

International Cooperation in On-Line Identity Theft Investigations: A Hopeful Future but a Frustrating Present

Michael J. Elston* and Scott A. Stein**

I. Identity Theft - A Growing Problem

In a simpler time, our identities were relatively secure. Growing up in the 1970s, our parents could go to the grocery store, and they knew the people who owned the store or worked there. They would pay for our food either with cash or a check – no need to show identification, because the people at the store knew who you were. Then it was your good name that mattered; today, it is only whether your numbers are good that matters. Your social security account number is the key to your credit history, which is, in turn, made up of numbers: credit card numbers, bank account numbers, and mortgage and car loan account numbers. When you pay for groceries now, you either have to pay with a credit card or show multiple forms of identification to pay with a check – even if the cashier knows you.

According to the Identity Theft Resource Center of the Privacy Rights Clearinghouse, an estimated 700,000 people in the United States were victims of identity theft in 2001.¹ The city of Los

* Assistant United States Attorney, Cybercrime Unit, and Co-Chief of the Criminal Appellate Section, Office of the United States Attorney for the Eastern District of Virginia.

** Assistant United States Attorney, Cybercrime Unit, Office of the United States Attorney for the Eastern District of Virginia. The views expressed are solely the opinions of the authors and do not in any way represent the views of the United States Attorney, the Department of Justice, or any other entity.

¹ See www.idtheftcenter.org. The Identity Theft Resource Center is affiliated with Privacy Rights Clearinghouse (PRC), a nonprofit program concerned with privacy issues founded in 1992. See also J. Pollock & J. May, Authentication Technology: Identity Theft and Account Takeover, 71 FBI Law Enforcement Bulletin 1 (June 2002) (estimating that identity theft affects 900,000 new victims each year); J. Ott, Identity Theft: A Fast Growing Crime, 69 FBI Law Enforcement Bulletin 8 (August 2000) (estimating that identity theft affects 350,000 to 500,000 victims each year). More conservative estimates suggest that there are approximately 2000 new cases of identity theft each week, or more than 100,000

Angeles alone has approximately 4000 cases annually.² These are big numbers, and a substantial amount of money is at stake. One estimate puts the annual loss at more than \$2 billion.³

There is no doubt that the problem is getting worse, not better. In March 2002, the General Accounting Office released a report on identity theft in response to a request from the Senate Subcommittee on Technology, Terrorism and Government Information.⁴ Despite substantial barriers to quantitative analysis, the report concluded that “the prevalence and cost of identity theft seem to be

⁵ For example, consumer inquiries to national consumer reporting agencies regarding identity theft increased 84 percent from 1998 to 2000.⁶ One agency had approximately 89,000 consumer files with fraud alerts resulting from identity theft in 2000 – up from approximately 27,800 in 1995.⁷ The Federal Trade Commission received approximately 94,100 identity-theft complaints from November 1999 through September 2001, and almost half of those complaints were from five states: California, Florida, Illinois, New York and Texas.⁸ The Social Security Administration reported 65,220 cases of misuse of social security account numbers in fiscal year 2001 – up from just 11,058 in fiscal

cases each year. L. LoPucki, *Human Identification Theory and the Identity Theft Problem*, 80 *Tex. L. Rev.* 89 (2001). *See also* S. Hoar, *Identity Theft: The Crime of the New Millennium*, 80 *Or. L. Rev.* 1423 (2001) (noting that 42% of the 204,000 consumer fraud complaints entered into the Federal Trade Commission’s Consumer Sentinel database related to identity theft).

² S. Wexler, *Nation’s Fastest Growing Crime: Identity Theft*, 29 *Law Enforcement Tech.* 28 (Apr. 2002).

³ L. LoPucki, *Human Identification Theory and the Identity Theft Problem*, 80 *Tex. L. Rev.* 89 (2001).

⁴ U.S. Gen. Accounting Office, *Identity Theft: Prevalence and Cost Appear to Be Growing*, Report No. GAO-02-363 (March 1, 2002) (hereinafter, “GAO

⁵ GAO Report at 2.

⁶ GAO Report at 21.

⁷ GAO Report at 23.

year 1998.⁹ Of the nearly 26,000 identity theft calls to the Social Security Administration's fraud hotline from March to September 2001, 9,488 – or 36.5% – dealt with credit cards.¹⁰

With respect to the money involved, the GAO obtained loss figures from Visa and MasterCard, which represent approximately 75% of the general purpose credit card market.¹¹ In 2000, their direct identity theft losses totaled \$114.3 million, more than double the 1996 figure of \$33.1 million.¹² This, of course, is not the only cost imposed by identity theft. Credit reporting agencies, credit card companies, banks and other financial institutions are spending substantial sums on loss prevention and fraud investigation. For example, all eleven responding super-regional or money center banks responding to a survey of the American Banking Association said they spent more than a half million dollars in 1999 on preventing, detecting, investigating and prosecuting check fraud; four of the responding banks spent \$10 million or more.¹³

II. The Internet and Identity Theft

The Internet has vastly expanded the opportunities for and methods of committing identity theft and related crimes. Computer technology in general, and the Internet in particular, have brought about so many changes that have improved our lives and generated substantial growth in productivity and in prosperity.

