The Richmond Journal of Law and Technology

Volume IX, Issue 1,
Fall 2002

In Search of a Balance Between Police Power and Privacy in the Cybercrime Treaty

By D.C. Kennedy[1]

[1] Ms. Kennedy graduated from Emory University School of Law in December 2001 and is a licensed attorney in Georgia. She has served as the Atlanta bureau chief for The Internet Law Journal and has worked as a research assistant for the Center for Social and Legal Research, a non-profit organization focused on privacy issues.

Introduction

Imagine that you wake up one morning, turn on your computer, and open an e-mail message with a catchy phrase in the subject line. Immediately after opening the e-mail's attachment, your personal computer is severely damaged. Obviously having a bad day, you head to your job as an attorney for a multinational corporation. By the time you arrive at work, there has been damage to company computers across the globe. The monetary costs of the damage, coupled with the downtime, are astronomical. The CEO of your company is furious. You hope to diffuse the situation by informing your boss that the person who released the virus has been apprehended. Unfortunately, soon after explaining the good news of the perpetrator's capture, you learn that the individual, who admits involvement with the e-mail virus, will not be prosecuted in his home state because that state had no laws on the books outlawing his behavior at the time of the incident. In fact, none of the states where damage occurred will be able to prosecute because of lack of jurisdiction. The damage is done and the perpetrator is free.

Although the situation may sound far fetched, this is the basic story of the events surrounding the dissemination of the I LOVE YOU virus. The perpetrator was allowed to go free because the Philippines did not have appropriate cybercrime laws instituted at the time the virus was released.[2] This high-profile case is a superb introduction to the difficult issues arising from the existence of cyberspace.[3]

---

[2] *See* CBS News Online, *Love Bug Suspect Off the Hook, at* http://www.cbsnews.com/stories/2000/08/21/tech/main226472.shtml (Aug. 21, 2000).

[3] *See generally* Jay Krasovec, *Cyberspace: The Final Frontier, for Regulation?,* 31 AKRON L. REV. 101, 103 n.1 (1997) (defining cyberspace generically "to encompass the use of electronic communications over computer networks mainly via the Internet.").

In this "Age of the Internet,"[4] access to information is unprecedented. This access can be positively used to contact friends and businesses around the world or can be negatively used to gain unauthorized access to information or to steal profitable data. With the threat of sinister uses for access comes the need for protection – protection from attacks such as the I LOVE YOU virus[5] and protection from prying eyes.[6] Even though protection from these threats is hampered because of the international scope of the threat, this same scope assists the cybercriminal. No longer must a criminal be located physically in the proximity of his crime. Instead, through the same technology that makes the Internet such a popular personal and business instrument, the criminal is able to cause damage regardless of national borders. The ability of the cybercriminal to cross national borders without effort, coupled with the relative ease of his causing harm, present problems for states that want to crack down on cybercrime. These states must determine effective ways to investigate activity that occurs outside of their national boundaries, including investigations in states that may not outlaw the activity. In addition, the states investigating these crimes must employ individuals with the appropriate technical training who can devote long hours to tracing the electronic trails of cybercriminals.

In an effort to address the difficulties of investigating cybercriminals, the Council of Europe put forward a cybercrime treaty to harmonize definitions of cybercrime in states that

---

[4] Susan Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 SAN DIEGO L. REV. 1153 (1997) (using term from title of Gindin's article).
[5] *See generally* James Evans, *Cyber-Crime Laws Emerge, but Slowly*, IDG.net, *available at* http://www.cnn.com/2000/TECH/computing/07/05/cyber.laws.idg/ (July 5, 2000) (describing how the "I Love You" virus brought attention to the need for domestic cybercrime laws).
[6] *See* Gavin Skok, *Establishing a Legitimate Expectation of Privacy in Clickstream Data*, 6 MICH. TELECOMM. & TECH. L. REV. 61, 61 (1999/2000) (explaining that the "prying eyes" concept refers to those who track individuals' activities on the Internet).

become parties to the treaty.[7] To assist law enforcement with investigation of these crimes, the treaty provides for procedures to assist law enforcement in the search and seizure of computer data and facilitates cooperative investigations by states affected in specific cybercrime incidents.[8] The increase in police power that would result from the treaty concerns many privacy advocates.[9] The basis for this concern is the limited protection available to support privacy of information pertaining to individuals.[10]

To examine the privacy issues at stake, this paper will first explore the increase in police power granted by the treaty. The paper will follow this assessment by looking at the concerns raised by the formulation of the treaty itself. It will then end by exploring the opportunity missed by the treaty drafters to address fundamental privacy concerns. Part I will analyze the concept of cybercrime in an effort to define the evil that the treaty is intended to address. As part of this

---

[7] *Crime in Cyberspace: First Draft of International Convention Released for Public Discu*ssion, s*ee infra* note 46 (criminalizing illegal access, interception, or interference with computer systems).

[8] Juliana Gruenwald, *Europeans Defining the Long Arm of The Cyberlaw, at* http://news.zdnet.co.uk/story/0,,s2081836,00.html (Sept. 25, 2000)(on file with the Richmond Journal of Law & Technology)(noting that the treaty requires states to "provide law enforcement authorities with the ability to conduct computer searches and seize computer data"); s*ee also id.* sec. 2, art. 15 (subjecting treaty powers to conditions and safeguards as provided for under national law).

[9] *See e.g.,* LIBERATING CYBERSPACE: CIVIL LIBERTIES, HUMAN RIGHTS AND THE INTERNET 2 (Liberty ed., 1999) ("Can the requirements of law enforcement be reconciled with individuals' right to privacy?"). Note that technological possibilities that would theoretically guarantee complete personal privacy would also likely prevent law enforcement from tracing crimes related to such information. *See* Toby Lester, *The Reinvention of Privacy*, THE ATLANTIC MONTHLY, Mar. 1, 2001, at 27 (detailing a piece of software that would allow the user to conduct business on the Internet in an anonymous way, to the extent that the provider would not have the names of the user to provide if subpoenaed).

[10] *See* ALAN F. WESTIN, PRIVACY AND FREEDOM 367 (Atheneum New York 1967) (detailing privacy concerns in the Information Age); *see also* Tony Lester, *The Reinvention of Privacy*, THE ATLANTIC MONTHLY, Mar. 1, 2001, at 27 (discussing the forward looking nature of the 1967 privacy book by Westin). The argument for protection of privacy assumes that individuals have an expectation of privacy concerning personal information, but that this expectation has, for the most part, not been protected by law. *See* LIBERATING CYBERSPACE: CIVIL LIBERTIES, HUMAN RIGHTS AND THE INTERNET 6 (Liberty ed., 1999).

discussion, Part I will examine the new 'tools' available to criminals in the Internet Age and, conversely, the new dilemmas that these 'tools' create for law enforcement. Part II will discuss the recently proposed cybercrime treaty. It will examine the provisions of the first publicly-released draft, the list of complaints that flooded into the Council of Europe after the release of the draft, and the revisions that resulted from the complaints. Part III will use two hypotheticals to study the impact of the treaty. In the hypotheticals, three Southeast Asian states – with privacy protection levels spanning from low to high – will interact with a European state in a cybercrime investigation. The paper will assert that the interaction that ensues, the very interaction contemplated by the treaty, will have the potential to lower privacy protections for the states involved. Part IV will explore the concept of privacy at the international level, paying particular attention to the definitions of privacy provided by the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. It will compare the traditional international understandings of privacy – privacy of communication, freedom of expression, and criminal procedure protections – with the revolutionary change needed for the concept of privacy in the Internet Age. Part IV will end by arguing that this new conception of privacy should account for intrusions by governments, businesses, and rogue individuals. Part V will conclude by arguing that the increase in police power required by the treaty necessitates an offsetting increase in privacy protection for individuals. It will contend that the treaty should have included a privacy provision that required parties to enact, through domestic legislation, protection of informational privacy from unwanted violations by governments, businesses, or rogue individuals. In the absence of such a provision, there can only be a hope that governments will adopt such legislation on their own and that reinterpretations of international treaties will include protections for informational privacy.

I. The Problem of Cybercrime

A. Cybercrime and the Cybercriminal

In this Age of the Internet, 'cybercrime' has become a household word, but its definition is seldom explained. Books and articles written on the subject often assume that the reader understands the many facets of cybercrime. For many, however, computer hacking[11] and computer viruses[12] are the main images conveyed by the term. While these crimes comprise two important categories of cybercrime, many other crimes can be committed or facilitated utilizing computer networks. A non-exhaustive list of cybercrimes includes: fraud, forgery, counterfeiting, gambling, transmission of child pornography, transmission of threats, transmission of harassing communications, interception of communications, copyright infringement, and theft of trade secrets.[13]

The motivations of those who commit cybercrimes may be as varied as the nature of the cybercrime itself. Juveniles may be drawn by the prestige of outwitting adults.[14] Insiders may

---

[11] The term 'hacking' is somewhat confusing because people use the term to refer to different types of activities. A comprehensive definition of hacking includes numerous aspects of the term. A hacker is "[a] person who enjoys exploring the details of computers and how to stretch their capabilities." A hacker is "[a] malicious or inquisitive meddler who tries to discover information by poking around." A hacker is "[a] person who enjoys learning the details of programming systems and how to stretch their capabilities, as opposed to most users who prefer to learn on the minimum necessary." Sans Institute Resources, *NSA Glossary of Terms Used in Security and Intrusion Detection*, *at* http://www.sans.org/newlook/resources/glossary.htm (Apr. 1998).

[12] A virus is "[a] program or piece of code that is loaded onto [a] computer without [the user's] knowledge and runs against [the user's] wishes." Webopedia, *at* http://webopedia.internet.com/TERM/v/virus.html (last modified Feb. 5, 2002).

[13] David Goldstone & Betty-Ellen Shave, *International Dimensions of Crimes in Cyberspace*, 22 FORDHAM INT'L L.J. 1924, 1925 (1999); Gavin Skok, *Establishing a Legitimate Expectation of Privacy in Clickstream Data*, 6 MICH. TELECOMM. & TECH. L. REV. 61, 68 n.23 (1999/2000).

[14] In most instances, commentators distinguish juvenile cybercriminals, who are believed to be acting mischievously but not maliciously, from advanced criminals, who are expected to cause serious consequences by their actions. MODEL CODE OF CYBERCRIMES INVESTIGATIVE PROCEDURE Art. 1, § 2(c), *at* http://cybercrimes.net/MCCIP/art1.htm (2001).

be seeking retribution for a perceived wrong by a business or a former employer.[15] Hackers may simply want bragging rights associated with compromising a particular computer system.[16] Virus writers may be motivated by prestige, as well as by malicious feelings towards others.[17] Criminal groups functioning on the Internet may seek monetary gain.[18] Foreign terrorists may seek foreign intelligence.[19] Even with these various motivators, there is at least one common characteristic of the people who commit cybercrimes. Yesterday's street criminal had "street smarts"; today's cybercriminal has "computer smarts." In order to be successful at their craft, cybercriminals need to possess a knowledge of computers that is far superior to the average user's amateur skills. This knowledge allows the criminal to mask his criminal activity and to divert the efforts of law enforcement officials.[20]

B. The New Tools of the Cybercriminal

Technology provides the cybercriminal with a new bag of 'tools' that make him more effective at his craft. In this Internet Age, the 'tools' are not physical implements, but instead are advantages for those who commit cybercrime. The first such 'tool' is the ability to hide evidence pertaining to the cybercrime. The evidence is virtually hidden because of the instantaneous transfer of data through computer systems.[21] The cybercriminal has the capacity to act at one site in cyberspace and then, taking the evidence of the crime with him, to leave instantaneously. The second 'tool' is the cybercriminal's ability to hide his identity. In effect, a skilled

---

[15] *See id.*
[16] *See id.*
[17] *See id.*
[18] *See id.*
[19] *See id.*
[20] *See id.*
[21] U. Sieber, *Computer Crime and Criminal Information Law – New Trends in the International Risk and Information Society,* Section E, Criminal Procedural Law, *at* http://www.uplink.com.au/lawlibrary/Documents/Docs/Doc122.html (last visited Sept. 17, 2002) (on file with the Richmond Journal of Law & Technology).

cybercriminal is able to attack computer systems leaving few, if any, clues as to his identity. His identity is further concealed because he can easily commit the cybercrime without being physically present in a jurisdiction.[22] The third 'tool' is the cybercriminal's ability to increase his cybercriminal activity with minimal effort. The cybercriminal can ignore international boundaries[23] by simultaneously targeting multiple victims in multiple states.[24] Ultimately, these 'tools' provide the cybercriminal with an international forum for cybercrime in a world where laws criminalizing his behavior are limited to domestic borders.

C. Challenges for Law Enforcement

With each of the cybercriminal's new 'tools,' law enforcement officials face new challenges.[25] The cybercriminal's first 'tool,' his instantaneous ability to hide data in computer systems, creates a host of problems for law enforcement.[26] In domestic investigations, law enforcement officials may discover that critical data is stored on a networked computer that is located in another state. Law enforcement must then determine if their domestic court order is sufficient to search the storage facility outside the state's territory or if mutual assistance must be sought with law enforcement in the other state.[27] Even in the instance of information stored with ISPs, the procedures that law enforcement need to follow are not uniform from state to state, meaning that the task of obtaining the information may be quite time consuming.[28] If the evidence is encrypted, there is a question as to whether a witness can be compelled to provide a printout of encrypted data when questioned by law enforcement authorities or interrogated in

[22] David Goldstone & Betty-Ellen Shave, *International Dimensions of Crimes in Cyberspace*, 22 FORDHAM INT'L L.J. 1924, 1925 (1999).
[23] *See id.*
[24] *See id.*
[25] *See id.*
[26] Sieber, *supra* note 21.
[27] Goldstone & Shave, *supra* note 22, at 1937-38.
[28] *Id.* at 1937.

court. This situation becomes particularly daunting when an encryption key[29] is held by a second person who is located outside the state's territory.[30] All of these inquiries take time and may provide the cybercriminal the time frame needed to further conceal the incriminating data.

The second 'tool' to which law enforcement must respond is the cybercriminal's ability to hide his identity. By skillfully using a computer system, the cybercriminal has the ability to mask his identity or remain anonymous.[31] If the law enforcement cannot identify the cybercriminal by the clues left in cyberspace, it may be extremely difficult to track the criminal.[32] Because the cybercriminal can commit a crime without being present in a jurisdiction, the cybercrime scene has no physical boundaries[33] and leaves law enforcement with few, if any, physical leads as to the identity of the cybercriminal. Unlike the situation where a criminal's location can be approximated by the distance that he could possibly have traveled

---

[29] One of the two forms of encryption is public-key encryption. Public-key encryption is "[a] cryptographic system that uses two keys – a public key known to everyone and a private or secret key known only to the recipient of the message. When John wants to send a secure message to Jane, he uses Jane's public key to encrypt the message. Jane then uses her private key to decrypt it. An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. Moreover, it is virtually impossible to deduce the private key if you know the public key." Webopedia, *at* http://webopedia.internet.com/TERM/p/public_key_cryptography.html (last modified Oct. 29, 2001).

