Communications of the IIMA

Volume 6 | Issue 1 Article 4

2006

Are Cybercrime Laws Keeping up with the Triple Convergence of Information, Innovation and Technology?

Ramesh Subramanian
Quinnipiac University

Steven Sedita
Quinnipiac University

Recommended Citation

Subramanian, Ramesh and Sedita, Steven (2006) "Are Cybercrime Laws Keeping up with the Triple Convergence of Information, Innovation and Technology?," *Communications of the IIMA*: Vol. 6: Iss. 1, Article 4.
DOI: https://doi.org/10.58729/1941-6687.1293
Available at: https://scholarworks.lib.csusb.edu/ciima/vol6/iss1/4

Are Cybercrime Laws Keeping up with the Triple Convergence of Information, Innovation and Technology?

Ramesh Subramanian
Information Systems Management Department
Quinnipiac University School of Business
275 Mount Carmel Avenue
Hamden, CT 06518
Phone: 203-582-5276 Fax: 203-582-8664
Ramesh.Subramanian@quinnipiac.edu

Steven Sedita
Information Systems Management Department
Quinnipiac University School of Business
275 Mount Carmel Avenue
Hamden, CT 06518
Phone: 203-582-5276 Fax: 203-582-8664
Steven.Sedita@quinnipiac.edu

ABSTRACT

This paper analyzes the emergence and development of cyberlaws. In many countries around the world, cyberlaws are being enacted in order to curb or prosecute cybercriminals. Cybercriminals have very rapidly adapted to developments in technology, specifically Internet technology, and use its characteristics of transience, anonymity, speed and vast spread to perpetrate various types of crimes. Thus the triple convergence of information, innovation and technology has also aided criminals to practice their nefarious "trade." The paper analyzes how various countries are taking counter measures by enacting cyberlaws. These actions are often slow and reactive rather than proactive. In addition, the laws often have several gaps which are further manipulated by criminals. The paper analyzes the cyberlaws of the US and EU. Points of confusion, complexity and differences between the US and EU laws are discussed. The paper concludes with some ideas to be considered in enacting such laws, as well as directions for future research.

Keywords: Cybercrime, cyberlaws, Internet, US laws, EU laws, criminal justice

INTRODUCTION

The last decade of the twentieth century was the decade of the "public" Internet. The Internet, which was until then primarily used by academic institutions and the military, became vastly accessible to the public with the invention of the world-wide web (web) by Tim Berners-Lee. Berners-Lee built the first web site in 1991 while working at the European Organization for Nuclear Research (or CERN) in Geneva, Switzerland. This started a world-wide trend in developing web sites not only for personal and research purposes, but for information dissemination by governments and as a tool for electronic commerce by commercial organizations situated around the world. Thus the Internet, with its "killer application," the web, heralded the furious pace of globalization in the 1990s. But the popularity and ease of use of this technology also attracted criminals and fraudsters who rapidly adapted to the technology, using its anonymity and global reach to perpetrate crimes directed not only at private citizens but also against governments and nations. The advent of Internet-based crimes has spawned new vocabulary such as "cyberspace," "cybercrime," "cyberlaw," "cyber terrorism" and "identity theft." The term "cyberspace" was originally coined by science fiction author William Gibson in his 1984 novel *Neuromancer*. It refers to the on-line, virtual world that one enters when accessing the Internet. "Cybercrime," which originates from "cyberspace," is "a term used broadly to describe criminal activity in which computers or communications networks are the tools, targets, or places of criminal activity" (from "Cybercrime," 2006, para # 1).

In this paper we are interested in analyzing the current state of cyberlaws, with a view to determining if such laws have kept up pace with the triple convergence of information, innovation, and technology. We therefore discuss the emergence and development of cyberlaws by analyzing some of the nuances of the laws, their complexities, and difficulties in implementing or prosecuting cybercriminals. Our focus is primarily from a US and EU standpoint. The paper is organized as follows: in the next section we briefly categorize the types of cybercrimes. Following that we divide the paper into two main sections – one focusing on the US approach to cybercrime and cyberlaw, and the second pertaining to the EU context. We also focus on the differences with which specific jurisdictional issues such as pornography, privacy and IP protection are treated within the US and EU legal systems. Finally, we present our analysis and conclusions.