At the same time, however, technology has opened up new avenues for criminals to obtain money and property that belong to hard-working members of society. By operating in the relative privacy of cyberspace, criminals – as long as they have the right numbers or combinations of numbers – can gain

⁸ GAO Report at 26.

⁹ GAO Report at 29.

¹⁰ GAO Report at 30.

¹¹ GAO Report at 44.

¹² GAO Report at 43.

¹³ GAO Report at 47.

access to your money or charge their new high-definition big-screen television to your credit card. The criminal is not anywhere near the scene of the crime. Identity theft based on fraudulent paper documents, such as social security cards, of course remains a problem.¹⁴ In Virginia, we learned how easy it was to obtain false identification using fraudulent documents after the September 11, 2001 terrorist attacks on the United States. To our dismay, several of the hijackers had used fraudulent documents to obtain Virginia driver's licenses, which were then easier to obtain because of a loophole that allowed proof of identity and residence with an affidavit rather than an official document.¹⁵ The loophole is now closed.¹⁶ In the United States, a state-issued driver's license is an invaluable piece of identification. It is the single-most useful ID card, even preferred at federal and state government offices over the authors' Department of Justice credentials. Virginia has taken steps to tighten the list of identification documents that may be used to obtain drivers' licences, and rightly so. Technology can undoubtedly enhance the detection and prevention of identity fraud, but that is a subject beyond the scope of this paper.

Simply put, technology makes simple identity theft easier and makes large-scale identity theft possible. As Deputy Assistant Attorney General Bruce Swartz explained to Congress in 2001:

A January 2001 study by Meridien Research . . . reports that with the continuing growth of e-commerce, payment-card fraud on the Internet will increase worldwide from \$1.6 billion in 2000 to \$15.5 billion by 2005. The Securities and Exchange Commission staff reports that it receives 200 to 300 online complaints a day about Internet-related securities fraud. Foreign law enforcement authorities also regard Internet fraud as a

¹⁴ See, e.g., P. Legall, "Tampered Vehicle ID Numbers Led to Car-Theft Ring," Hamilton (Ontario) Spectator, Aug. 14, 2002, p. A8 (noting that storage locker of car-theft ring leaders contained 123 car keys, more than 100 pieces of stolen personal identification documents, computers filled with bank information, Ministry of Transportation documents, almost \$70,000 in Canadian and American money, and \$3,280 of counterfeit money).

¹⁵ B. Masters, "Man Sentenced to Time Served for ID Fraud," Wash. Post, May 18, 2002, p.A14.

¹⁶ DMV Tightens Requirements for Identification Documents, Virginia Department of Motor Vehicles News Release (December 10, 2001) (available on the Internet at <http://www.dmvnow.com/webdoc/general/news/news.asp?id=1261>).

growing problem. Earlier this year, the European Commission reported that in 2000, payment-card fraud in the European Union rose by 50 percent to \$553 million in fraudulent transactions, and noted that the fraud was increasing most in relation to remote payment transactions, especially on the Internet. Similarly, the International Chamber of Commerce's Commercial Crime Service reported that nearly two-thirds of all cases it handled in 2000 involved on-line fraud.¹⁷

There is a widespread belief that transactions conducted on-line are more susceptible to identity theft than face-to-face transactions. There are even companies offering identity-theft protection services on the Internet.¹⁸ Indeed, this fear is now a part of the popular culture. Visa in 2002 began marketing a credit card with a security code through commercials starring Dallas Cowboys football star Emmitt Smith. Visa asks whether we are sure that it is really us who are shopping on-line as a series of men and women, young and old, black, white, and Asian, declare straight-faced to the camera, "I am these concerns, e-commerce is growing exponentially. It is estimated that consumers spent \$10.8 billion on-line during the 2000 holiday season.¹⁹ Fifteen years ago, no one was selling products on-line; today, every major retailer has an extensive website. Thirty years ago, very little personal information was stored on computers; now almost all of our personal data is stored on computers. This is fertile ground for would-be identity thieves.

A few recent cases prosecuted in the Eastern District of Virginia provide a glimpse into the ease with which identity theft can occur – often without the knowledge of the person whose identity was stolen.