[30] Interview with Bill Thompson, Internet Privacy and Security Issues Expert for Special Services Group, in Atlanta, Ga. (Sept. 15, 2000); *see also* U. Sieber, *Computer Crime and Criminal Information Law – New Trends in the International Risk and Information Society*, Section E, Criminal Procedural Law, *at* http://www.uplink.com.au/lawlibrary/Documents/Docs/Doc122.html (last visited Sept. 17, 2002).

[31] The cybercriminal is able to remain anonymous not because the technology does not exist to track him, but because the resources needed to train and fund law enforcement in tracing techniques are generally not adequate. Interview with Bill Thompson, Internet Privacy and Security Issues Expert for Special Services Group, in Atlanta, Ga. (Sept. 15, 2000).

[32] David Goldstone & Betty-Ellen Shave, *International Dimensions of Crimes in Cyberspace*, 22 FORDHAM INT'L L.J. 1924, 1937 (1999); s*ee also* Nan Hunter, et al., *Contemporary Challenges to Privacy Rights*, 43 N.Y.L. SCH. L. REV. 195,198 (1999).

since the crime occurred, cybercriminals have no effective limitation on their distance from the crime scene – even a second after the crime was committed.

The cybercriminal's third 'tool,' his ability to increase criminal activity by striking multiple victims in multiple states, creates several problems. Law enforcement must first determine whether domestic criminal laws are applicable to crimes committed by utilizing international data networks.[34] If the domestic court system makes a determination that the laws are not applicable, an investigation may be inappropriate, as no domestic laws have been violated. Even if the domestic criminal law applies, jurisdictional issues must still be addressed.[35] If a perpetrator has committed crimes in more than one state, the home state must make a determination concerning extradition. In a crime involving multiple victim states, a home state that is willing to extradite the accused must decide on one state to which to send the accused. Conversely, a home state may be unable to extradite because the laws regarding cybercrimes vary substantially in the two states.[36] In the case where extradition is not possible, the home state may have the option of prosecuting the accused if jurisdiction can be established by the presence of the accused in the home state. This solution may not satisfy the victim, as the penalties for the cybercrime may be different in the home state and the victim state. In addition, the victim may not believe that the same diligence will be used in the prosecution of the accused in the home state as would be used in the victim state. The possibility also exists that the

---

[33] *See* MODEL CODE OF CYBERCRIMES INVESTIGATIVE PROCEDURE Art. VII, *at* http://cybercrimes.net/MCCIP/art7.htm (2001)(obtaining evidence - search and seizure).
[34] U. Sieber, *Computer Crime and Criminal Information Law – New Trends in the International Risk and Information Society*, Section E, Criminal Procedural Law, *at* http://www.uplink.com.au/lawlibrary/Documents/Docs/Doc122.html (last visited Sept. 17, 2002) (on file with the Richmond Journal of Law & Technology).
[35] David Goldstone & Betty-Ellen Shave, *International Dimensions of Crimes in Cyberspace*, 22 FORDHAM INT'L L.J. 1924, 1938-39 (1999).
[36] *Id.*

accused committed no crime according to the laws of the home state; thus, he would face no penalty for his activity.[37]

While the term 'cybercrime' did not exist twenty years ago, today the number of attacks is increasing and the monetary damage from the crimes is staggering. Cybercriminals are able to benefit from the use of their new 'tools,' while law enforcement is plagued with a host of new cyberproblems. To even the playing field, law enforcement officials need increased police powers to combat the new 'tools' of cybercriminals.

II. Treaty on Cybercrime

A. Draft 19: The First Publicly-Released Version of the Cybercrime Treaty[38]

Although no treaty is likely to address the full scope of the problems created by cybercriminals' new 'tools,' the treaty drafted by the Council of Europe[39] endeavors to address several of the basic problems. The Council of Europe first examined the problems associated with the international nature of cybercrimes when it drafted a 1995 paper recommending that states adopt laws regarding cybercrime.[40] Realizing the need for a legally binding instrument,

---

[37] "In addition to the formal concerns related to substantive laws and procedural laws, international computer crime investigations are hampered by a variety of operational issues." *Id.* at 1939. These concerns include: "expertise and coordination," "communication," and "timeliness." *Id.*; *see also Cybercrime Part II – Law Enforcement Challenges*, 54 Mishpat Cyberlaw Informer, *at* http://mishpat.net/cyberlaw/archive/cyberlaw54.shtml (last visited Sept. 20, 2001).

[38] In April 2000, the treaty was released to the public via the Website of the Council of Europe. Drafters of the treaty had been working on the project since May 1997. Reuters, *Cybercrime Treaty Gets a Makeover*, *available at* http://news.zdnet.co.uk/story/0,,s2082557,00.html (Nov. 14, 2000).

[39] The Council of Europe is a "41-nation human rights watchdog." *Id.*

[40] Juliana Gruenwald, *Europeans Defining the Long Arm of The Cyberlaw*, *at* http://news.zdnet.co.uk/story/0,,s2081836,00.html (Sept. 25, 2000) (on file with the Richmond Journal of Law & Technology) (describing reaction to the release of Draft 19). As noted in Part I of the paper, problems associated with the international nature of the crimes include the cooperation needed between states to adequately investigate such crimes and the hurdles created when the activity is not illegal in one of the states involved.

the Council of Europe began deliberations on the cybercrime treaty in 1997.[41] The Council invited observers from Canada, Israel, Japan, South Africa, and the United States[42] to take part in the negotiations in the hopes that the resulting treaty would have international impact.[43] The goal of these discussions was to create a cybercrime treaty which would "harmonize laws against hacking, fraud, computer viruses, child pornography and other Internet crimes"[44] as well as "make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of electronic evidence of a criminal offense."[45]

In April 2000, after nearly three years of negotiations, the Council posted to its website the first publicly-released version of the proposed treaty.[46] The proposed treaty addressed four principal areas: cybercrime, search and seizure, jurisdiction, and international cooperation.[47] In the area of cybercrime, this draft of the treaty criminalized four categories of crime: access crimes, data crimes, systems crimes, and crimes involving "illegal devices."[48] The first category,

---

[41] *Id.*
[42] James Evans, *Cyber-Crime Laws Emerge, but Slowly*, IDG.net, *available at* http://www.cnn.com/2000/TECH/computing/07/05/cyber.laws.idg/ (July 5, 2000).
[43] The council included these additional countries because of the high level of Internet activity in each country. Eighty percent of the world's Internet traffic emanates from the states participating in the negotiations. Reuters, *Cybercrime Treaty Gets a Makeover, available at* http://news.zdnet.co.uk/story/0,,s2082557,00.html (Nov. 14, 2000).
[44] *Id.*
[45] Preamble, *Final Draft Convention on Cyber-crime, at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (Nov. 23, 2001).
[46] The draft released was number 19. *Crime in Cyberspace: First Draft of International Conventional Released for Public Discussion, at* http://conventions.coe.int/Treaty/EN/projets/cybercrime (on file with the Richmond Journal of Law & Technology). The current draft is available at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (Nov. 23, 2001).
[47] In this paper, I have omitted discussion of Offenses Related to Child Pornography (Article 9), Intellectual Property (Article 10), Attempt and Aiding and Abetting (Article 11), and Corporate Liability (Article 12). *Id.*
[48] For a definition of "illegal devices," see infra note 57. Similar categories are also used in a report compiled by McConnell International concerning the state of cybercrime laws throughout the world. This report divided cybercrime into the categories of data crimes, network crimes,

access crimes, outlawed unauthorized access to data contained in a computer system and access to the computer system itself.[49] Under this provision of the treaty, it would be possible for a cybercriminal to be convicted of both gaining access to a computer system where desired data was stored and obtaining the desired data.[50] Data crimes, a second category of crime outlined in the treaty, made illegal the interception of data and interference with data.[51] The definitions of the two data crimes provided in the draft make it unclear whether data theft,[52] the outright taking or copying for the cybercriminal's use, was outlawed. The third category, systems crimes, outlawed actions that intentionally hindered the functionality of a computer system.[53] A clear example of such a violation is a denial of service attack.[54] Less clear is whether the

---

access crimes, and related crimes. The data crimes category included data interception, data modification, and data theft. Included in the network crimes category were network interference and network sabotage. The access crimes category included unauthorized access and virus dissemination. Included in the related crimes category were aiding and abetting cybercrimes, computer-related forgery, and computer-related fraud. MCCONNELL INT'L, CYBER CRIME… AND PUNISHMENT? ARCHAIC LAWS THREATEN GLOBAL INFORMATION, *at* http://www.mcconnellinternational.com/services/CyberCrime.htm (Dec. 2000).

[49] Article 2 defined illegal access as "intentional[]… access to the whole or any part of a computer system without right." Convention Draft, Convention Draft, *supra* note 46.

[50] Because the particulars of the offenses are enacted through domestic legislation, the act of breaching the system and the act of obtaining the data might or might not both be illegal in a particular state.

[51] Article 3 defined illegal interception as "intentional[]… interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, as well as electromagnetic emissions from a computer system carrying such data." Article 4 defined data interference as "intentional[]… damaging, deletion, deterioration, alteration, or suppression of computer data without right." Convention Draft, Convention Draft, *supra* note 46.

[52] MCCONNELL INT'L, CYBER CRIME… AND PUNISHMENT? ARCHAIC LAWS THREATEN GLOBAL INFORMATION, *at* http://www.mcconnellinternational.com/services/CyberCrime.htm (Dec. 2000).

[53] Article 5 defined system interference as "intentional[]…serious hindering without right of the functioning of a computer system by inputting, damaging, deleting, deteriorating, altering or suppressing computer data." Convention Draft, Convention Draft, *supra* note 46.

[54] A denial of service attack is "a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic." Webopedia, *at* http://webopedia.internet.com/TERM/D/DoS_attack.html (last modified Feb. 6, 2002).

dissemination of a computer virus[55] or computer worm[56] would constitute a violation. The final category of crime, "illegal devices," made it a crime to produce, sell, or obtain for use any device created or changed to facilitate the commission of any of the crimes enumerated in the treaty.[57] The illegal device provision raised the question as to how an individual who possessed a device could establish innocence. The provision was written with the presumption that an individual who possessed a device had the intent to use the device to engage in a cybercrime. Because the same devices are used by cybercriminals and by those employed to check the security of business systems, the presumed criminal intent was unfounded.[58]

The cybercrime articles included in the draft shared several common characteristics. First, the illegality of each crime was to be executed through the adoption of domestic legislation in each of the signator states.[59] Second, the definition of each cybercrime was to include the requirements of "intentionally" and "without right."[60] With the foregoing provisions, the treaty provided a framework to outlaw four categories of cybercrimes.

---

[55] A computer virus is "an insidious piece of computer code written to damage systems. Viruses can be hidden in executable program files posted online." Netdictionary, *at* http://www.netdictionary.com/html/v.html (last visited Sept. 20, 2001).

[56] A computer worm is "an insidious and usually illegal computer program that is designed to replicate itself over a network for the purpose of causing harm and/or destruction. While a virus is designed to invade a single computer's hard drive, a worm is designed to invade a network. The most infamous worm was created by Robert Tappan Morris in November 1988; it infiltrated over 6,000 network systems around the globe." Netdictionary, *at* http://www.netdictionary.com/html/w.html (last visited Sept. 20, 2001).

[57] Article 6 defined an illegal device as "a device…[used] for the purpose of committing any of the offenses established in accordance with Article 2-5." McConnell, s*upra* note 48.

[58] Brian Krebs, *Tech Groups Still Wary of International Cyber-Crime Treaty*, *at* http://www.newsbytes.com/news/00/158848.html (last modified Dec. 1, 2000)(on file with the Richmond Journal of Law & Technology) (covering the continuing concerns of security professionals over the illegal devices provision of the cybercrime treaty even after revisions attempted to address the perceived problem).

[59] Convention Draft, Convention Draft, *supra* note 46.

[60] "Without right" is not fully defined in Articles 2-6. The draft provided the option for the state to add the requirement of dishonest intent to the criminal definition. Convention Draft, Convention Draft, *supra* note 46.

As the preamble of the proposed cybercrime treaty envisioned that one of the purposes of the instrument was as "an international agreement to regulate trans-border search and seizure,"[61] this draft of the treaty also addressed search and seizure issues. The proposed treaty empowered law enforcement officials with the authority to search and seize data stored on computer systems, when such actions were taken as part of an investigation of cybercrime.[62] As part of this search and seizure power, the treaty authorized the officials to retain copies of the data.[63] Another power granted to law enforcement was the authority to order persons in its territory to produce specific computer data.[64] In investigations where a lapse of time could lead to a loss of computer-stored evidence, the proposed treaty authorized law enforcement officials to expedite the preservation of stored data and of traffic data.[65] As to stored data, expediting referred to shortening the time required to obtain a search and seizure warrant or a production order. With traffic data, the draft authorized law enforcement officials to require that ISPs retain traffic related to a suspect. In addition, the service provider was required to reveal enough of the traffic so that law enforcement officials could track the path by which the communication was transmitted.

---

[61] Convention Draft, *supra* note 46 (draft number 19).

[62] Article 14 of draft number 19 "empower[ed] competent authorities to search or similarly access a computer system… and computer data stored therein." In the article, the "competent authorities" were empowered to "seize or similarly secure computer data accessed… in view of their possible use in criminal investigations and proceedings." Convention Draft, *supra* note 46.

[63] In addition to seizure, Article 14 of draft number 19 authorized "mak[ing] and retain[ing] a copy of those computer data" and "render[ing] inaccessible or remov[ing] those computer data." Convention Draft, *supra* note 46.

[64] Article 15 of draft number 19 authorized "competent authorities to order a person in its territory… to submit specified computer data under this person's control." Convention Draft, *supra* note 46.

[65] Article 16 of draft number 19 enabled "competent authorities to order…the expeditious preservation of data that is stored by means of a computer system, at least where there are grounds to believe that the data…is [] particularly vulnerable to loss or modification." Article 17 of the same draft "ensure[d] the expeditious preservation of [] traffic data [concerning a specific

As was the case with the categories of cybercrime, the search and seizure articles shared several characteristics. First, according to the proposed treaty, the provisions were to be implemented through domestic legislation in each of the signatory states. Second, in an effort to address privacy concerns, each of the articles specifically provided that "the powers and procedures referred to in the present article shall be subject to conditions and safeguards as provided for under national law."[66] Third, conspicuously absent from the search and seizure provisions was any mention of a requirement for judicial review for particular applications of the new law enforcement authority.[67] Without a judicial check on the power granted to law enforcement officials, individuals would have no guaranteed protection against abuses. As such, the foregoing provisions outlined the search and seizure powers granted under the treaty.

Jurisdiction was the third area addressed by the treaty.[68] According to the proposed treaty, jurisdiction was based either on territory or on the nationality of the accused. The draft skirted the issue of whether the term "territory" applied to the state where the harm occurred or to the state where the perpetrator was located at the time that the cybercrime was committed. Instead of settling this issue, the treaty provided that disputes over jurisdiction should be decided between the states involved. With the foregoing provisions, the drafters espoused a structure for jurisdictional concerns.

---

communication], regardless of whether one or more service providers were involved in the transmission of that communication." Convention Draft, *supra* note 46.

[66] Convention Draft, *supra* note 46.

