomes when it is extrapolated to deal with conduct occurring in or by means of the "virtual world" of cyberspace. On the one hand, the *Bach* court correctly rejected the notion that law enforcement officers can wholly delegate the process of evidence collection to private parties; on the other hand, the *Bach* court did not consider precisely how the Fourth Amendment's requirement of "reasonableness" should be translated into this new environment, balancing the constitutional rights of one who, like Bach, is the object of a search warrant against the legitimate concerns of others whose privacy would be infringed by giving officers access to the computer systems of Internet Service Providers. It is to be hoped that the Eighth Circuit, to which the matter has been appealed, can arrive at some "reasonable" resolution of these extraordinarily difficult issues.

D. THE PLAN: LIKE THE BOY SCOUTS, "BE PREPARED"

The only way to deal adequately with transborder cybercrime is to develop, execute and maintain a plan of attack. Any such plan will require educating prosecutors with regard to transborder and general cybercrime issues. Prosecutors must be attuned to these needs and designate assistants in their offices to take on the task of dealing with these issues. The skills are specialized, and they will take time away from other, "real world" crimes. But it can be done, and there are resources available. The National White Collar Crime Center provides three different courses to state and local investigators.[181] Other agencies have also begun outreach programs to involve "locals."[182] Some local jurisdictions already have high tech crimes task forces that bring together local

180. *See U.S. v. Bach*, (Eighth Circuit – No. 02-1238, Criminal), Brief of Appellant 20-22 <http://www.ca8.uscourts.gov/tmp/021238.html> (assessed Sept. 2002); *see also U.S. v. Bach*, (Eighth Circuit – No. 02-1238, Criminal), Brief of Amici Curiae Yahoo!, Inc., the Computer & Communications Industry Association, Net Coalition and the United States Internet Service Providers Association 5-13 (on file with the authors).

181. *See* National Cybercrime Training Partnership <http://www.nctp.org/> (assessed Sept. 2002).

182. The National Infrastructure Protection Center (NIPC) regularly educates state and local people with regard to cybercrime issues. *See* National Infrastructure Protection Center <http://www.nipc.gov/> (assessed Sept. 2002). The same is true of the Federal Law Enforcement Training Center (FLETC); while it might seem that FLETC should train only federal law enforcement personnel, it actually educates local law enforcement officers, as well. *See* Federal Law Enforcement Training Center <http://www.fletc.gov/> (assessed Sept. 2002).

and federal personnel.[183] Such a model is very effective and, hopefully, will be utilized by other jurisdictions.

The establishment of a well thought out, written plan is absolutely necessary for a local prosecutor's office. One of the first things we are going to have to do is to determine who within the office is going to be involved. Certainly, a supervisor should be appointed head of any of this type of cybercrime prosecution. Of course, if you already have a division that is allocated to doing cybercrime prosecutions, this would be unnecessarily duplicative work and you would just want to re-educate your current staff with regard to transborder issues. However, in most cases, as I suspect, this will be a new section. The supervisor will then want to help pick at least one or two assistants who would be able to help, even if it is only on a part-time basis. Most likely, the supervisor will want to pick assistants with some experience in the computer crime area (i.e. kiddie porn or people who have dealt with computer forensic analysis). It is also suggested that the supervisor include any investigators that may be particularly involved with the new jurisdiction. If you are not lucky enough to have a computer crime investigator within your jurisdiction, then determine who is going to interact with those with the expertise. This is not only good to facilitate the actual investigations but having investigators on board and involved would be a great source of technical information when going through these prosecutions.

It is important that the supervisor give clear guidelines as to the time that those assistants will be able to allocate to these types of prosecutions. In the beginning, it is anticipated that prosecutors will be doing this on a part-time basis because the workload will not dictate any full-time loads in all but the biggest cities. Thus, the assistant should be given a clear understanding of how much time he is to spend investigating and prosecuting these cases, or even with regard to educating him or herself. Please remember that the amount of time allocated will determine largely whether or not the efforts will be proactive or reactive.[184]

It's important to assess the current abilities of the staff devoted to this area. To some extent, it might even be helpful to bring in an outside consultant or other experienced prosecutor with regard to these cases. A clear example of when that would be necessary is when the person in charge admittedly does not have enough knowledge to assess the current

183. *See e.g.* New York Electronic Crimes Task Force <http://www.ectaskforce.org/> (assessed Sept. 2002); Pittsburgh High Technology Crimes Task Force <http://www.cyber-response.org> (assessed Sept. 2002).

184. If given enough time, the prosecutors office may become proactive in that it can go help and educate the community and local police officers as to what may be necessary with regard to transborder evidence gathering and prosecution. Without adequate time, the prosecutors likely will be "putting out fires" more than they will be actively seeking to assist in investigations.

situation. The main thing to look at, of course, is education with regard to the legal and technical issues dealing with cybercrime prosecutions on a transnational basis. This would include not only the basics of cybercrime prosecutions in a domestic arena, but also at least familiarity with the international issues. If lacking in any way, education should be an immediate and first priority with regard to prosecutors.

Once you have determined your personnel and assessed their abilities, it is important to determine the actual nuts and bolts procedures for dealing with these issues. While you are going to want to have more than one assistant dealing with and having a background with different issues, it is important to assign a primary responsibility to certain areas. For example, one assistant will most likely be designated to deal with the Office of International Affairs with regard to putting in actual requests through diplomatic channels. Another will probably be responsible for dealing with legal requirements under domestic and international wiretap laws with regard to acquisition of digital evidence. But, it is also necessary to determine what actions will require supervisor approval, and who will make the final decisions with regard to what cases likely will be prosecuted. It is absolutely important to determine guidelines as to the cash value of cases in determining what you will prosecute. When determining what cases to devote resources to, the investigators and prosecutors will have to know whether or not the particular case they are working on will be something that the local office is devoted to prosecuting.[185]

E. Execution of the Plan

It is important that you form informal relationships. (*See* Interpol.) It is also important that you designate point persons for the particular agencies with those informal relationships. Therefore, these individuals will be able to gain inroads and familiarity with the personnel involved.

As part of this strategy, the local prosecutors must develop protocols for the acquisition and use of cybercrime evidence. For instance, if there are no funds to bring in a custodian of records or a witness from abroad, then the prosecutor must incorporate this reality into his strategy and limit his investigations accordingly. It is a sad fact that sometimes crimes will not be prosecuted due to a lack of resources. But for this reason, it may be advisable to explore the possibility of combining resources across local jurisdictions to adequately address cybercrime.

185. For example, a prosecutor is not going to devote a significant amount of time investigating locally a case that will hinge on acquisition of evidence from a third world country which a local prosecutor is not devoted to prosecuting or obtaining evidence from. Limited resources are a uniform concept throughout all local prosecutors' offices. Having guidelines for prosecution will assist in allocation of those resources.

Finally, there must be some method established with regard to information sharing. Hopefully, this will be considered by the Office of Homeland Defense.

CONCLUSION

The acquisition of digital evidence across national boundaries will be challenging for some time to come. International cooperative efforts among law enforcement personnel will be an essential component of any strategy designed to deal with this problem. Even if this is achieved, however, local prosecutors will continue face great challenges in this arena. Without adequate planning, execution and endorsement, the local prosecutor will stand very little chance of efficiently prosecuting cases involving transborder issues.