¹⁷ Statement of Mr. Bruce Swartz, Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice, before that Subcommittee on Commerce, Trade and Consumer Protection of the Committee on Energy and Commerce of the U.S. House of Representatives (May 23, 2001) (quoted in GAO Report at 52).

¹⁸ M. Martin, Insurance: The cost to protect you identity is sometimes excessive, 56 Kiplinger's Personal Finance 104 (Nov. 2002).

¹⁹ GAO Report at 53.

The defendant in *United States v. Kimble*²⁰ was a captain in the United States Army assigned to the recruiting command. Instead of sticking to a budget and paying his own debts, Captain Kimble stole the names, Social Security account numbers, and birth dates of six other people, including a soldier serving under Kimble's command and civilians who came to his recruiting station to get information about enlisting in the Army. Kimble then used their identifiers to obtain credit cards over the Internet, using the same commercial mail drop in Woodbridge, Virginia, for all of the new credit card accounts. Kimble then transferred almost \$47,000 of his personal debts to those cards. Kimble was only caught when one of the victims discovered an account on his credit report and traced the source of the problem to the military and his visit to Kimble's recruiting station. The United States Attorney noted in a statement that "the credit histories of those whose identities were used 'reflect credit cards they never authorized and debts that were not their own.'"²¹ In other words, the crime had real victims with credit history problems that were not of their own making and that they will likely spend months, if not years, trying to correct.

In *United States v. Tatum*,²² the government prosecuted a travel agent who used stolen credit card numbers to buy airline tickets for some of her customers (from whom she pocketed the cash), friends, family and herself – including a trip to Jamaica. Her travel agency and the airlines were stuck with the bill. When her access to the reservation system was cut off, she signed up with an on-line travel agency based in Florida and started all over again. She bought more tickets, some with the same credit card numbers she had used before, further damaging the credit histories of the individual victims.

In both the *Tatum* and *Kimble* cases, the defendants face prison time due to the substantial penalties for identity theft prescribed by Congress. Fifteen years ago, it is likely that neither defendant

²⁰ *United States v. Michael F. Kimble, Sr.*, No. 02-CR-549-A (E.D. Va.).

²¹ T. Jackman, Army Recruiter Guilty in Identity Theft: Credit Cards Obtained in Victims' Names Used to Charge Nearly \$47,000 in Debt, Wash. Post, October 22, 2002, at B3.

²² *United States v. Regina Tatum*, No. 02-CR-446-A (E.D. Va.).

would have spent a night in jail.

III. Efforts in the United States to Combat Identity Theft

In 1998, Congress passed the Identity Theft and Assumption Deterrence Act, making identity theft – the unauthorized transfer or use of any means of identification with the intent to commit a crime – a separate crime punishable by up to 15 years of imprisonment.²³ Upon signing the bill into law, then-President Clinton stated as follows:

Tens of thousands of Americans have been victims of identity theft. Imposters often run up huge debts, file for bankruptcy, and commit serious crimes. It can take years for victims of identity theft to restore their credit ratings and their reputations. This legislation will enable the United States Secret Service, the Federal Bureau of Investigation, and other law enforcement agencies to combat this type of crime, which can financially devastate its victims.²⁴

The new law amended 18 U.S.C. § 1028 to make the unlawful transfer or use of identity information a crime equivalent to fraud in relation to identification documents. Additionally, the statute clearly recognized as victims of the crime the individuals whose identities are stolen – not just the banks and credit card companies who bear the direct financial loss.

The original version of Section 1028, which was signed into law by President Ronald Reagan in 1982, made fraud in connection with identification *documents* a crime.²⁵ A major purpose of Section 1028 was to criminalize offenses involving identification documents used “to support the creation of a new identity” that often facilitates “drug trafficking, alien smuggling, credit card fraud, and unlawful flight from

²⁶ Between 1982 and 1998, of course, identity theft – like the rest of the world – went on-

²³ The Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, 112 Stat. 3007.

²⁴ Statement by President Clinton upon Signing H.R. 4151, U.S.C.C.A.N. 709 (Oct. 30, 1998).

²⁵ False Identification Crime Control Act of 1982, Pub. L. No. 97-398, 96 Stat 2009.

²⁶ H.R. Conf. Rep. No. 97-975 (1982) (quoted in S. Rep. 105-274, at 5 (1998)).

The 1998 Act also directed the United States Sentencing Commission “to consider certain factors when establishing penalties for section 1028 offenses,” including “the number of victims and the number of means of identification, identification or false identification documents involved in the offense” and the “harm to reputation, inconvenience, and other difficulties resulting from the offense, is an adequate measure for establishing penalties.”³⁰ Clearly, Congress thought the sentencing guidelines needed to treat defendants convicted of identity theft more harshly. Thus, under the current applicable sentencing guidelines for identity theft, a first time offender with no monetary loss to the victim generally will be sentenced to some imprisonment.