[67] Margret Johnston, *US Companies Find Europe's Cyber Crime Treaty Too Vague: Americans Fear Individual Countries' Due-Process Laws Could be Violated*, IDG News Service, *at* http://www.e-businessworld.com/english/crd_treaty_321309.html (Dec. 8, 2000)(on file with the Richmond Journal of Law & Technology) (detailing concerns by US companies that cybercrime treaty has provisions that may cause harm to those with no intention of breaking the law).

[68] Article 19 of draft number 19 provided that a state had jurisdiction "when an offense [was] committed in whole or in part in its territory, or on a ship, an aircraft, or a satellite flying its flag or registered in that Party, or by one of its nationals." The article stated that it did "not exclude

The fourth and final area addressed by the proposed treaty was international cooperation.[69] Mutual cooperation for investigation of crimes was expected of states that became parties to the treaty. The mutual cooperation article was vague as to the procedures that would be necessary to carry out the assisted investigation. As to extradition, the draft ensured that either an existing instrument or this treaty could be used as the basis for extradition of a cybercriminal. The foregoing provisions thus provided a skeletal plan for international cooperation. As outlined in this section, the proposed treaty attempted to address the new 'tools' of cybercriminals by providing law enforcement with new powers to investigate the international nature of cybercrime. The inadequacies of the proposed treaty, which have been suggested in this section, did not pass unnoticed for long.

B. The Outcry

Until the public release of the proposed treaty in April 2000, member delegations had worked in virtual secrecy on the negotiations.[70] The Internet release of the treaty triggered

---

any criminal jurisdiction exercised in accordance with national law." Convention Draft, *supra* note 46.

[69] Article 20 in draft 19 provided for the "application of relevant international instruments on international co-operation in criminal matters." Article 21 concerned extradition. It stated that the criminal offences established in the treaty "shall be deemed as extraditable offences in any extradition treaty" existing between parties and for parties that do not have an extradition treaty the cybercrime treaty may be considered the basis for extradition. Article 22 provided for mutual assistance. In particular, the article provides for "mutual assistance to the widest extent possible for the purpose of investigations and proceedings concerning criminal offences relating to computer systems and data, or for the collection of electronic evidence of a criminal offence." Article 27 outlined access to computer data outside one's territory without the need for mutual assistance. In the case where computer data is publicly available, mutual assistance is not required regardless of the geographic location of the data. A state may also access computer data outside its territory, without the aid of mutual assistance, when it obtained the "voluntary consent of the person who has the lawful authority to permit the [state] access… to that data." Convention Draft, *supra* note 46.

[70] The Council has given no explanation for the lack of openness in the first three years of negotiations. Reuters, *Cybercrime Treaty Gets a Makeover, at* http://news.zdnet.co.uk/story/0,,s2082557,00.html (Nov. 14, 2000); Rick Perera, *UPDATE: Human Rights Groups Slam Cyber Crime Pact, at* http://www.idg.net/ic_273062_1794_9-

angered outcries from more than 400 e-mailers[71] and garnered the condemnation of a coalition of 29 international cyber-rights organizations, which represented the views of privacy experts, data protection officials, and technical experts.[72] In a letter to the Council of Europe, the Global Internet Liberty Campaign (GILC)[73] outlined its concerns with the proposed treaty.[74] Technical experts complained that the treaty's broad provision concerning illegal devices[75] would

---

10000.html (Oct. 18, 2000). *See also* Juliana Gruenwald, *Europeans Defining the Long Arm of The Cyberlaw, at* http://news.zdnet.co.uk/story/0,,s2081836,00.html (Sept. 25, 2000) (on file with the Richmond Journal of Law & Technology). In the GILC letter, the coalition writes, "We also object in very strong terms to the manner under which this proposal was developed. Police agencies and powerful private interests acting outside of the democratic means of accountability have sought to use a closed process to establish rules that will have the effect of binding legislation. We believe this process violates requirements of transparency and is at odds with democratic decisionmaking." *Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime, at* http://www.gilc.org/privacy/coe-letter-1000.html (Oct. 18, 2000).

[71] Although it is unclear why the author of the article "Cybercrime Treaty Gets a Makeover" chose to state that the council was "inundated" with over 400 e-mails when there are millions of on-line users, a fair reading of the statement may take into consideration the relative obscurity of the proposal. Few Internet media sources covered the proposal, suggesting that the 400 people who e-mailed were interested enough to find the treaty by partaking of their own searches. Reuters, *Cybercrime Treaty Gets a Makeover, at* http://news.zdnet.co.uk/story/0,,s2082557,00.html (Nov. 14, 2000); *see also Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime, at* http://www.gilc.org/privacy/coe-letter-1000.html (Oct. 18, 2000).

[72] Robert Lemos, *Coalition Slams Cybercrime Treaty, at* http://www.zdnet.com/zdnn/stories/news/0,4586,2642290,00.html (Oct. 18, 2000).

[73] The Global Internet Liberty Campaign is a coalition of 29 international cyber-rights organizations that joined forced to speak out against the proposed treaty. Organizations included in the coalition are the U.S.'s American Civil Liberties Union, Bits of Freedom, U.K.'s Cyber-Rights and Cyber-Liberties, Electronic Frontiers Australia, Russia's Human Rights Network, France's IRIS, Spain's Kriptopolis, and South Africa's LINK Centre. *See* Robert Lemos, *Coalition Slams Cybercrime Treaty, at* http://www.zdnet.com/zdnn/stories/news/0,4586,2642290,00.html (Oct. 18, 2000); Rick Perera, *Update: Human Rights Groups Slam Cyber Crime Pact, at* http://www.idg.net/ic_273062_1794_9-10000.html (Oct. 18, 2000).

[74] *Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime, at* http://www.gilc.org/privacy/coe-letter-1000.html (Oct. 18, 2000). The letter also addresses copyright crimes, but that provision of the treaty is beyond the scope of this paper.

[75] Article 6 of the proposed treaty defined an illegal device as "a device…[used] for the purpose of committing any of the offenses established in accordance with Article 2-5." Convention Draft, *supra* note 46.

criminalize possession of devises used by security practitioners, educators, and researchers to increase the security of computer systems.[76] The concern centered on the fact that the devices used to ensure security within a system are the same ones utilized by hackers to gain unauthorized access to computer systems.[77] Those involved in securing systems worried that the provision of the treaty outlawed possession of such devices without regard to their intended use.[78] The coalition asserted that procedures for international investigations[79] had been omitted from the proposed treaty, and that such procedures should be agreed upon in order to ensure that a consistently high level of individual rights was maintained.[80] As to search and seizure,[81] the

---

[76] *Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime, at* http://www.gilc.org/privacy/coe-letter-1000.html (Oct. 18, 2000).
[77] Brian Krebs, *Tech Groups Still Wary of International Cyber-Crime Treaty, at* http://www.newsbytes.com/news/00/158848.html (last modified Dec. 1, 2000) (on file with the Richmond Journal of Law & Technology)(covering the continuing concerns of security professionals over the illegal devices provision of the cybercrime treaty even after revisions attempted to address the perceived problem).
[78] *Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime, at* http://www.gilc.org/privacy/coe-letter-1000.html (last modified Oct. 18, 2000).
[79] Article 20 provided for the "application of relevant international instruments on international co-operation in criminal matters." Article 21 concerned extradition. It stated that the criminal offences established in the treaty "shall be deemed as extraditable offences in any extradition treaty" existing between parties and for parties that do not have an extradition treaty the cybercrime treaty may be considered the basis for extradition. Article 22 provided for mutual assistance. In particular, the article provides for "mutual assistance to the widest extent possible for the purpose of investigations and proceedings concerning criminal offences relating to computer systems and data, or for the collection of electronic evidence of a criminal offence." Article 27 outlined access to computer data outside one's territory without the need for mutual assistance. In the case where computer data is publicly available, mutual assistance is not required regardless of the geographic location of the data. A state may also access computer data outside its territory, without the aid of mutual assistance, when it obtained the "voluntary consent of the person who has the lawful authority to permit the [state] access… to that data." Convention Draft, *supra* note 46.
[80] *Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime, at* http://www.gilc.org/privacy/coe-letter-1000.html (Oct. 18, 2000).
[81] Article 14 "empower[ed] competent authorities to search or similarly access a computer system… and computer data stored therein." In the article, the "competent authorities" were empowered to "seize or similarly secure computer data accessed… in view of their possible use in criminal investigations and proceedings." Article 15 authorized "competent authorities to order a person in its territory… to submit specified computer data under this person's control."

coalition stated that the treaty lacked any assurance of an independent judicial review in particular instances were the search and seizure powers would be utilized.[82] The treaty's provisions pertaining to the preservation of Internet traffic and the review of the content of communications relating to an individual under investigation[83] raised a host of concerns. For the ISPs, the requirement to preserve communications meant an increase in operating costs. Additional costs incurred by the ISPs would include the personnel hours and the storage space necessary to execute the requests of law enforcement.[84] For the cyber-rights organizations involved in the coalition, the requirement that traffic and content information be made available to law enforcement raised substantial privacy concerns. The coalition asserted that the treaty would encourage "inappropriate monitoring of private communications,"[85] which would violate accepted privacy norms.[86] One of the specific worries was that inappropriate monitoring would lead to persecution of dissidents and minorities.[87] In summing up their position, the coalition stated that the treaty improperly extended police power while failing to protect privacy of

---

Article 16 enabled "competent authorities to order…the expeditious preservation of data that is stored by means of a computer system, at least where there are grounds to believe that the data…is [] particularly vulnerable to loss or modification." Article 17 "ensure[d] the expeditious preservation of [] traffic data [concerning a specific communication], regardless of whether one or more service providers were involved in the transmission of that communication." Convention Draft, *supra* note 46.

[82] *Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime, at* http://www.gilc.org/privacy/coe-letter-1000.html (Oct. 18, 2000).

[83] Article 17 of the proposed treaty "ensure[d] the expeditious preservation of [] traffic data [concerning a specific communication], regardless of whether one or more service providers were involved in the transmission of that communication." Convention Draft, *supra* note 46.

[84] Steven Abood, *The Draft Convention on Cybercrime: What Every Internet Service Provider Should Know,* at http://www.tilj.com/content/webarticle02050101.htm (Feb. 5, 2001).

[85] *Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime, at* http://www.gilc.org/privacy/coe-letter-1000.html (Oct. 18, 2000).

[86] *Id*. (specifically citing a violation of the Data Protection Directive of the European Union).

[87] Nadine Strossen, *Contemporary Challenges to Privacy Rights*, 43 N.Y.L. SCH. L. REV. 195, 198 (1999) (pursuing the same line of reasoning).

communication, freedom of expression, or criminal procedure protections, all of which are considered rights under the Universal Declaration of Human Rights.[88]

C. Draft 27: The Final Revision to the Treaty[89]

The criticism stunned the Council of Europe.[90] Peter Csonka, deputy head of the Council of Europe's economic crime division,[91] said, "We were surprised by the violence of these comments, ... We have learned we have to explain what we mean in plain language because legal terms are sometimes not clear."[92] Through a series of drafts, the Council worked to address the issues raised concerning illegal devices, procedural safeguards, and ISP retention of traffic[93] and content data.[94] The drafters responded to the concern expressed by security personnel that the treaty criminalized the mere use of certain devises by adding a provision, which provided that those who possessed the devises without the intent of committing cybercrimes had not acted

---

[88] *Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime*, *at* http://www.gilc.org/privacy/coe-letter-1000.html (Oct. 18, 2000) ("We believe that the draft treaty is contrary to well established norms for the protection of the individual [and] it improperly extends the police authority of our national government . . . .").

[89] "A committee on crimes for the Council of Europe signed off . . . on the final draft of a broad treaty that aims to help countries fight cybercrime . . . . [The treaty] reached its 27th draft before being approved . . . . " Robert Lymos, *International Cybercrime Treaty Finalized*, *at* http://news.cnet.com/news/0-1003-200-6352408.html?tag=mn_hd (June 22, 2001).

[90] Reuters, *Cybercrime Treaty Gets a Makeover*, at http://news.zdnet.co.uk/story/0,,s2082557,00.html (Nov. 14, 2000).

[91] *Id.* (stating that the economic crime division of the Council of Europe is overseeing the creation of the treaty).

[92] *Id.*

[93] "Traffic data" is defined in Article 1.d. as "any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, including the communication's origin, destination, route, time, date, size, duration, or type of underlying service." *Final Draft Convention on Cybercrime* art. 1, *at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm/ (Nov. 23, 2001).

[94] "Content data" is not defined in the treaty, but is defined in the Explanatory Memorandum as "[t]he message or information being conveyed by the communication (other than the traffic data)." *Draft Convention on Cybercrime and Explanatory Memorandum Related Thereto* tit. 5, ¶ 209, *at* http://conventions.coe.int/treaty/EN/projets/FinalCyberRapex.htm (Nov. 8, 2001).

illegally.[95] In an effort to avoid the increased criminalization feared by GILC, the drafters required that two types of intent be established for an individual to be convicted of the crime of misuse of devises. The first type of intent was a general intent to engage in illegal activity. Second, the specific intent to use the devise to commit one of four crimes outlined in the treaty – illegal access, illegal interception, data interference, or system interference – had to be established.[96]

With regards to criminal procedure issues, the drafters inserted an article requiring minimum safeguards to adequately protect human rights and liberties.[97] The treaty required each state to ensure, through domestic legislation, independent supervision of the treaty power in question, justification of the use of the power, and a limitation on the scope and duration of the power.[98] The decision as to which treaty powers are sufficiently intrusive to require the safeguards set out in the article was left to the respective states.[99]

---

[95] Surprisingly, the main focus of the treaty, the harmonization of the definitions of cybercrimes, met with little opposition. One exception to this general acceptance of the definitions was the provision on illegal devices. "This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use… is not for the purpose of committing and offense… of this Convention, such as for the authorized testing or protection of a computer system." *Final Draft Convention on Cybercrime* art. 6, *at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (Nov. 23, 2001).

[96] *Draft Convention on Cybercrime and Explanatory Memorandum Related Thereto* tit. 1, ¶ 73-76, *at* http://conventions.coe.int/treaty/EN/projets/FinalCyberRapex.htm (Nov. 8, 2001).

[97] Article 15 is entitled "Conditions and safeguards." *Final Draft Convention on Cybercrime* art. 15, § 1**,** *at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (Nov. 23, 2001). These minimum safeguards are those to which the state is obliged under applicable international human rights treaties. Most of the states would be bound to those safeguards outlined in the International Covenant on Civil and Political Rights, *Draft Convention on Cybercrime and Explanatory Memorandum Related Thereto* tit.1, ¶ 145, *at* http://conventions.coe.int/treaty/EN/projets/FinalCyberRapex.htm (Nov. 8, 2001).

[98] In particular, the safeguards included "judicial or other independent supervision, grounds justifying application, and limitation on the scope and the duration of such power and procedure." *Final Draft Convention on Cybe-crime* art. 15, § 2, *at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (Nov. 23, 2001).

[99] *Draft Convention on Cybercrime and Explanatory Memorandum Related Thereto* tit. 1, ¶ 147, *at* http://conventions.coe.int/treaty/EN/projets/FinalCyberRapex.htm (Nov. 8, 2001).