The individual states have also acted to criminalize and punish identity theft. In 1998, only a few states had specific laws against identity theft. Today, a majority of states have such laws.³¹

In 2002, bills were introduced in both the House of Representatives and the Senate to establish increased penalties for aggravated identity theft.³² Both bills would provide for increased penalties when

²⁷ S. Rep. 105-274, at 5 (1998).

²⁸ S. Rep. 105-274, at 5 (1998).

²⁹ S. Rep. 105-274, at 5 (1998).

³⁰ S. Rep. 105-274, at 11 (1998).

³¹ GAO Report at 11.

³² H.R. 5588, 107th Cong., 2d Sess. (introduced Oct. 9, 2002); S. 2541, 107th Cong., 2d Sess.

identity theft is committed in connection with numerous other felonies, including immigration offenses, mail fraud, bank fraud, and wire fraud. Specifically, such aggravated identity theft would result in a sentence of up to two years of imprisonment (five years in cases where the predicate felony is a terrorism offense) on top of any sentence imposed for any other offense. The bills, in addition to requiring a consecutive sentence, would prohibit courts from reducing the sentence for the predicate felony to compensate for the aggravated identity theft penalty.³³

As of November 1, 2002, the bills were both in committee. The Senate Judiciary Committee's subcommittee on technology, terrorism and government information held a hearing on the Senate bill in July 2002, while the House bill has been referred to the House Judiciary Committee. A lame duck session of the 107th Congress is expected after the November 5 election, but it appears unlikely that either bill will become law this year. All of these legislative efforts bear witness to the fact that identity theft is a growing problem and a major concern to the American people.

Law enforcement efforts to combat identity theft, however, virtually stop at the border. As a result, international identity theft is a source of real concern. In 1998, the U.S. Postal Inspection Service and the U.S. Secret Service reported to Congress that "their investigations indicate that increasingly criminals involved with identity theft are part of international criminal syndicates committing financial, drug-related, immigration and violent crimes."³⁴ After September 11, 2001, "terrorism" can be added to that list.

In the Eastern District of Virginia, we are seeing some patterns. There are individuals and groups engaged in the large-scale trafficking of the personal identifiers that facilitate identity theft. In one case, for example, we found e-mail message after e-mail message with lists of names, addresses, birth dates and social security numbers. An analysis of the IP addresses gaining access to the e-mail account indicated that

(introduced May 22, 2002).

³³ *See, e.g.*, H.R. 5588 § 2(a).

³⁴ S. Rep. 105-274, at 7 (1998).

it was being accessed from both inside and outside of the United States.

We are also seeing on-line purchases made with stolen credit cards. When the IP address is traced, the source is outside of the United States and often in Africa. The merchandise purchased is shipped to a “drop site” in the United States where a relative or associate repackages the items and ships them to the foreign purchaser. When the authorities check out the drop site, the relative or associate – the only potential defendant in the United States – has the defense of plausible deniability. Finding and prosecuting the foreign conspirators is difficult and consumes substantially more law enforcement and prosecutorial resources.

In Internet chat rooms, we are seeing something even more disturbing. Identity thieves can request credit card numbers with a push of a button. An automated process then generates a name, a credit card number, an address and an expiration date – that are valid. The thief then goes shopping more easily than if he had stolen the credit card from your wallet or purse.

Media reports similarly suggest that international identity theft is a multi-billion dollar business and a major law enforcement problem.³⁵ Unfortunately, successful transnational prosecutions of identity theft are rare.

IV. Barriers to Effective International Cooperation

In the authors’ experience, international cooperation in identity theft cases is hampered by numerous factors, only a few of which are addressed in this paper. First, any single incident of identity theft is not likely to result in sufficient loss to the victim to justify a cross-border investigation of the crime.³⁶ Law enforcement resources are limited, and tough decisions about the allocation of those resources have to be

³⁵ Identity Theft is Rife in Russia, Wired.com, <http://www.wired.com/news/business/0,1367,54427,00.html> (Aug. 19, 2002).

³⁶ See M. Sabol, The Identity Theft and Assumption Deterrence Act of 1998: Do Individual Victims Finally Get Their Day in Court?, 11 Loy. Consumer L. Rev. 165, 168 (1999) (noting that some law enforcement agencies do not prosecute cases with less than a \$50,000 loss).

made. The resources necessary to investigate and prosecute an international identity theft are substantially greater than the resources necessary to investigate and prosecute a domestic identity theft.

Second, technology makes it easy to appear to be someone you are not – spoofing e-mail, IP addresses, etc. – or to appear to be several different (or several hundred different) people. Accordingly, it is difficult to discern a pattern of activity by an individual or group of individuals engaged in large-scale identity theft using the Internet.

Third, the evidence in on-line identity cases is ephemeral. Internet protocol (IP) addresses, connection logs, e-mail – all of it is simply digital bits and bytes in cyberspace. When you hit the delete button, it is gone. Most Internet service providers (ISPs) have data retention schedules, but they vary widely. And, depending on the information needed, it can be gone in days. *Dilaciones semper exhorret*³⁷ and “justice delayed is justice”³⁸ These adages have only gained in relevance over time.

In cyberspace, where only “real time” counts, an investigation delayed is often an investigation failed, and justice is frustrated.

Fourth, and most importantly, there are systemic, legal barriers to effective international law enforcement cooperation on Internet identity theft investigations. These are the most important factors because they are, theoretically, within the control of law-abiding citizens of the United States and the other democracies of the world, and thus we can do something about them. Moreover, making changes that enhance international cooperation between law enforcement agencies can decrease the impact of the other factors.

Before addressing three specific legal barriers to effective international cooperation in identity theft cases, we want to emphasize that in many individual cases with certain countries, law enforcement cooperation is *outstanding* and remarkably fast. Dedicated and talented law enforcement officers exist

³⁷ The law abhors delay.

in every country, and they all share the same goal: catch the crooks and gather sufficient evidence to lock them up for a while. This is particularly true when a U.S. law enforcement officer (such as an FBI or Customs Service agent) stationed in the U.S. Embassy (a legal attache or “legat”) is involved in the case. The legat’s contacts can be invaluable in emergency situations. In the average on-line fraud case, however, it simply is not feasible to complete the cumbersome process for obtaining evidence expeditiously.

A. Requests for Mutual Legal Assistance³⁹

The standard method for obtaining evidence from a foreign jurisdiction is prescribed by the terms of the relevant mutual legal assistance treaty (MLAT) between the United States and the foreign country. Such treaties impose reciprocal obligations on the parties. The treaties generally provide that requested “assistance will be provided directly between the U.S. Justice Department and its foreign prosecutorial counterpart outside the normal diplomatic channels and with minimal judicial involvement.”⁴⁰ Although the treaties recognize the need for relatively swift action on requests, this process was not designed with the Internet Age in mind.

Typically, a prosecutor involved in the investigation drafts a request for mutual legal assistance, outlining the assistance needed. In on-line identity theft investigations, assistance is usually needed in obtaining some form of computer evidence, such as a suspect’s computer or the records of a foreign ISP. The request is submitted to the national justice ministry (in the United States, the Department of Justice), which may or may not make changes or ask for more information from the prosecutor before forwarding it to the ministry’s counterpart in the other country. Once received, the justice ministry in the receiving

³⁸ *Jones v. Clinton*, 72 F.3d 1354, 1363 (8th Cir. 1996) (Beam, J., concurring).

³⁹ Where no Mutual Legal Assistance Treaty exists between the nations involved, evidence can be obtained through letters rogatory. The same issues that arise in the context of MLAT requests arise in that context as well.

⁴⁰ J. Knapp, *Mutual Legal Assistance Treaties as a Way to Pierce Bank Secrecy*, 20 Case Western J. Int’l L. 405, 406-07 (1988).

country generally refers the request to a local prosecutor to do what is necessary to obtain the requested evidence in a form that will be admissible in the requesting country.

For requests directed to the United States, this process is spelled out in federal law.⁴¹ Congress's stated purpose for enacting the statute was ". . . to improve the United States judicial procedures for . . . obtaining evidence in the United States in connection with proceedings before foreign and international tribunals"⁴² In essence, the law authorizes a federal court to appoint a commissioner for the purpose of obtaining evidence in accordance with the request for mutual legal assistance. The reception of letters of request and the appointment of a commissioner to execute them are matters customarily handled *ex parte*, and persons with objections to the request raise those objections by moving to quash any subpoenas issued by the commissioner.⁴³ The commissioner has the authority to issue a subpoena for a deposition or for documents and other records.⁴⁴

The problem with MLAT requests is not in the concept but in the practice. The process is simply too slow and cumbersome to be useful, by itself, in obtaining electronic evidence. The authors have made MLAT requests to other countries and have served as commissioners on behalf of foreign countries such as Germany, Switzerland and the United Kingdom where the electronic evidence sought included ISP records, connection logs, and e-mail messages. With respect to the requests received from other countries, they are often too late or incomplete or both.

For example, we regularly receive requests seeking basic subscriber information for the subscriber assigned to a specific IP address. Many of these requests are received three or four months after the original request is dated, which was already several months after the incident being investigated.

⁴¹ 28 U.S.C. § 1782.

⁴² S. Rep. No. 88-1580, 1964 U.S.C.C.A.N. 3782.

⁴³ *In Re Letters Rogatory from Tokyo District, Tokyo*, 539 F.2d 1216, 1219 (9th Cir. 1976).