To address the concerns pertaining to ISP retention of Internet traffic and content data, the drafters clarified the requirements by stipulating that the ISPs would only be asked to store specific data related to suspected crimes.[100] In these provisions, however, the drafters did not limit the time period for which the ISPs would be required to retain traffic and content data concerning alleged crimes. Although the drafters restricted the scope of the data to be maintained,[101] without a limitation concerning the time period for retention of data, ISPs could still incur significant business costs in adhering to the provisions of the treaty.[102] In addition, when law enforcement officials engaged service providers to collect data, the requirement that the providers keep confidential the fact that data was being collected[103] put the ISPs at odds with the privacy interests of their customers.[104]

---

[100] Two provisions of the treaty provide that ISPs can only be compelled to collect data associated with specific communications. The two articles are Article 20 -- Real-time Collection of Traffic Data and Article 21 -- Interception of Content Data. *Final Draft Convention on Cybercrime, at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (Nov. 23, 2001). The memorandum defines "traffic data" as relating to the time, duration, and size of the communication while "content data" refers to the actual text or visuals. *Draft Convention on Cybercrime and Explanatory Memorandum Related Thereto,* tit. 5, ¶ 227, *at* http://conventions.coe.int/treaty/EN/projets/FinalCyberRapex.htm (Nov. 8, 2001).

[101] "[T]he Convention does not require or authorize the general or indiscriminate surveillance and collection of large amounts of traffic data. It does not authorise the situation of 'fishing expeditions' where criminal activities are hopefully sought to be discovered . . . ." *Draft Convention on Cybercrime and Explanatory Memorandum Related Thereto,* tit. 5, ¶ 219, *at* http://conventions.coe.int/treaty/EN/projets/FinalCyberRapex.htm (Nov. 8, 2001).

[102] Business costs would include staff hours to track the data and storage space to keep records. Steven Abood, *The Draft Convention on Cybercrime: What Every Internet Service Provider Should Know,* The Internet Law Journal, *at* http://www.tilj.com/content/webarticle02050101.htm (Feb. 5, 2001).

[103] This provision was contained in both Article 20 and Article 21. *Final Draft Convention on Cybercrime, at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (Nov. 23, 2001).

[104] Recognizing this issue, the drafters required each state to adopt legislation to oblige the service provider to keep confidential the fact that the government was collecting data on the customer. *Id*. art. 20, § 2. According to the drafters, this would relieve the service provider of any contractual or legal obligation to notify the customer of the surveillance activity. *Draft Convention on Cybercrime and Explanatory Memorandum Related Thereto* tit. 5, ¶ 226, *at* http://conventions.coe.int/treaty/EN/projets/FinalCyberRapex.htm (Nov. 8, 2001).

While three of the revisions made by the drafters addressed specific concerns regarding illegal devices, procedural safeguards, and ISPs' retention of data, additional modifications to the treaty raised new issues. The treaty itself unnecessarily created four sets of problems concerning sovereignty, jurisdiction, search and seizure of computer data, and international investigation. In the arena of sovereignty, both the article concerning search and seizure and the article pertaining to trans-border access to data without consent[105] permit law enforcement officials to cross state boundaries without notifying or gaining permission from the intruded state.[106] Although some experts argue, "[i]t may be legitimate and important for law enforcement to be allowed to conduct a remote search of computers in a foreign country,"[107] it is unclear why the drafters have allowed these intrusions of sovereignty when the treaty provides for mutual assistance between states and provides for expedited mutual assistance when necessary.

[105] As in the original draft, trans-border access to stored computer data was allowed in certain circumstances without the consent of the state where the information was located. Access was permissible when the data was publicly available or when the investigating state obtained consent from a person who has lawful authority to disclose the data. The article pertaining to trans-border access, Article 32, provided, " A Party may, without obtaining the authorization of another Party: a. access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b. access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system." *Final Draft Convention on Cybercrime***,** *at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (Nov. 23, 2001) (observing that no precise definition is given for "publicly available" and that directly preceding the quoted words are the words "open source" in parentheses).

[106] Under Article 19, this invasion was authorized if the person who owned the computer was present in the state or if the ISP offered services in the state. *Id.* As to trans-border access without consent of the intruded state, access was allowed if the data was publicly available or if permission was gained from a person in the state who had legal authority to give such permission. *Id*.

[107] David Goldstone & Betty-Ellen Shave, *International Dimensions of Crimes in Cybercrime*, 22 FORDHAM INT'L L.J. 1924, 1937-38 (1999).

In the area of jurisdiction, the drafters failed to address the problems raised by the existence of cyberspace.[108] No state has jurisdiction over cyberspace.[109] Thus, jurisdiction cannot simply be based on the place where the cybercrime took place. According to the treaty, jurisdiction was based primarily on territory and secondarily on nationality.[110] In an instance where more than one state claimed jurisdiction over an alleged offense, the treaty provided for the states involved to decide the "most appropriate jurisdiction for prosecution."[111] The "most appropriate jurisdiction" clause will likely be much invoked because of the ambiguity in the meaning of territory-based jurisdiction. The provision could be interpreted to provide jurisdiction to the state in which the perpetrator was located, as happened in the case of the I LOVE YOU virus where the Philippine government investigated the individual who released the virus from that state.[112] Unfortunately, this provision could just as easily be interpreted to give jurisdiction to the state in which the damage from the attack occurred. Alternatively, the provision could be construed to grant jurisdiction in either the host state or the victim state, with

---

[108] The provision concerning jurisdiction received only minor clarifications that did not address the main problem with the provision. One such minor clarification was that, under the first draft, jurisdiction based on territory could be established in relation to a satellite flying the flag of the state. Convention Draft, *supra* note 46. The mention of satellites was dropped from Draft 27 of the treaty. *Final Draft Convention on Cybercrime* art. 22, *at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (Nov. 23, 2001).

[109] Interview with Bill Thompson, Internet Privacy and Security Issues Expert for Special Services Group, in Atlanta, Ga. (Sept. 15, 2000).

[110] Under Article 22, jurisdiction over any offence in the treaty may be established if the offence was committed "in its territory, or on board a ship flying its flag, or on board an aircraft registered under the laws of that Party, or by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State." *Final Draft Convention on Cybercrime*, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (Nov. 23, 2001).

[111] "When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution." *Id.*

[112] James Evans, *Cyber-Crime Laws Emerge, but Slowly, at* http://www.cnn.com/2000/TECH/computing/07/05/cyber.laws.idg/ (July 5, 2000).

place of jurisdiction depending on the particular cybercrime at issue.[113] The drafters made no attempt to solve this predicament.[114] It is unclear why the drafters simply did not choose one of the above-mentioned meanings of the term 'territory.'

In search and seizure of computer data, the drafters clarified those who are subject to orders that require production of specified computer data for use in law enforcement investigations.[115] Under the newly crafted provision, any person physically located in the state or any service provider offering services within the state would be required to submit data

[113] Examples involving two cybercrimes may help to clarify. In the instance of a computer virus, it may be easiest to try the perpetrator in the state where the individual was located at the time of the attack for two reasons. First, the law enforcement officials will likely be able to physically detain the individual. Second, because there are likely multiple victims in multiple states, the process of prosecuting will be simplified by occurring in only one state, namely the state where the individual is located. In a case of cybertheft, however, it may be that the drafters intended for the state where the theft occurred to have jurisdiction. Because there may only be one victim, the initial investigation of the cybertheft can easily begin by tracking the accused from the compromised computer in the victim state. This investigation can be accomplished without initially knowing where the perpetrator was located.

[114] Provisions concerning assistance between states changed little from the first publicly-released draft. Article 24 on extradition provided that the offenses in the treaty fulfilled the requirement of extraditable offenses for any existing extradition treaty between states and that the treaty would act as an extradition treaty for any states that lack such a treaty. Article 25, concerning general principles of mutual assistance, stipulated that the provisions on mutual assistance "shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties." Mutual assistance regarding accessing of stored computer data, discussed in Article 31, provided, "A Party may request another Party to search or similarly access, seize, or similarly secure, and disclose stored data by means of a computer system located with the territory of the requested Party." Article 33, mutual assistance regarding the real-time collection of traffic data, stipulated that "[t]he Parties shall provide mutual assistance to each other with respect to the real-time collection of traffic data associated with specified communications in its territory transmitted by means of a computer system." Mutual assistance regarding the interception of content data, Article 34, provided, "The Parties shall provide mutual assistance to each other with respect to the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent applicable by their applicable treaties and domestic laws." Articles 29 and 30 allowed for law enforcement officials to expedite requests for preservation of stored data and disclosure of preserved data. *See* Convention Draft, *supra* note 46.

[115] In the initial draft, Draft 19, production orders applied to "a person in its territory." No clarification of "person" or "in the territory" was provided. Convention Draft, *supra* note 46.

requested by means of a production order.[116] According to this language, production could be required from a computer outside the state so long as it belonged to an individual who was physically present in the state or to a service provider that provided services within the state. A complimentary provision provided for search and seizure of stored computer data.[117] The draft empowered competent authorities to search and seize computer data within the state. Reading the two provisions together would allow for data produced from outside the state, pursuant to a production order, to be seized once in the state.

Generally speaking, the problems created by the treaty are unnecessary. The treaty is intended to encourage uniform definitions of cybercrime and through such uniformity to enhance the ability of law enforcement to investigate these cybercrimes. A carefully written treaty with well-defined provisions could have avoided much unnecessary confusion. The question remains as to whether overall privacy concerns have been adequately addressed by the revisions to the treaty. In international investigations, the drafters omitted any clear procedures that could have ensured high levels of protection for individual rights.[118] In an effort to address broad privacy concerns, the "powers and procedures" provision of the articles on expedited preservation of stored computer data, expedited preservation and partial disclosure of traffic data, production orders, search and seizure of stored computer data, real-time collection of traffic data, and

[116] Article 18, Production Orders, empowers [a state's] competent authorities to order a person in [the state's] territory as well as a service provider offering its services in a territory to submit computer data under its possession or control to law enforcement officials. *Final Draft Convention on Cyber-crime, at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (Nov. 23, 2001).

[117] Article 19 empowers competent authorities to search a computer system and to seize a computer system or a computer-data storage medium in a search. *Id*.

[118] *Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime, at* http://www.gilc.org/privacy/coe-letter-1000.html (Oct. 18, 2000).

interception of content data are all "subject to Article 14 and 15."[119] These two articles provide that the powers and procedures are subject to the safeguards provided under domestic law and under applicable international human rights treaties.[120] Thus, critical to an understanding of the privacy protections afforded by the treaty is knowledge of the safeguards provided by domestic law and by pertinent international human rights treaties.

III. Examples of Privacy Protections Provided Under Domestic Laws

A. Treaty Expected to Become International Standard

While the focus of the treaty is to increase police power to allow law enforcement officials to effectively battle the new 'tools' of cybercriminals, there is a concern that the increase in police power will not be properly rebalanced with the privacy rights of individuals.[121] In an attempt to rebalance the scales between police power and privacy, the treaty protects privacy through safeguards provided under domestic laws and under applicable human rights treaties. Because the first set of safeguards provided under the treaty are those found in domestic laws,[122] the first part of the answer to the question of whether the treaty adequately addresses Internet-Age privacy concerns must be found by examining domestic protections of privacy.

---

[119] Articles 16, 17, 18, 19, 20, and 21, respectively. *Final Draft Convention on Cyber-crime, at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (Nov. 23, 2001).

[120] Article 14 calls for each state to establish the "powers and procedures" necessary for "the purpose of specific criminal investigations or proceedings." Article 15 states that the powers and procedures shall be subject to the conditions and safeguards provided for under the domestic law of each Party concerned, with due regard for the adequate protection of human rights. It further states that "such conditions and safeguards shall, as appropriate in view of the nature of the power or procedure concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation on the scope and the duration of such power or procedure." *Final Draft Convention on Cyber-crime, at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (Nov. 23, 2001).

[121] *See* Fletcher N. Baldwin, Jr., *Cybercrime: The Dawning of the Age of the Internet, in* 1 CYBERCRIME & SECURITY 18 (Alan E. Brill et al. eds., 1998).

[122] *Final Draft Convention on Cybercrime* art. 15, *at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (Nov. 23, 2001).

The key to understanding the privacy protections afforded by current domestic laws is two-fold, meaning that a recognition of the policies enacted in the states is needed as well as a grasp of the impact of each state's policies when two or more states interact. The policies adopted by states will first be examined to determine the goals that the state desires to further with its Internet crime control policy in addition to exploring the ability of the government to prosecute the crime and the capacity of the victim to recover for his losses. The outcomes of interactions between states with differing levels of privacy protection will then be explored.

B. Three Examples of Southeast Asian States with Differing Levels of Privacy Protection

As it is not possible to examine every state, several states in Southeast Asia have been chosen to illustrate the overall approach to privacy protection afforded by the treaty.[123] Three Southeast Asian states were selected to illustrate the first prong of the approach, privacy protection afforded by domestic laws. Southeast Asian states were selected because their history of colonialism, which they subsequently replaced with emerging capitalist economies, represents the experience of many of the states that exist outside of Europe.[124] Singapore, Thailand, and the Special Administrative Region of Hong Kong have been specifically chosen because each provides an example of a differing level of privacy protection. For each of these three, Internet crime control policies will be examined. The second prong of the approach, which examines the

[123] Even though the treaty will originally be open only to the 41 members of the Council of Europe and limited non-members, such as Canada, Israel, Japan, South Africa and the United States, there is a belief that the treaty will at some point become global in scope. As such, the hypotheticals examine interactions that include states not initially signatories to the treaty. *See* Press Release, Council of Europe, Crime in Cyberspace: First Draft of International Conventional Released for Public Discussion, *at* http://conventions.coe.int/treaty/en/projets/cyber.htm (Apr. 27, 2000).

[124] Several countries in this region are known as Asian Tigers due to fast growing economies that create vast concentrations of wealth. In addition, this area of the world has a significant population.

outcomes of the interactions between states with differing levels of privacy protection, will be illustrated with two hypothetical interactions between a European state and the three Southeast Asian states.

1. Singapore: An Example of a Low Level of Privacy Protection

The kind of society that a state supports determines the goals concerning privacy protection that underlie the Internet crime control policy of that state.[125] Totalitarian states oppose privacy rights while liberal democratic systems support individual privacy rights and freedoms.[126] These two abstract kinds of societies lie on opposite poles of the political spectrum.[127] Singapore is known for its near totalitarian regime. In support of the doctrine that the kind of society determines the level of privacy protection, Singapore has a reputation for aggressively using surveillance for social control.[128] In its approach to Internet crime control, the goal of the government is to shield its citizens from any undesirable influences.[129] In an effort to

---

[125] *See* C. Keith Boone, *Privacy and Community*, 9 SOC. THEORY & PRAC. 1 (1983), *reprinted in* RICHARD C. TURKINGTON & ANITA L. ALLEN, PRIVACY LAW: CASES AND MATERIALS 16 (West 1999). "[W]hether or not privacy and community are antagonistic depends on the *kind* of society in question." *Id.*

[126] "Consider two kinds of societies lying at opposite poles of the political spectrum, as in the cases of a statist totalitarian society and a liberal democracy. Essential to the development of the totalitarian society is the full expansion of the public into the private sphere, such that no society may properly be termed totalitarian until it has 'simply liquidated the whole sphere of privacy.'

. . .