⁴⁴ 28 U.S.C. § 1782.

Transmission from investigator to prosecutor to ministry of justice to the U.S. Department of Justice to prosecutor takes a long time, and everyone involved usually writes a cover letter reiterating what is in the original request. If the request has to be translated into English, it is delayed even longer. Once the request is received, it often turns out to be incomplete. For example, one recent request did not include specific dates and times for the IP addresses. The ISPs to whom the request was directed do not provide their subscribers with a fixed IP address. Instead, a different IP address could be assigned to the subscriber every time he or she dialed in to the ISPs network (dynamic IP addresses). As a result, nothing could be done with the request. The information provided was insufficient to form even the basis of a section 2703(f) preservation letter.⁴⁵ The Office of International Affairs at the U.S. Department of Justice was notified of the problem immediately, but more than a month passed without any additional information being provided by the authorities in the requesting jurisdiction. All the while, the ephemeral data being sought was disappearing as the ISPs systematically deleted old data.

B. The Electronic Communications Privacy Act

A further barrier to effective international cooperation in on-line identity theft investigations is the Electronic Communications Privacy Act (ECPA).⁴⁶ Enacted in 1986,⁴⁷ ECPA was a rare example of Congress legislating *ahead of* technology. While there are many notable, important, and effective aspects to ECPA (which has been amended on numerous occasions since 1986), the section governing law enforcement efforts to obtain electronic communications and records from ISPs is a significant barrier to foreign investigations involving ISPs located in the United States – even when the ISP subscriber is not

⁴⁵ Pursuant to 18 U.S.C. § 2703(f), a governmental entity can send a letter to an ISP requiring them to preserve records for 90 days pending issuance of a court order or other process.

⁴⁶ 18 U.S.C. § 2701 *et seq.* The appendix is a chart showing the intricacies of evidence collection under ECPA as amended by the USA PATRIOT Act.

⁴⁷ Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (Oct. 21, 1986).

located in the United States.

In a traditional criminal investigation, law enforcement officers gather evidence about a crime in a variety of ways, often working covertly to avoid alerting a suspect to the investigation. If a third party has relevant documents but refuses to turn them over voluntarily, the government can compel production of the records with a grand jury subpoena. Even medical and banking records must be produced in response to a grand jury subpoena.

In an investigation involving Internet crime, however, the rules are different. The only thing a subpoena will get a grand jury is the basic subscriber information (name, address, length and type of service, subscriber number or identity), connection records and session times and durations, and billing records.⁴⁸

If an investigator wants e-mail messages (“stored electronic communications”), the method used to obtain them depends on whether the communications have been retrieved and, if unretrieved, how long the messages have been in electronic storage. If the e-mail message has been retrieved, or if it has not been retrieved but stored for more than 180 days, it can be obtained with a search warrant, a court order, or a subpoena issued with notice to the subscriber.⁴⁹ Notice, however, can be delayed for up to 90 days by court order or “upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may” result in endangerment of the life or physical safety of a person, the flight of the suspect, destruction of evidence, intimidation of witnesses, or some other serious harm to an investigation or undue delay of a trial.⁵⁰

If an e-mail message has not been retrieved and has been in electronic storage for less than 180

⁴⁸ 18 U.S.C. § 2703(c).

⁴⁹ 18 U.S.C. § 2703(b).

⁵⁰ 18 U.S.C. § 2705.

days, the only way to obtain it is to get a search warrant.⁵¹ Thus, as a practical matter, law enforcement officers generally have to obtain search warrants. Assuming the suspect deletes his incoming and outgoing e-mail messages on a regular basis, the only helpful information is going to be in new, unretrieved e-mail messages. The standard for obtaining a search warrant requires the law enforcement officer to show that there is probable cause to believe that a crime has been committed and that evidence of the crime will be found in the e-mail account. This is a fairly high standard that can rarely be met in the beginning stages of a domestic investigation and is even harder to meet in the early stage of an international investigation. Moreover, most foreign investigators are unaware of ECPA's requirements, and they rarely provide sufficient information in their MLAT request to support a search warrant application. Thus, there is even further delay, and ephemeral evidence is lost with each passing day.

The ECPA requirements regarding stored wire and electronic communications are often viewed with incredulity by our foreign counterparts because they are based on a peculiarly American view of privacy. First, they suggest that Americans value the privacy of their e-mail messages more than their bank records and medical histories. This may be true for some people, but not for most. Second, and most importantly, they reflect a misperception that the greatest threat to on-line personal privacy is from the government. As the statistics quoted above demonstrate, the greatest threat to the privacy of Americans (particularly, American consumers) are criminals, followed closely by marketing research firms.⁵² Frankly, the government has too many real criminals too worry about. Speaking for the two of us, we simply have better things to do than to try and read the e-mail messages of law-abiding citizens.