By contrast, consider a liberal democratic system committed to long-standing political concepts of equal liberty, individual rights and freedoms, and an open, nonrepressive [sic] democratic process. . . . Linked as it is to the moral and material well-being of individuals, liberal social philosophy emphasizes the importance of nourishing individuality and liberty in its citizenry.

. . .

. . . It is apparent, then, that within the normative framework of a liberal democracy, it is the suppression of privacy, not its invigoration, that is antagonistic to community." *Id*. at 16-18.

[127] *Id*. at 16.

[128] *See* PRIVACY INT'L, PRIVACY AND HUMAN RIGHTS 2000: COUNTRY REPORT ON SINGAPORE, *at* http://www.privacyinternational.org/survey/phr2000 (2000).

[129] Baldwin, *supra* note 122, at 17. Singapore's general approach to Internet policy is censorship. *See* Steven M. Hanley, *International Internet Regulation: A Multinational*

ensure government supervision of Internet usage, all ISPs are government-owned or government-controlled companies.[130] The Telecommunications Authority of Singapore has extensive authority to monitor any activity considered to be a threat to national security.[131] The Authority routinely monitors phone conversations and Internet use.[132]

Singapore has no constitutionally protected right to privacy against government acts.[133] Although government officials are normally required to obtain court-issued search warrants, exceptions exist to this general warrant rule. Law enforcement may search without a warrant if they believe the intrusion is necessary to preserve evidence and warrantless searches are permitted in drug-related and organized-crime-related incidents.[134] Specific to Internet-related crime, the police do not need a warrant to search computers under the Electronic Transactions Act (ETA).[135]

Singapore has passed criminal laws that enable the prosecution of perpetrators of Internet crime. The Computer Misuse Act (CMA)[136] prohibits unauthorized access to computer data,

---

Approach, 16 J. MARSHALL J. COMPUTER & INFO. L. 997, 1012 (1998); Lewis S. Malakoff, *Are You My Mommy, or My Big Brother? Comparing Internet Censorship in Singapore and the United States*, 8 PAC. RIM L. & POL'Y J. 423; Joseph C. Rodriguez, *A Comparative Study of the Internet Content Regulations in the United States and Singapore: The Invincibility of Cyberporn*, 1 ASIAN-PAC. L. & POL'Y J. 9 (2000); Peng Hwa Ang & Berlinda Nadarajan, *Censorship and Internet: A Singapore Perspective*, *at* http://www.isoc.org/HMP/PAPER/132/txt/paper.txt (last modified May 4, 1995).

[130] PRIVACY INT'L, PRIVACY AND HUMAN RIGHTS 2000: COUNTRY REPORT ON SINGAPORE, *at* http://www.privacyinternational.org/survey/phr2000 (2000).

[131] *Id.*

[132] *Id.*

[133] *Id.*

[134] U.S. DEPT. OF STATE, COUNTRY REPORTS ON HUMAN RIGHTS: PRACTICES FOR 1996: SINGAPORE, http://www.privacy.org/pi/reports/hr96_privacy_report.html (Jan. 1997).

[135] Electronics Transactions Act ch. 88, pt. XII, § 53 (Sing.), *at* http://www.lawnet.com.sg/free/vldb.htm (July 10, 1998); *see also* PRIVACY INT'L, *supra* note 131.

[136] Computer Misuse Act ch. 50A, pt. III, § 16 (Sing.), *at* http://www.lawnet.com.sg/free/vldb.htm (1998); *see also* PRIVACY INT'L, *supra* note 131.

unauthorized modification of computer data, unauthorized obstruction of the use of computers, and unauthorized disclosure of access codes.[137] The ETA imposes a duty of confidentiality on individuals who possess data obtained under the act and imposes sanctions for disclosing such data without authorization. [138]

As to whether Singapore has jurisdiction over such crimes, the policy of Singapore is to extend the territorial principle[139] in cases where there is some nexus between the territory and the crime.[140] In particular, the CMA grants to courts jurisdiction over anyone who commits a crime under the act. Regardless of citizenship, the accused is treated as if he was in Singapore at the time of the incident or as if the computer, the program, or the data was in Singapore at the time of the incident.[141]

As to recovery of losses by the victim, no general data protection or privacy laws exist in Singapore.[142] However, in association with criminal prosecution against businesses and rogue individuals, the CMA requires the perpetrator to pay compensation, which the victim can recover through civil debt procedures.[143] Even in cases where a criminal prosecution was not achieved,

---

[137] Under the CMA, police may access any computer at any time, including data that is encrypted. Anyone refusing to assist the police in a cybercrime investigation may be prosecuted. The police are authorized to arrest, without warrant, any person who is reasonably expected to have committed an offense under the CMA. Computer Misuse Act ch. 50A, pt. III, § 15(1)(a) (Sing.), *at* http://www.lawnet.com.sg/free/vldb.htm (1998).

[138] Electronics Transactions Act ch. 88, pt. XII, § 48 (Sing.), *at* http://www.lawnet.com.sg/free/vldb.htm (July 10, 1998).

[139] "[E]quality of states and non-interference in domestic affairs of a state are the foundations of the international order. Hence, territoriality was the accepted basis of exercising jurisdiction as it accorded with these organising principles of international law." M. Sornarajah, *Globalisation and Crime: The Challenges to Jurisdictional Principles*, 1999 SINGAPORE J. OF LEGAL STUD. 409, 411-12 (1999), *available at* http://www.law.nus.edu.sg/sjls/articles.htm.

[140] *Id*. at 412.

[141] Computer Misuse Act ch. 50A, pt. III, § 11 (Sing.), *at* http://www.lawnet.com.sg/free/vldb.htm (1998); *see a*lso PRIVACY INT'L, *supra* note 131.

[142] Ravi Chandran, *Privacy in Employment*, 2000 SINGAPORE J. LEGAL STUD. 263, 265 (2000).

[143] Computer Misuse Act ch. 50A, pt. 3, § 13 (Sing.), *at* http://www.lawnet.com.sg/free/vldb.htm (1998).

the victim can sue the business or rogue individual based on tort law, in an action for breach of confidence.[144] To be successful, the victim must establish that the data is not trivial, that he had a legitimate expectation of privacy in the data, and that the use of the data was unauthorized.[145] In Singapore, the government can prosecute cybercrime and the victim has a means to recover damages that result from the cybercrime. As the goal of the Internet crime control policy is social control, Singapore is an example of a low level of privacy protection.

2. Thailand: An Example of an Intermediate Level of Privacy Protection

On the totalitarian/liberal democracy spectrum, Thailand falls into the middle of the range. The government's concerns over national security and public morals drive its privacy policies.[146] On the privacy-of-communications front, Thailand's Constitution provides for the protection of privacy.[147] Specifically, the constitution stipulates a protection of communication. Although the state guarantees privacy by law, in reality privacy is not protected. Activities such as illegal wiretapping are commonplace in Thailand.[148] As for protection against unreasonable government intrusion, in most instances, law enforcement officers are required to obtain a

---

[144] Ravi Chandran, *Privacy in Employment*, 2000 SINGAPORE J. LEGAL STUD. 263, 265 (2000) (examining employee/employer context, but generally applicable to situations that arise in Singapore).

[145] *Id.* at 265-281(including a discussion of how the tort applies to e-mail).

[146] THAIL. CONST. § 37 (1997), *available at* http://www.krisdika.go.th/law/text/lawpub/e11102540/text.htm (last visited Sept. 17, 2002) (stating that persons "shall enjoy the liberty of communication by lawful means" and providing an exception for action taken "by virtue of the law specifically enacted for security of the State or maintaining public order or good morals"); *see also* PRIVACY INT'L, PRIVACY AND HUMAN RIGHTS 2000: COUNTRY REPORT ON KINGDOM OF THAILAND, *at* http://www.privacyinternational.org/survey/phr2000 (2000).

[147] THAIL. CONST. § 34, 37 (1997), *available at* http://www.krisdika.go.th/law/text/lawpub/e11102540/text.htm (last visited Sept. 20, 2001) (section 34 states that "the right of privacy shall be protected" and section 37 protects freedom of communications); *see also* PRIVACY INT'L, PRIVACY AND HUMAN RIGHTS 2000: COUNTRY REPORT ON KINGDOM OF THAILAND, *at* http://www.privacyinternational.org/survey/phr2000 (2000).

warrant prior to a search. A major exception to this protection however allows police to issue warrants; such warrants are not subject to judicial review.[149]

Thailand is one of the world's many countries that has no specific legislation on cybercrime. This means that it would be difficult, if not impossible, to prosecute a perpetrator of cybercrime who was located in Thailand.[150] Thailand has no specific laws that protect personal information. This means that currently the victim could not recover for losses. Realizing the need to "prevent misuse of information and give rights to data owners," Thailand officials are finalizing a data protection law.[151] In Thailand, the government has no means to prosecute cybercrime and the victim has no avenue to recover damages that result from the cybercrime. Because the goal of the Internet crime control policy is driven by concerns over morals but does not rise to the level of social control, Thailand is an example of an intermediate level of privacy protection.

3. Hong Kong: An Example of a High Level of Privacy Protection

On the political spectrum that ranges from totalitarian to liberal democracy, the Special Administrative Region of Hong Kong falls near the liberal democratic end. Until 1997, Hong Kong was part of the British Commonwealth, mirroring many British traditions including

---

[148] PRIVACY INT'L, PRIVACY AND HUMAN RIGHTS 2000: COUNTRY REPORT ON KINGDOM OF THAILAND, *at* http://www.privacyinternational.org/survey/phr2000 (2000).

[149] U.S. DEPT. OF STATE, COUNTRY REPORTS ON HUMAN RIGHTS: PRACTICES FOR 1996: THAILAND, *at* http://www.usis.usemb.se/human/1996/eastasia/thailand.html (Jan. 1997)(stating that the issuance of warrants by the police requires prior approval from the Ministry of Interior or the provincial governor).

[150] *See* Fletcher N. Baldwin, Jr., *Cybercrime: The Dawning of the Age of the Internet, in* 1 CYBERCRIME & SECURITY 17 (Alan E. Brill et al. eds., 1998)(arguing that although it is possible that Thailand has no political agenda concerning Internet crime control, it is more likely that Thailand has yet to perceive such crime as a significant threat because of the low numbers of its citizens that have access to the Internet).

democratically elected government officials and trial by jury.[152] According to the Basic Law of Hong Kong, the agreement hammered out between Great Britain and China before the 1997 handover to China, Hong Kong's form of government will remain unchanged until 2047.[153] Hong Kong remains a party to the International Covenant on Civil and Political Rights; this treaty creates an international obligation for the government to protect privacy.[154] Although there is some concern that the Chinese government will modify the policy,[155] Hong Kong's

---

[151] Karnjana Karnjanatawe, *Data Protection Laws Under Discussion*, BANGKOK POST, July 4, 2001, *available at* http://scoop.bangkokpost.co.th/bkkpost/2001/july2001/db040701/040701_database02.html.

[152] U.S. DEPARTMENT OF STATE, COUNTRY REPORTS ON HUMAN RIGHTS PRACTICES FOR 1996: HONG KONG, *at* http://www.usis.usemb.se/human/1996/eastasia/hong_kong.html (Jan. 30, 1997)(detailing Hong Kong's past).

[153] The Basic Law of the Hong Kong Special Administrative Region ch. 1, art. 5 (1990), *at* http://www.tdctrade.com/blaw/index.htm. (the Basic Law is referred to as the "mini constitution" of Hong Kong).

[154] The Basic Law of the Hong Kong Special Administrative Region ch. 3, art. 39 (1990), *at* http://www.tdctrade.com/blaw/blaw_ch1.htm (assuring that the International Covenant on Civil and Political Rights shall remain in force even though Hong Kong is now a Special Administrative Region of China); *see also* United Nations International Covenant on Civil and Political Rights (entered into force Mar. 23, 1976), *at* http://www.un.org/Depts/Treaty/final/ts2/newfiles/part_boo/iv_boo/iv_4.html (last visited Sept. 11, 2002) (China is not a signator of the treaty).

[155] *See* Steven M. Hanley, *International Internet Regulation: A Multinational Approach*, 16 J. MARSHALL J. COMPUTER & INFO. L. 997, 1012 (1998).

Even though China is not considered part of Southeast Asia, the domestic policies of China are included here because of its new governance of Hong Kong, the fourth largest financial center in the world. (Additionally, China is an undeniable force in the geographic region because of its enormous population coupled with its new-found interest in becoming a world economic power.)

Hong Kong democratic activists are concerned that China will be able to circumvent the law. China's Computer Information and Internet Security Regulations raises concerns as it provides, "These regulations [referring to the act as a whole] should be consulted with regards to the implementation of the security, protection, and management of computer information networks connecting to networks in the Hong Kong Special Administrative Region . . . ." Computer Information Network and Internet Security, Protection and Management Regulations ch. V, art. 24 (1997), *at* http://www.qis.net/chinalaw/prclaw54.htm (last modified Apr. 7, 1998).

In Chinese law, there is a provision for the secrecy of communication. In practical terms, however, this has little or no impact since the Chinese government has, for centuries, kept meticulous records on its people. PRIVACY INTERNATIONAL AND THE ELECTRONIC PRIVACY INFORMATION CENTER, PRIVACY AND HUMAN RIGHTS 2000: COUNTRY REPORT ON CHINA, *at*

general Internet policy is based on self-regulation and a concern for economic well-being.[156] As to privacy of communications, the Basic Law of Hong Kong provides for privacy of communications.[157] The law stipulates that this privacy can only be compromised through

---

http://www.privacyinternational.org/survey/index.html (last visited Sept. 20, 2001). China's newly enacted criminal procedure law provides that "when a search is conducted, a search warrant must be shown to the person searched." Criminal Procedural Law art. 111 (P.R.C.)(1996), *available at* http://product.chinawe.com/cgi-bin/lawdetail.pl?LawID=288. Seizure of the targeted items is proper when the object "may be used to prove a criminal suspect's guilt or innocence." Criminal Procedural Law art. 114 (P.R.C.)(1996), *available at* http://product.chinawe.com/cgi-bin/lawdetail.pl?LawID=288.

In an effort to modernize the country, China views the adoption of the Internet as "a necessary communication tool for successful economic competition." Scott Feir, *Regulations Restricting Internet Access: Attempted Repair of Rupture in China's Great Wall Restraining the Free Exchange of Ideas*, 6 PAC. RIM. L. & POL'Y J. 361, 361 (1997). While believing that this technology is necessary for economic development, the government is concerned that access to information is a threat to its ability to control the population. *Id.* In response to the perceived threat, the Chinese government required that a nation-wide firewall be developed – a technology that has limited information entering the country. ISPs must abide by the requirements of the Great Firewall of China. Scott Feir, *Regulations Restricting Internet Access: Attempted Repair of Rupture in China's Great Wall Restraining the Free Exchange of Ideas*, 6 PAC. RIM. L. & POL'Y J. 361, 361 (1997). China has also set up a special Internet police force to ensure compliance with its Internet policies. PRIVACY INTERNATIONAL AND THE ELECTRONIC PRIVACY INFORMATION CENTER, PRIVACY AND HUMAN RIGHTS 2000: COUNTRY REPORT ON CHINA, *at* http://www.privacyinternational.org/survey/index.html (last visited Sept. 20, 2001). China's Computer Information Network and Internet Security, Protection and Management Regulations (CINISPMR) require that Internet users register with the State security forces. Computer Information Network and Internet Security, Protection and Management Regulations art. 10, 13 (1997), *at* http://www.qis.net/chinalaw/prclaw54.htm (last modified Apr. 7, 1998).

CINISPMR protects the freedom and privacy of network users from intrusion by individuals, but provides no protection from the activity of the State. The article also requires that those who engage in Internet businesses must assist the State in "discovering" and "properly handling" law violations involving computer activities. Computer Information Network and Internet Security, Protection and Management Regulations art. 7 (1997), *at* http://www.qis.net/chinalaw/prclaw54.htm (last modified Apr. 7, 1998).
China's approach to governance restricts the rights of individuals while strengthening control by the government. The general approach to Internet policy is one of censorship, to limit access to information. *See* Steven Stanley, *International Internet Regulation: A Multinational Approach*, 16 J. MARSHALL J. COMPUTER & INFO. L. 997, 1012 (1998).

[156] Office of the Privacy Commissioner for Personal Data, Hong Kong, The Personal Data (Privacy) Ordinance, Slide 4, *at* http://www.pco.org.hk/misc/hk_apdpf/sld004.htm (Aug.3, 1995).

[157] U.S. DEPARTMENT OF STATE, BACKGROUND NOTE: HONG KONG, *at* http://www.state.gov/r/pa/ei/bgn/2747.htm (Nov. 2001).

means of legal procedures that allow for protection of public security or investigation of criminal activity.[158] With regard to government intrusion, police are required to obtain court-issued warrants before obtaining evidence.[159]

In the realm of Internet crime control policy, Hong Kong has enacted the Personal Data Privacy Act (PDPA) that regulates the collection, use, and security of personal data.[160] The PDPA covers "any data relating directly or indirectly to a living individual" if from the data it is possible to ascertain the individual's identity and if the data "is in a form in which access of processing is practicable."[161] The PDPA applies to any person who directs the collection, processing, or use of personal data.[162] The PDPA applies to both public and private sectors,

---

[158] Article 30 of the Basic Law provides "the freedom and privacy of communications of Hong Kong residents." According to the article, these rights may not be infringed "except…[by] relevant authorities [who] may inspect communications in accordance with legal procedures to meet the needs of public security or of investigation into criminal offenses." The Basic Law of the Hong Kong Special Administrative Region ch. 3, art. 30 (1990), *at* http://www.tdctrade.com/blaw/blaw_ch3.htm; *see also* PRIVACY INTERNATIONAL AND THE ELECTRONIC PRIVACY INFORMATION CENTER, PRIVACY AND HUMAN RIGHTS 2000: COUNTRY REPORT ON SPECIAL ADMINISTRATIVE REGION OF HONG KONG, *at* http://www.privacyinternational.org/survey/phr2000/countriesag.html#Heading9 (last visited Sept. 20, 2001) (stating that although Hong Kong generally protects privacy, an exception exists for crime involving organized crime because of Hong Kong's history and thus stricter measures are used in this area).

[159] Although the Independent Commission Against Corruption, a body created to address historical corruption problems, once had the independent authority to issue search warrants, it must now utilize the court system to obtain such warrants. U.S. DEPARTMENT OF STATE, COUNTRY REPORTS ON HUMAN RIGHTS PRACTICES FOR 1996: HONG KONG, *at* http://www.usis.usemb.se/human/1996/eastasia/hong_kong.html (Jan. 30, 1997).

[160] Office of the Privacy Commissioner for Personal Data, Hong Kong, Personal Data Privacy Ordinance, *at* http://www.pco.org.hk/english/ordinance/ordglance.html (Aug. 3, 1995); *see also* PRIVACY INTERNATIONAL AND THE ELECTRONIC PRIVACY INFORMATION CENTER, PRIVACY AND HUMAN RIGHTS 2000: COUNTRY REPORT ON SPECIAL ADMINISTRATIVE REGION OF HONG KONG, *at* http://www.privacyinternational.org/survey/phr2000/countriesag.html#Heading9 (last visited Sept. 20, 2001).

[161] Office of the Privacy Commissioner for Personal Data, Hong Kong, Personal Data Privacy Ordinance, *at* http://www.pco.org.hk/english/ordinance/ordglance.html (Aug.3, 1995).

[162] *Id.*

although many of the exceptions to the act apply primarily to the public sector.[163] Under the PDPA, the government can prosecute cybercrime[164] and the victim has the ability to recover damages that result from the cybercrime.[165] As the goal of Internet crime control is to root out crime without impinging on privacy protections, Hong Kong is an example of a high level of privacy protection. In Southeast Asia, Hong Kong provides significant protections for individual privacy while Singapore and, to a more limited degree, Thailand support state control to the detriment of individual privacy protections. As the Internet enables access across borders, there is a concern about how states with differing levels of privacy protections will interact under the cybercrime treaty.

C. Interactions between Southeast Asian States and a European State

The critical question to determine in deciding if the cybercrime treaty adequately protects privacy through domestic laws is whether the outcomes from interactions between states enhance or at least maintain the protections currently afforded in the states involved. In the following two hypotheticals, three Southeast Asian states will be examined in interaction with a European

---

[163] PRIVACY INTERNATIONAL AND THE ELECTRONIC PRIVACY INFORMATION CENTER, PRIVACY AND HUMAN RIGHTS 2000: COUNTRY REPORT ON SPECIAL ADMINISTRATIVE REGION OF HONG KONG, *at* http://www.privacyinternational.org/survey/phr2000/countriesag.html#Heading9 (last visited Sept. 20, 2001).

[164] "There are a variety of offences, for example non-compliance with an enforcement notice served by the Privacy Commissioner carries a penalty of a fine at Level 5 (at present $25,001 to $50,000) and imprisonment for 2 years." Office of the Privacy Commissioner for Personal Data, Hong Kong, Personal Data Privacy Ordinance (Aug. 3,1995), *at* http://www.pco.org.hk/english/ordinance/ordglance1.html#offences/ (last visited Sept. 11, 2002); *see generally* Office of the Privacy Commissioner for Personal Data, Hong Kong, Personal Data Privacy Ordinance, *at* http://www.pco.org.hk/english/ordinance/section_68.html (Aug. 3, 1995) (detailing the entire list of offenses).

[165] "An individual who suffers damage, including injured feeling, by reason of a contravention of the Ordinance in relation to his or her personal data may seek compensation from the data user concerned." Office of the Privacy Commissioner for Personal Data, Hong Kong, Personal Data Privacy Ordinance, *at* http://www.pco.org.hk/english/ordinance/ordglance1.html#offences/ (Aug. 3, 1995); *see generally* Office of the Privacy Commissioner for Personal Data, Hong Kong,

state.[166] In each hypothetical, the relevant questions to be answered are whether the evidence can be gathered, whether the accused can be prosecuted in the state, and whether the victim can recover damages. If the outcomes of these interactions enhance or at least maintain the protections currently afforded to privacy in the states involved, then the treaty has successfully increased police power while maintaining guarantees of privacy.

1. Hypothetical One: European perpetrator and Southeast Asian victims

In this first hypothetical, a European perpetrator has instigated a denial-of-service attack[167] affecting computer systems in Singapore, Thailand, and Hong Kong. All three Southeast Asian states investigate with the aim of prosecuting the perpetrator. Each state must determine if access to evidence is possible and subsequently if prosecution is possible. In addition, a determination needs to be made as to whether the victim can recover for his losses. Because the attack did not commence in Singapore, Thailand, or Hong Kong, under the cybercrime treaty the states can explore avenues to access information that both require[168] and do not require mutual assistance[169] from the European state. As to those provisions that do not require mutual assistance, the production order provision of the treaty[170] provides that law

---

Personal Data Privacy Ordinance, *at* http://www.pco.org.hk/english/ordinance/section_68.html (Aug. 3, 1995).

[166] Because of the European Union's comprehensive data protection directive, all European states have a high level of privacy protection, search and seizure by court-issued warrant, and regulation of the cybercrimes listed in the treaty. Although there are distinctions between the European states, for the hypothetical "European state" will be used to refer to an entity that promotes the general policies of any of these states. *See* Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 SAN DIEGO L. REV. 1153, 1182 (1997).

[167] A denial-of-service attack is "a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic." Webopedia, *at* http://webopedia.internet.com/TERM/D/DoS_attack.html (last modified Feb. 5, 2002).

[168] *Final Draft Convention on Cybercrime* art. 27, 31, 33, 34, *at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm/ (Nov. 23, 2001).

[169] *Id*. art. 32.

[170] *Id*. art. 18.

enforcement may gain access to data that is outside their territory if the person who owns the computer is in their territory or if the ISP concerned provides service in their territory. In this hypothetical, it is unlikely that the European perpetrator will travel to any of the effected Southeast Asian states. The provision concerning ISPs,[171] however, may be helpful in certain states. Singapore substantially restricts those who can operate ISPs in the state's territory,[172] so it is unlikely that the European perpetrator utilized an ISP from which the Singapore authorities can obtain assistance. The laws concerning ISPs in Thailand and Hong Kong are not so restrictive, so it is possible that the perpetrator will have utilized an ISP operating both in the victim state and in the European state. Noting the likely sophistication of the cybercriminal, odds favor the fact that he will have used more than one ISP to instigate the attack. If this is the case, then the authorities in Thailand and Hong Kong may be able to trace part of the path of the perpetrator, but will likely be frustrated once the perpetrator's path switches to a second ISP. Under the trans-border access provision of the treaty,[173] any of the three victim states can access information if it is publicly available on the Internet or if the perpetrator gives consent for the authorities to access the information. It is unlikely that either of these conditions will be met.

Because it is unlikely that the above mentioned treaty articles will provide access to critical evidence, Singapore, Thailand, and Hong Kong may utilize the mutual assistance articles of the treaty.[174] Singapore, Thailand, and Hong Kong will be required to satisfy the conditions provided for by the law of the European state, the state from whom the information is requested.[175] The laws of the European state require a warrant for search and seizure. Hong

---

[171] *Id*. arts. 20, 21.
[172] *See* PRIVACY INT'L, *supra* note 131.
[173] *Final Draft Convention on Cybercrime* art. 20, 21, *at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm/ (Nov. 23, 2001).
[174] *Id*. arts. 25, 31, 33, 34.
[175] *Id*. art. 25, § 4.

Kong easily meets this standard, as their domestic laws require court-issued warrants.[176] It is unclear whether Thailand's normal procedure in search and seizure cases would meet the requirement of the European state. Thailand's laws require a warrant before the search and seizure is undertaken, but in many cases the police issue the warrant.[177] Thai officials may be required to secure a warrant from a judge – a process not provided for under their domestic law. The Singapore situation is also complicated. Under Singapore's Electronics Transaction Act (ETA),[178] no warrant is required in Internet cases. Regardless of this domestic law, Singapore officials may be required to secure a warrant from a judge in order to benefit from mutual assistance.

As to collecting evidence, it is likely that Thailand and Hong Kong could retrieve data from an ISP, but less likely that the ISP used by the European perpetrator would have been one who operated in Singapore – thus decreasing the likelihood that Singapore authorities would obtain useful information from a Singapore-affiliated ISP. As for mutual assistance, Hong Kong could easily obtain mutual assistance from the European state, while Thailand and Singapore could face potentially irreconcilable complications.

If the investigations were successful, each of the victim states would desire to prosecute the European perpetrator. To do so, the individual state must have a domestic law that outlaws the specific activity in question. Thus, Thailand could not prosecute until after such time as it adopted cybercrime legislation. Because Thailand has no laws under which to prosecute, it

---

[176] U.S. DEPARTMENT OF STATE, COUNTRY REPORTS ON HUMAN RIGHTS PRACTICES FOR 1996, *at* http://www.privacy.org/pi/reports/hr96_privacy_report.html (Jan. 30, 1997)(Hong Kong).
[177] *Id.* (Thailand).
[178] *See* Electronics Transactions Act ch. 88, pt. XII, § 53 (July 10, 1998)(Sing.), *at* http://www.lawnet.com.sg/free/vldb.htm; PRIVACY INTERNATIONAL AND THE ELECTRONIC PRIVACY INFORMATION CENTER, PRIVACY AND HUMAN RIGHTS 2000: COUNTRY REPORT ON REPUBLIC OF SINGAPORE, *at*

would have to request that the European state prosecute and argue that jurisdiction was proper for the European state because the perpetrator was physically located there.[179] In contrast, Hong Kong could prosecute under its Personal Data Privacy Act[180] and Singapore could prosecute the perpetrator under its Computer Misuse Act.[181] To proceed with prosecution, Hong Kong and Singapore would need to establish jurisdiction over the European perpetrator. Under the cybercrime treaty, jurisdiction is conferred by territory,[182] among other provisions. Hong Kong would have to argue that this provision refers to the territory where the damage occurred.[183] Singapore would site its Computer Misuse Act,[184] which clarifies any jurisdictional confusion by stating that jurisdiction extends to anyone who commits a crime under the act. As to prosecution, Thailand could not prosecute while Hong Kong and Singapore could prosecute, if they could establish jurisdiction.

Regarding recovery of damages by the victim, the victim could not currently recover in Thailand because the state has no laws concerning recover for damages incurred as a result of

---

http://www.privacyinternational.org/survey/phr2000/countriesru.html (last visited Sept. 20, 2001).

[179] Both Hong Kong and Singapore would object to the assertion that the European state had jurisdiction to prosecute. Both would argue for extradition of the perpetrator to their respective state.

[180] Office of the Privacy Commissioner for Personal Data, Hong Kong, Personal Data Privacy Ordinance ch. 486, pt. IX (Aug. 3,1995), *at* http://www.pco.org.hk/english/ordinance/section_68.html (last visited Sept. 20, 2001).

[181] Computer Misuse Act ch. 50A (Sing.)(1998), *at* http://www.lawnet.com.sg/free/vldb.htm; PRIVACY INTERNATIONAL AND THE ELECTRONIC PRIVACY INFORMATION CENTER, PRIVACY AND HUMAN RIGHTS 2000: COUNTRY REPORT ON REPUBLIC OF SINGAPORE, *at* http://www.privacyinternational.org/survey/phr2000/countriesru.html (last visited Sept. 20, 2001).

[182] *Final Draft Convention on Cybercrime* art. 18, *at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (Nov.23, 2001).

[183] As stated earlier in the article, one argument regarding jurisdiction proposes that territorial jurisdiction refers to the place where the perpetrator is located. *See* Section II.C; *see generally Final Draft Convention on Cybercrime, at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (Nov. 23, 2001).

[184] *See* Computer Misuse Act, *supra* note 181.

Internet crimes. In Hong Kong, the victim has the ability to recover damages under the Personal Data Privacy Act.[185] In Singapore, the victim could recover under the Computer Misuse Act.[186] Thus, the victim in Thailand could not recover for damages while a victim in Hong Kong or Singapore likely could recover. As is demonstrated by this hypothetical, the outcomes under the treaty would vary greatly based on the domestic laws in the states.