C. Limitations on Extradition

Finally, assuming these barriers are overcome, many countries will not extradite a person unless

⁵¹ 18 U.S.C. § 2703(a) & (b).

⁵² See, e.g., E. Williams, "The Man Who Knows Too Much: The Math Whizzes at Fair, Issac Know What You Bought - And What You're Likely To Buy Next," 170 Forbes 68 (Nov. 11, 2002).

there is dual criminality. Dual criminality means that the conduct is criminal in both the sending and receiving jurisdictions. Unfortunately, with identity theft, the United States is on the cutting edge, and what is criminal here is not criminal in many other countries. As a result, many international investigations end without the prosecution and punishment of the responsible criminals.

V. Solutions on the Horizon? The Council of Europe Convention on Cybercrime

The Department of Justice has been working on many fronts to address global threats posed by international cybercrime. This includes participation in the negotiation and drafting of the Council of Europe Cybercrime Convention,⁵³ which is the first multilateral treaty to address the problems posed by the spread of criminal activity in cyberspace. The United States has signed the convention, but it has not been ratified by the Senate. The convention requires parties (1) to establish laws against cybercrime, (2) to ensure that their law enforcement officials have the necessary authority to investigate and prosecute cybercrime offenses, and (3) to provide international cooperation to others in the fight against cybercrime. The ISRCL Conference is fortunate to have Christopher Painter on its faculty, as he is one of the foremost U.S. experts on the Cybercrime Convention. Accordingly, we will limit our comments to a brief discussion of the promise of the convention in the area of investigation of international identity theft crimes.

According to the Department of Justice website, the United States government believes that “the vast bulk of the obligations and powers contemplated by the draft Convention are already provided for under United States law,” but “the Convention makes progress in this area by (1) requiring signatory countries to establish certain substantive offenses in the area of computer crime, (2) requiring parties to adopt domestic procedural laws to investigate computer crimes, and (3) providing a solid basis for

⁵³ The Convention on Cybercrime signed at Budapest, Hungary, on November 23, 2001 (hereinafter, “Cybercrime Convention”) (available on the Internet at <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>).

international law enforcement cooperation in combating crime committed through computer systems.”⁵⁴

Unfortunately, the crime of on-line identity theft is not among the crimes that signatories must criminalize. There are, however, many related crimes that are covered by the convention. These include illegal access to computers,⁵⁵ illegally accessing computer data,⁵⁶ and computer-related fraud.⁵⁷ While the principle of dual criminality may still prevent the full enforcement of U.S. identity theft laws by hampering extradition, the convention recognizes that the dual-criminality requirement should not be a barrier to mutual legal assistance as long as “the conduct underlying the offence for which assistance is sought” by the requesting party is criminal under the laws of the requested party.⁵⁸

One of the most important provisions of the convention from the perspective of law enforcement is Article 16, entitled “Expedited preservation of stored computer data.” Article 16 requires signatories to “adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system . . . for a period of time as long as necessary, up to a maximum of 90 days, to enable the competent authorities to seek its disclosure.”⁵⁹ The preservation provision of ECPA is remarkably similar to Article 16 of the Cybercrime Convention, and thus United States law is already consistent with Article 16.

Article 17 requires signatories to “ensure the expeditious disclosure to the Party’s competent

⁵⁴ See U.S. Department of Justice, Frequently Asked Questions About the Council of Europe Convention on Cybercrime, Question A4 (Jul. 10, 2001) (available on the Internet at <http://www.usdoj.gov/criminal/cybercrime/newCOEFAQs.html#Q4>).

⁵⁵ Cybercrime Convention, art. 2.

⁵⁶ Cybercrime Convention, art. 3.

⁵⁷ Cybercrime Convention, art. 8.

⁵⁸ Cybercrime Convention, art. 25(5).

⁵⁹ Cybercrime Convention, art. 16(1) & (2).

authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.”⁶⁰ Articles 18, 19, 20 and 21 address production orders, search and seizure of stored computer data, real-time collection of computer data, and interception of content data. All of these provisions are broadly consistent with United States law. The standardization of the legal regimes of so many countries will undoubtedly enhance international cooperation in on-line identity theft investigations.

The real promise of the Cybercrime Convention, however, lies in its procedural innovations. For example, Article 25 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.”⁶¹ The “requested Party” may respond in a like manner. This will undoubtedly speed up future MLAT requests and responses.

When an investigation involves two signatory countries that do not have a legal assistance treaty, Article 27 provides MLAT-like procedures to facilitate cooperation. These procedures include the following dealing with expedited requests:

- a. In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.
- b. Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).⁶²

⁶⁰ Cybercrime Convention, art. 17(1)(b).