2. Hypothetical Two: Southeast Asian perpetrators and European victim

In the second hypothetical, a European person has been the victim of cybertheft at the hands of three Southeast Asian perpetrators – one from Singapore, one from Thailand, and one from Hong Kong. The European state wants to investigate with the aim of prosecuting the perpetrator. First, the European state must determine if access to evidence is possible. Next, the state must decide if prosecution is viable. In addition, a determination needs to be made as to whether the victim can recover damages.

While the European state faces the same basic problems as those faced by the victim states in first hypothetical, the mutual assistance request sheds light on a particularly illuminating result that arises under the treaty. When requesting mutual assistance, the European state will be required to satisfy the conditions provided for by the law of the state from which it is requesting assistance.[187] The European state will successful meet the requirements of Hong Kong's domestic laws because both the European state and Hong Kong require court-issued warrants.[188] In requesting information from Thailand and Singapore, the European state will encounter a

---

[185] Office of the Privacy Commissioner for Personal Data, Hong Kong, Personal Data Privacy Ordinance ch. 486, pt. IX *at* http://www.pco.org.hk/english/ordinance/section_68.html (Aug. 3, 1995).
[186] *See* Computer Misuse Act, s*upra* note 181.
[187] *Final Draft Convention on Cybercrime* art. 25, § 4, *at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (Nov. 23, 2001).
[188] U.S. DEPARTMENT OF STATE, COUNTRY REPORTS ON HUMAN RIGHTS PRACTICES FOR 1996, *at* http://www.privacy.org/pi/reports/hr96_privacy_report.html (Jan. 30, 1997).

troublesome situation for privacy advocates. Thailand does not require a court-issued warrant[189] and Singapore requires no search warrant.[190] Thus, the European state would not be required to procure a search warrant to obtain information from Thailand or Singapore.

This second hypothetical highlights the problems associated with the treaty utilizing safeguards provided under domestic laws. As privacy advocates have lamented, the treaty lacks necessary search and seizure procedural safeguards.[191] By requiring no specified procedures in trans-border search and seizure, the treaty allows the European state to benefit from investigations undertaken without protections that would be required if the search were undertaken in the European state. The lack of required search and seizure procedures may allow a 'race to the bottom' in regards to protection of privacy. Because the outcome of an interaction between states with differing levels of domestic privacy protection likely decreases the currently provided protection in at least some of the states involved, the treaty has not successfully maintained, much less increased, guarantees of privacy while increasing police power.

IV. Why the Outcry over Privacy and Why it is Likely to Continue

A. Current International Concept of Privacy

Because the treaty affords the protections found in domestic laws as well as the protections found in international treaties, the second set of safeguards examined are provided by relevant human rights treaties. To appreciate the protections provided by international treaties, one must grasp the meaning of the term privacy and understand the specific aspects of privacy granted protection under international law. Alan Westin, one of the world's foremost authorities

---

[189] *Id.*
[190] *See* Computer Misuse Act, s*upra* note 181.
[191] "Requirements for search and seizure of stored computer data lack necessary procedural safeguards to safeguard the rights of the individual and to ensure due process of law. In particular, there is no effort to ensure that an independent judicial review." *Global Internet*

on privacy, explains privacy as "the voluntary and temporary withdrawal of a person from the general society through physical or psychological means . . ."[192] In the legal realm, this equates to "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[193] Due to the multi-faceted nature of the legal term, privacy has been divided into four general categories: privacy of association, privacy in making intimate decisions, privacy from unwanted intrusions, and privacy of personal information.[194] Associational privacy is freedom from interference of relationships with individuals or groups.[195] Decisional privacy involves freedom from interference in intimate personal decisions.[196] Privacy from unwanted intrusions relates to physical and electronic invasion.[197] Privacy of personal information concerns "the rights of individuals to control information about themselves."[198]

Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime, at http://www.gilc.org/privacy/coe-letter-1000.html (Oct. 18, 2000).

[192] ALAN F. WESTIN, PRIVACY AND FREEDOM 367 (Atheneum New York 1967).

[193] *Id.*

[194] *See* Fletcher N. Baldwin, Jr., *Impact of the Cyberspace on the Right to Privac*y, *in* 3 CYBERCRIME & SECURITY IIIA1.5 (Alan E. Brill et al. eds., 1998)(combining ideas of Constitutional and common law privacy).

[195] *Id.* at IIIA.1-6.

[196] *Id.*

[197] *Id.* at IIIA.1-5 to IIIA.1-6. Lessig suggests an alternative categorization of privacy components with three intertwined meanings. One of these meanings seeks to minimize intrusion. The test for a violation of this type of privacy is the burden of the state's intervention; if the intrusion is minimally burdensome, then the protection against the intrusion should be minimal. A second category of privacy hinges on the concept of dignity. Under this doctrine, even if the individual did not notice a search, it is nonetheless an invasion of privacy because it is an offense to dignity. The third category views privacy as a way to constrain the power of government to regulate. *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 146 (Basic Books, A Member of the Persus Books Group 1999).

[198] Baldwin, *supra* note 195, at IIIA.1-6. As to the concept of privacy generally, another explanation is that privacy incorporates "ideas of bodily and social autonomy, of self-determination, and of the ability to create zones of intimacy and exclusion that define and shape our relationships with each other." Yet another definition of privacy is "'the right of individuals' to decide for themselves how much they wish to share with others in terms of thoughts, feelings, and facts of personal life." SUSAN DRUCKER & GARY GUMPERT, REAL LAW @ VIRTUAL SPACE:

The current international understanding of privacy encompasses the protections secured in the Universal Declaration of Human Rights (UDHR) and in the International Covenant on Civil and Political Rights (ICCPR).[199] Under the UDHR, privacy of communication, freedom of expression, and criminal procedure protections are secured.[200] Privacy of communication is protected from arbitrary government interference.[201] As to freedom of expression, the UDHR protects an individual's right to hold a belief and to exchange information and ideas through any media.[202] In the area of criminal procedure protections, the UDHR protects individuals from arbitrary arrest and detention.[203] The ICCPR clarifies the general guidelines of privacy put forth in the UDHR.[204] In the ICCPR, communications are protected primarily from divulgence to anyone but the intended recipient and against interruption or interference.[205] The safeguards

---

REGULATION IN CYBERSPACE 326 (1999). In all of the conceptions of privacy mentioned in this paper, control over personal information is a component of the understanding of privacy. A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1463 (2000).

[199] Regional treaties are not here included because such treaties do not bind states that are not signatories. *Draft Convention on Cybercrime and Explanatory Memorandum Related Thereto* ¶ 110, *at* http://conventions.coe.int/treaty/EN/projets/FinalCyberRapex.htm (Nov. 8, 2001).

[200] *Universal Declaration of Human Rights*, U.N. GAOR, 3d Sess., pt. 1 at 71 arts. 12,19, U.N. Doc. A/RES/217 A (III).

[201] Article 12 of the UDHR states "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence…. Everyone has the right to the protection of the law against such interference or attacks." *Id.* at art. 12.

[202] Article 19 states, "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." *Id.* at art. 19.

[203] *Id.* at art. 9.

[204] Fernando Volio, *Legal Personality, Privacy, and the Family*, in THE INTERNATIONAL BILL OF RIGHTS: THE COVENANT ON CIVIL AND POLITICAL RIGHTS 190 (Louis Henkin ed., 1981). Article 17 states that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence . . .[and that] [e]veryone has the right to the protection of the law against such interferences or attacks." International Covenant on Civil and Political Rights, *opened for signature* Dec. 19, 1966, 6 I.L.M. 360, 373.

[205] Volio, *supra* note 205, at 197; *see* HENRY STEINER AND PHILIP ALSTON, INTERNATIONAL HUMAN RIGHTS IN CONTEXT: LAW, POLITICS, AND MORALS 529 (1996).

only apply to "arbitrary or unlawful" interference.[206] According to the ICCPR, freedom of expression is protected "regardless of frontiers."[207] However, special responsibilities are attached to the rights associated with freedom of expression, meaning that the rights may be restricted under certain circumstances.[208] Approved justifications for governments to implement laws to restrict freedom of expression include protection of national security or public order and respect for the rights of others.[209] In the criminal procedure arena, pertinent protections in the ICCPR pertain to lawful arrests, judicial control for criminal procedures concerning arrests, and judicial review of the legality of arrests.[210] This means judicial review ensures privacy protection against unreasonable intrusions by government actors engaged in investigation or arrest activities. The General Assembly of the United Nations made the provisions of the ICCPR applicable to violations by governments, businesses, and rogue individuals.[211]

When examined in light of the categories of privacy introduced at the beginning of the section, the international understanding of privacy touches all the categories but does not provide full coverage to the ideas encompassed in the categories. Both privacy of communication and freedom of expression provide some protection in the area of associational privacy by allowing an individual to maintain secret communications with groups or individuals disfavored by governments. Decisional privacy is peripherally guarded by freedom of expression because this protection allows an individual to receive or impart information concerning a sensitive decision.

---

[206] Volio, *supra* note 205, at 191. Those involved in drafting the ICCPR discussed "unlawful" as being "itself contrary to human rights" and "arbitrary" as meaning that "even when [the act] is not in violation of positive law [the act] is arbitrary or capricious." *Id.*; *see* STEINER, *supra* note 206, at 524.
[207] International Covenant on Civil and Political Rights, *supra* note 205, at 374, art.19, § 2.
[208] *Id.* at 374, art.19, § 3.
[209] *Id*.
[210] STEINER, *supra* note 205, at 156.

Privacy of communication provides some protection in the area of privacy of personal information by guarding communications from interruption or interference as well as keeping the communications from anyone except the intended recipient. Criminal procedure protections provide defense from unwanted intrusions and protect personal information by limiting a government's ability to intrude upon personal information. (See Chart 1.)

B. Privacy Concept in the Internet Age

In revisions to the treaty, the drafters added a provision that would guard human rights in accordance with currently existing protections provided in international treaties.[212] Those involved with GILC envisioned a "forward-looking" interpretation[213] of these international instruments, arguing the privacy of communication, freedom of expression, and criminal procedure protections extend to cyberspace.[214] The problem with this "forward-looking" assessment by members of GILC is that the philosophers and diplomats whose ideas shaped the current international standard did not and could not consider the vast privacy concerns associated with the Internet.

---

[211] The ICCPR Committee stated "effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it . . ." *Id.* at 529.

[212] Article 15 provides that the powers and procedures granted in the treaty ". . . shall be subject to . . . due regard for the adequate protection of human rights, in particular as provided in applicable international human rights instruments." *Final Draft Convention on Cybercrime* art. 15, *at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (Nov. 23, 2001).

[213] *Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime*, *at* http://www.gilc.org/privacy/coe-letter-1000.html (Oct. 18, 2000).

[214] *See Id.* Part II.B. The argument proposed by GILC is that the cybercrime treaty violates the guarantees of privacy of communication and freedom of expression as well as criminal procedure protections in existing international instruments. For this argument to be valid, it must first be established that these protections extend into cyberspace. This has yet to be established on the international scene. The term cyberspace "encompasses the use of electronic communications over computer networks mainly via the Internet." Jay Krasovec, *Cyberspace: The Final Frontier for Regulation?*, 31 AKRON L. REV. 101, 101, n.1 (1997).

These privacy concerns center on the collection and possible misuse of data.[215] The potential opportunities to exploit data are growing exponentially because technological developments are lowering the cost of data collection and surveillance while increasing the quality and quantity of the data.[216] In this Age of the Internet, consumers are concerned that governments are selling personal information – ranging from driver's license data, to health records, to tax documents – to make a profit[217] and that e-companies are using consumer preferences for business advantages. In essence, the all-seeing eye from George Orwell's *1984* "need not necessarily belong to the government, as many in the private sector find it valuable to conduct various forms of surveillance or to 'mine' data collected by others."[218] Today's privacy concerns encompass violations from governments, businesses, and rogue individuals.[219]

The drafters of this treaty had the opportunity to address this monumental development in the privacy arena by requiring signatory states to adopt new domestic laws guaranteeing privacy rights against governments, businesses, and rogue individuals. Although the rights would vary

---

[215] *See* Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 819 (2000); *see also* Susan E. Gindin, *Lost and Found in Cyberspace: Information Privacy in the Age of the Internet*, 34 SAN DIEGO L. REV. 1153, 1156-58 (1997).

[216] A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1463 (2000). Access is available because personal data is stored on networked computers, is collected by Web sites, and is available due to the underlying technical structure of the Internet which allows simultaneous collection and transmission of information. Schwartz, *supra* note 215, at 820;Gindin, *supra* note 215, at 1156. In addition, generation of comprehensive records of online behavior is possible. Schwartz, *supra* note 216, at 818; *see* Gavin Skok, *Establishing a Legitimate Expectation of Privacy in Clickstream Data*, 6 MICH. TELECOMM. TECH. L. REV. 61, 61 ¶ 1 (2000), *at* http://www.mttlr.org/volsix/skok.html.

[217] Andrew Ecclestone, *Freedom of Information: An Electronic Window Onto the Government*, *in* LIBERATING CYBERSPACE: CIVIL LIBERTIES, HUMAN RIGHTS AND THE INTERNET 62 (Liberty ed., 1999).

[218] Froomkin, *supra* note 217, at 1463.

[219] Lawrence Lessig, *Cyberspace and Privacy: A New Legal Paradigm? Foreward*, 52 STAN. L. REV. 987, 998-99 (2000). The concern of experts is that "traditional legal doctrines appear ill equipped to deal with contemporary [privacy] problems that originate in cyberspace." Amy E. Wells, *Criminal Procedure: The Fourth Amendment Collides with the Problem of Child Pornography and the Internet*, 53 OKLA. L. REV. 99, 99 (2000).

from state to state, this could have been a major step in protecting informational privacy,[220] which is as critically important in the Internet Age as the ability to prosecute cybercrimes.

V. Solutions for balancing the scales between police power and privacy

The cybercrime treaty addresses the need to expand police power in an age when one individual in the Philippines unleashed a computer virus[221] that succeeded in creating $8 billion worth of damage to computer systems around the world.[222] The treaty, however, creates an imbalance in the scales that weigh police power and privacy by introducing new procedural powers for police to search and seize computer data, to investigate cybercrimes outside their state, and to receive mutual assistance in cross-border investigations, without increasing protection for personal privacy.[223] Although the drafters of the treaty were "mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights,"[224] the treaty largely sidesteps this balancing act by failing to address protection of privacy in the Age of the Internet.

---

[220] *See infra* pt. V.A. (definition of this term).

[221] A computer virus is "an insidious piece of computer code written to damage systems. Viruses can be hidden in executable program files posted online." Netdictionary, *at* http://www.netdictionary.com/html/v.html (last visited Sept. 20, 2001).

[222] James Evans, *Cyber-Crime Laws Emerge, But Slowly*, *at* http://www.cnn.com/2000/TECH/computing/07/05/cyber.laws.idg/ (July 5, 2000).

[223] To increase police power in cybercrime investigations without increasing privacy protections "may result in serious disturbances of the complicated balance between the necessary powers of intervention of the [investigating and] prosecuting authorities on the one hand and civil liberties on the other hand." U. Sieber, *Computer Crime and Criminal Information Law, New Trends in the International Risk and Information Society*, Section E, Criminal Law Procedure, *at* http://www.jura.uni-muenchen.de/einrichtungen/ls/sieber/mitis/ComCriCriInf.htm (last visited Sept. 22, 2001) (on file with the Richmond Journal of Law & Technology).