⁶¹ Cybercrime Convention, art. 25(3).

⁶² Cybercrime Convention, art. 27(9).

This procedure would, of course, vastly improve the speed at which MLAT requests get into the hands of the officials who actually obtain the requested information. Unfortunately, the Convention includes an opt-out provision on this procedure: “Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.”⁶³

Article 35 requires each signatory to “designate a point of contact available on a 24 hour, 7 day per week basis in order to ensure the provision of immediate assistance 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.”⁶⁴ The “point of contact” must be prepared to provide technical advice, effect the preservation of data, collect evidence, give legal information, and locate suspects. This provision will be an immense help in the fight against cybercrime. It offers real hope that the data preservation regime called for by the Convention can be implemented effectively.

While these developments hold great promise for future investigations of on-line identity theft, it is unclear how much of an improvement the Cybercrime Convention offers. If it is implemented largely through its provisions for urgent matters (which it may well be, as the danger of loss of evidence is nearly always present in Internet-related investigations and preservation for 90 days will rarely be sufficient for completion of the traditional MLAT process), there is a chance that great improvements will be made. If, however, the convention is implemented primarily through existing procedures, it is unlikely that there will be any real improvement in the effort to catch international cybercriminals simply because the evidence will have disappeared before law enforcement can obtain it..

⁶³ Cybercrime Convention, art. 27(9)(e).

⁶⁴ Cybercrime Convention, art. 35(1).

VI. Conclusion

The current structure of international mutual legal assistance is simply too slow and cumbersome for the Internet Age. Electronic evidence is ephemeral, and the delay inherent in the current structure significantly lessens the chance that such evidence will be obtained and cybercriminals will be caught. On-line identity theft will continue to be lucrative and difficult to stop or to investigate. The Council of Europe Convention on Cybercrime, while not aimed directly at identity theft (a crime that can be committed off-line as well as on-line), provides some hope for future efforts to identify, track and catch international on-line identity thieves. Law enforcement officers in the United States and other countries may well have better access to electronic evidence in the near future, but the promise of the Cybercrime Convention will not be fulfilled if it is implemented largely (or exclusively) through the existing, slow, cumbersome MLAT process. The Internet Age demands a system that will put front-line prosecutors and investigators in contact with their counterparts quickly so that precious evidence is not lost due to delay.

APPENDIX
STORED WIRE & ELECTRONIC COMMUNICATIONS
QUICK REFERENCE GUIDE
(REFLECTING USA PATRIOT ACT)

Voluntary Disclosure Allowed?		Mechanisms to Compel Disclosure	
Public Provider	Non-Public Provider	Public Provider	Non-Public Provider

Basic subscriber, session & billing information†	No, unless §2702(c) exception applies [§ 2702(a)(3)]	Yes [§ 2702(a)(3)]	Subpoena; 2703(d) order; or search warrant [§ 2703(c)(2)]	Subpoena; 2703(d) order; or search warrant [§ 2703(c)(2)] [§ 2711(2)]
Other transactional and account records	No, unless §2702(c) exception applies [§ 2702(a)(3)]	Yes [§ 2702(a)(3)]	2703(d) order or search warrant [§ 2703(c)(1)]	2703(d) order or search warrant [§ 2703(c)(1)]
Retrieved communications‡ and content of other stored files	No, unless § 2702(b) exception applies [§ 2702(a)(2)]	Yes [§ 2702(a)(2) and § 2711(2)]	Subpoena with notice; 2703(d) order with notice; or search warrant [§ 2703(b)]	Subpoena; ECPA doesn't apply [§ 2711(2)]
Unretrieved communications‡ (in electronic storage more than 180 days)	No, unless § 2702(b) exception applies [§ 2702(a)(1)]	Yes [§ 2702(a)(1)]	Subpoena with notice; 2703(d) order with notice; or search warrant [§ 2703(a,b)]	Subpoena with notice; 2703(d) order with notice; or search warrant [§ 2703(a,b)]
Unretrieved communications‡ (in electronic storage 180 days or less)	No, unless § 2702(b) exception applies [§ 2702(a)(1)]	Yes [§ 2702(a)(1)]	Search warrant [§ 2703(a)]	Search warrant [§ 2703(a)]

† See 18 U.S.C. § 2703(c)(2) for listing of information covered. For telephone communications, the section includes, among other records, local and long distance connection records. For Internet connections, the section includes, among others, records of session times and durations, and IP address assigned to the user during the session.

‡ Includes the content of voice communications.

Computer Crime and Intellectual Property Section, United States Department of Justice, P.O. Box 887, Ben

Franklin Station, Washington, D.C., 20044-0887

Main (202)514-1026 Fax (202)514-6113 website www.cybercrime.gov