[224] Preamble, *Final Draft Convention on Cybercrime* (Nov. 23, 2001), *at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm. The drafters of the treaty realized the need to include privacy protections in the treaty. Henrik Kaspersen, chairman of the Committee on Experts on Crime in Cyber-Space for the Council of Europe, said, "We do not want to leave privacy apart from the convention." *COE Cyber Crime Treaty Debated, at* http://techlawjournal.com/crime/20001208.asp (Dec. 11, 2000). Even with this realization, the drafters did not adequately address privacy concerns.

A. The theoretical answer

To understand the missed opportunity to increase privacy protection, it is necessary to examine an Internet-Age concept of privacy – informational privacy. While the general concept of privacy encompasses associational privacy,[225] decisional privacy,[226] privacy from unwanted intrusions,[227] and privacy of personal information,[228] informational privacy focuses only on the last two of these classifications. Today's most talked about privacy violations are those where e-mails are obtained by governments and where clickstreams[229] are tracked by businesses. These are violations related to how information was obtained; in these examples, information was obtained by means of unwanted electronic intrusions. In most instances, the person whose privacy was violated generated the data that was later captured. In the government invasion, the person had written the e-mails. When the business intruded, the person had created a clickstream as he viewed numerous Web pages. These unwanted electronic invasions are one type of violation of a person's privacy. Violations related to privacy of personal information are a second type common in the Internet Age; these violations pertain to a person's ability to control how information about him is used. In this category, the information may or may not have been generated by the person. An example of personal information not generated by the individual is a Social Security number. The number is assigned by the government, yet is considered to be personal information that helps to verify the identification of the individual. In this category of

---

[225] Associational privacy is freedom from interference of relationships with individuals or groups. Fletcher N. Baldwin, Jr., *Impact of the Cyberage on the Right to Privacy, in* 3 CYBERCRIME & SECURITY IIIA.1-5 to IIIA.1-6 (Alan E. Brill et al. eds., 1998).
[226] Decisional privacy involves freedom from interference in intimate personal decisions. *Id.*
[227] Privacy from unwanted intrusions relates to physical and electronic invasion. *See id.*
[228] Privacy of personal information concerns "the rights of individuals to control information about themselves." *Id.* at IIIA.1-6.
[229] A clickstream is "[t]he series of electronic footprints created when a Web user moves about in cyberspace . . . ." Gavin Skok, *Establishing a Legitimate Expectation of Privacy in Clickstream Data*, 6 MICH. TELECOMM. TECH. L. REV. 61, 61 (2000).

privacy, the information may or may not be physically controlled by the individual. An example of information not held by the person is the record of an individual's bank account, which is stored on the bank's computer system. These foregoing examples sketch an outline of aspects of informational privacy that could have been protected by the treaty.

Because informational privacy may be violated by governments as well as by businesses and rogue individuals, the concept may be divided into four categories – privacy from unwanted intrusions by governments, privacy of personal information against governments, privacy from unwanted intrusions by businesses and rogue individuals, and privacy of personal information against businesses and rogue individuals. (See Chart 2.) For each of these categories, a prominent U.S. legal scholar has written a forward-looking account that provides insight into the concept of informational privacy in the Internet Age.[230]

Justice Louis Brandeis addressed the issue of privacy from unwanted government intrusion in a U.S. Supreme Court case concerning whether such privacy protection extended to invasions that were not physical in nature.[231] Arguing in his famous 1928 *Olmstead* dissent[232] that the protection did indeed extend to non-physical invasions, Brandeis asserted, "It is not… the rummaging of his drawers that constitutes the offense, but it is the invasion of his indefeasible right of personal security, personal liberty and private property…."[233] Brandeis contended that the individual should be protected from any form of unreasonable government

---

[230] *See infra* notes 232-60.

[231] Olmstead v. United States, 277 U.S. 438, 471-78 (1928). The case centered around a conviction based on evidence gathered from a wiretap. Brandeis' argument was based primarily on the Fourth Amendment of the United States Constitution. In particular, his assertion was based on the provision that states, "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated…" *Id*. (quoting U.S. CONST. amend. IV.).

[232] *Id*.

[233] *Id*. at 474-75. This proposition asserted by Brandeis in 1928 was not adopted by the United States Supreme Court until *Mapp v. Ohio*. Mapp v. Ohio, 367 U.S. 643, 659 (1961).

intrusion because the privacy protection stemmed from a person's most basic right, the right to be left alone.[234] He argued that government violated this fundamental right of privacy with every unjustified intrusion, regardless of the means that might be developed to effectuate the invasion.[235] In the dissent, Brandeis' foreshadowed government invasion of e-mail messages by suggesting that, in the future, the government would be able to reproduce personal information in court without removing the papers from the person's house.[236] Brandeis' forward-looking legal thinking laid the groundwork for the assertion that individuals have a right against unreasonable electronic intrusion by government.[237]

A second category of informational privacy focuses on yet another right against unreasonable government imposition. Justice William Brennan discussed this second category, privacy of personal information against government, in his dissent in the 1976 U.S. Supreme Court case of *United States v. Miller*.[238] The case centered on whether the defendant had a right of privacy in personal information that was not under his physical control; in this case the data had been technologically captured[239] in bank records.[240] Even though the individual had physically released the information from his control, Brennan argued that the defendant had a

---

[234] "The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. . . . They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against Government, the right to be let alone – the most comprehensive of rights and the right most valued by civilized men." *Olmstead,* 277 U.S. at 478.
[235] "To protect that right [the right to be let alone], every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment." *Id.*
[236] "Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court." *Id.* at 474. "Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet." *Id.* at 473.
[237] *See* ALAN F.WESTIN, PRIVACY AND FREEDOM 370-77 (Atheneum New York 1967).
[238] United States v. Miller, 425 U.S. 435, 447-56 (1976).
[239] The bank maintained most of the records on microfilm. The bank made copies of deposit slips and checks. *Id.* at 438.
[240] *Id.* at 441-42.

reasonable expectation that the data would remain confidential between the bank and him,[241] unless the government provided sufficient documentation to garner a warrant or subpoena.[242] Brennan warned that the door had been opened for abuse of government power because the Court had affirmed the government's obtaining the information at issue without first demonstrating to a judicial official the need for such information.[243] His concern was that unfettered government access to personal information could be used to create a "virtual . . . biography," which could reveal "many aspects of … [a person's] affairs, opinions, habits, and associations."[244] Brennan advocated for a right against unreasonable invasion of personal information by government.

While forward-looking discussions of the two categories of informational privacy that address government violations arose in U.S. Supreme Court cases, discussions of these categories of informational privacy in relation to violations by businesses and rogue individuals appeared in two preeminent journal articles. In an influential piece on privacy, William Prosser[245] explained the tort of unwanted intrusion by businesses and rogue individuals.[246] Prosser agreed with Brandeis' assertion that the invasion need not be physical in nature[247] and outlined a two-part test for violation of the tort. First, he asserted that there must be prying, meaning that the intrusion must be of a nature that would be offensive to a reasonable person.[248]

---

[241] *Id.* at 448-49.
[242] *Id.* at 441.
[243] "To permit a police officer access to these records merely upon his request, without any judicial control as to the relevancy or other traditional requirements of legal process, and to allow the evidence to be used in any subsequent criminal prosecution against a defendant, opens the door to a vast and unlimited range of very real abuses of police power." *Id.* at 451.
[244] *Id.*
[245] Prosser was the former Dean of the University of California School of Law at Berkeley.
[246] Prosser classified four torts: intrusion, public disclosure of private facts, false light in the public eye, and appropriation. William Prosser, *Privacy*, 48 CAL. L.REV. 383, 389-407 (1960).
[247] *Id.* at 390.
[248] *Id.* at 391.

The second requirement explained by Prosser was that the information at issue must be entitled to be private, meaning that there be no legal requirement that it be public and that it not be public information.[249] Prosser's work advocated for the torts of privacy, particularly the tort of unwanted intrusion by businesses and rogue individuals.

Louis Brandeis and Samuel Warren wrote the seminal article on the issue of privacy in 1890.[250] Brandeis and Warren spoke of the right to keep information about oneself out of the public eye.[251] Although much of the focus was on publicity afforded to the creations of an author,[252] Brandeis and Warren stepped beyond this narrow focus. The two declared that protection should be afforded to information that concerns the "private life, habits, acts, and relations of an individual."[253] Their advocacy was for the protection of privacy of personal information against businesses and rogue individuals. In their scheme, recovery from businesses and rogue individuals would be provided through tort law.[254] The outcome of the tort action would be driven by the facts of the specific case[255] and would be balanced against the demands of public welfare and private justice.[256] As in the case of unwanted invasion by government,

---

[249] *Id.*
[250] Louis Brandeis & Samuel Warren, *The Right to Privacy*, 4 HARV. L. REV. 195 (1890). For a discussion of the article, see Fletcher N. Baldwin, Jr., *Impact of the Cyberage on the Right to Privacy*, *in* CYBERCRIME & SECURITY IIIA.1-3 (Alan E. Brill et al. eds., 1998) and William Prosser, *Privacy*, 48 CAL. L. REV. 383, 383-84 (1960).
[251] "In every such case the individual is entitled to decide whether that which is his shall be given to the public." Louis Brandeis & Samuel Warren, *The Right to Privacy*, 4 HARV. L. REV. 193, 199 (1890). The authors refer to a right not to publish, which is equated with a right to keep certain information from the public. *Id.* at 212.
[252] "No other has the right to publish his [the author's] productions in any form, without his consent. This right is wholly independent of the material on which, or the means by which, the thought, sentiment, or emotion is expressed." *Id.* at 199. "The principle which protects personal writings and any other productions of the intellect or of the emotions, is the right to privacy…." *Id.* at 213.
[253] *Id.* at 213, 216.
[254] *Id.* at 219.
[255] *Id.* at 215-16.
[256] *Id.* at 214.

Brandeis envisioned privacy of personal information as part of "the more general right of the individual to be let alone."[257]

While Brandeis linked the differing aspects of privacy under the umbrella term of the right "to be let alone,"[258] this section has laid out the aspects of another umbrella term, informational privacy. In the preceding paragraphs, protection of informational privacy from violation by government has been explored as a right[259] while tort law[260] has been examined as a means to address violations by businesses and rogue individuals. Unfortunately, the drafters of the treaty simply failed to address any protection of informational privacy.

B. The Practical Balancing Act

The particular increase in government police power provided for under the treaty will result in the loss of particular types of privacy for all individuals. Under the treaty, an individual's expectation of privately storing data in computer systems will be lessened because such data will be available for search and seizure in criminal investigations.[261] Anonymity of communications will also likely be compromised. To rebalance the scales between police power and privacy, a guaranteed protection of individual privacy needs to offset the increase in police power. As additional police power was called for because of the nature of the Internet, an increase in privacy protection is warranted in Internet-related activity to rebalance the police

---

[257] *Id.* at 205.
[258] Olmstead v. United States, 277 U.S. 438, 478 (1928); Louis Brandeis & Samuel Warren, *The Right to Privacy*, 4 HARV. L. REV. 195, 205 (1890).
[259] "Right" defined as "a legally enforceable claim that another will do or will not do a given act; a recognized and protected interest the violation of which is a wrong." BLACK'S LAW DICTIONARY 1322 (7th ed. 1999).
[260] "Tort" defined as "a civil wrong for which a remedy may be obtained, usually in the form of damages . . . . " BLACK'S LAW DICTIONARY 1496 (7th ed. 1999).
[261] This will be true regardless of whether the data is physically located within the state where the investigation is taking place. *See Final Draft Convention on Cybercrime* art. 26, 31, 33, 34, *at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (Nov. 23, 2001).

power/privacy scales. Particularly, the offsetting measure should involve increased informational privacy protection for individuals against unwanted invasion, whether by governments, businesses, or rogue individuals.

While the ideal solution to the issue of informational privacy would be for all states to adopt domestic legislation that protected individuals from unreasonable invasions by governments, businesses, and rogue individuals, it is impractical to believe that every state would currently adopt such a policy.[262] The best alternative available would have been for the drafters to have advocated for increased privacy protections in those states that were willing to adopt an informational privacy system while assuring that at least some minimal protections were guaranteed in all states that become parties to the cybercrime treaty.

In those states that are interested in protecting informational privacy, a system that provides a remedy for invasion would best protect the individual. While some argue that the content of cyberspace should be regulated,[263] it makes little sense to argue for such a scheme when discussing personal data. Personal data may be used in as many ways that may benefit the individual as that may harm the individual. Thus, to require that personal data be removed from cyberspace would create an unmanageable system. Instead, the individual should be guaranteed the right to pursue legal action against governments, businesses, and rogue individuals when

[262] The drafters found it impossible to include one international standard for privacy protection in the treaty. Margret Johnston, *US Companies Find Europe's Cyber Crime Treaty Too Vague: Americans Fear Individual Countries' Due-process Laws Could Be Violated*, IDG News Service, *at* http://www.e-businessworld.com/english/crd_treaty_321309.html (Dec. 8, 2000)(on file with the Richmond Journal of Law & Technology).

[263] In essence the argument is that it should be a crime for certain information to be on the Internet. A competing theory is that sanctions should only apply to the individual who places the information onto the Internet or who retrieves the information from the Internet.

personal information is used in unacceptable ways.[264] The particulars of this system would be developed through domestic law.

For those states that are not willing to guarantee this level of informational privacy, the treaty should have, nonetheless, required some level of protection. Henrik Kaspersen, chairman of the Committee on Experts on Crime in Cyber-Space for the Council of Europe, explained that the drafters did not want to leave privacy out of the treaty but found it impossible to include one international standard for privacy protection.[265] As such, the goal should not been one world standard but an incremental increase from the level of informational privacy protection currently provided by each state. This increase in informational privacy would have been an important step in rebalancing the police power and privacy scales of justice.

Conclusion

Today, cyberspace allows for many of the same activities as Main Street. Individuals can engage in cybershopping, cyberdating, and cyberlearning. As with Main Street, however, there is also a sinister element at work that is engaged in cybertheft, cyberfraud, and cyberdamage. To deal with these new cybercrimes, law enforcement officials require increased powers to investigate crimes involving computers systems. The cybercrime treaty will provide law enforcement with these needed powers. Such an increase in police power raises concerns about privacy protections. A treaty provision that ensured an incremental increase in informational privacy would have been an important step in allaying privacy concerns. As the treaty stands,

---

[264] *See* Gavin Skok, *Establishing a Legitimate Expectation of Privacy in Clickstream Data*, 6 MICH. TELECOMM. TECH. L. REV. 61, 82-83 (1999/2000); Susan Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 SAN DIEGO L. REV. 1153, 1182 (1997).

[265] Margret Johnston, *US Companies Find Europe's Cyber Crime Treaty Too Vague: Americans Fear Individual Countries' Due-process Laws Could Be Violated,* IDG News Service, *at* http://www.e-businessworld.com/english/crd_treaty_321309.html (Dec. 8, 2000)(on file with the Richmond Journal of Law & Technology).

individuals must rely on domestic laws and international treaties for protection. Without new domestic laws and revitalized interpretations of old international human rights treaties, the provided protections may prove to be paltry.