CATEGORIZING CYBERCRIMES

Cybercrime covers a wide swath of area, and can be categorized loosely into the following areas (adapted from "Cybercrime," 2006, para 2,3,4,5):

- Computers and networks as the **tools** of criminal activity. Examples: spamming, IP and copyright-related crimes, crimes committed through peer-to-peer networking.
- Computers and networks as the **target** of criminal activity. Examples: unauthorized access, denial of service, attacks using malicious code.
- Computers and networks as the **place** of criminal activity. Examples: computer-based frauds such as financial fraud.
- Computers and networks as new **facilitators** for older crimes. Examples: child pornography, Nigerian 419 schemes, online gambling, phishing, espionage, terrorism.

In addition, Kerr (2003) categorizes computer crimes as:

- Traditional crimes committed using computers (E.g. Internet fraud schemes, Internet gambling, online distribution of child pornography and cyberstalking), and
- Crimes of computer misuse (E.g. computer hacking, distribution of worms and viruses and denial-of-service attacks).

THE AMERICAN JUSTICE SYSTEM, CYBERLAWS AND PENALTIES

The American justice system can be generalized into two parts: one addresses criminal offenses and the other addresses civil offences. In order to prove a criminal offense three factors must be established: (1) Actus Reus (a guilty act), (2) Mens Rea (a guilty mind), and (3) the appropriate circumstances. These three factors need to be proven in order to convict a defendant of a criminal act. Civil offences include torts or breach of contracts. Criminal offenses are handled by criminal law and include two types: (1) statutory and (2) common law. Statutory law is written by legislature and ratified. Common law is refined and distinguished by the justice system itself through precedence. Based on common law, computer fraud is still fraud – it is just executed with a different medium. As new crimes emerge, new laws may have to be enacted to address them (Legislative Branch, 2006).

Federal and State Laws In the US Legal System

The judicial power of the Federal courts "extend to cases arising under the Constitution, an act of Congress, or a treaty of the United States; cases affecting ambassadors, ministers, and consuls of foreign countries in the United States; controversies in which the U.S. government is a party; controversies between states (or their citizens) and foreign nations (or their citizens or subjects); and bankruptcy cases" (Legislative Branch, 2006).

The state governments have the greatest influence over most Americans' daily lives. Each state has its own written constitution, government, and code of laws. There are sometimes great differences in law and procedure between individual states, concerning issues such as property, crime, health, and education (State, tribe and local governments, 2006).

US Computer Fraud Laws

Before the advent of the Internet, creating a virus and hacking was not classified by law. The earliest hackers belonged to the "414-gang" named after a telephone area code in Wisconsin. The 414 gang started hacking into computers from 1980 onwards and were arrested in 1983 by the FBI after hacking into the computers of the Los Alamos National Laboratory and New York's Sloan-Kettering Cancer Center in 1982. This was the earliest case of "hacker arrest" in the US (PC World Staff, 1999). This was when the world first came to understand the threat posed by hackers. This threat spurred enactment of new laws. One of the first computer protection acts was the Computer Fraud and Abuse Act (CFAA) 1984 later revised as the CFAA 1986. The CFAA was designed to protect against malicious acts and unauthorized access. Unauthorized access under the CFAA was classified as a situation where a user exceeded the access and use rights authorized to him/her. The CFAA also addressed Denial-of-service (DOS) attacks. If the DOS attack resulted in a loss of $1,000 or more the offender could be brought up on civil charges. The CFAA also stated that for a crime to be committed, simple unauthorized access was enough – there did not have to be any malicious intent. This act is the basis of all cyber crime acts that have since come into existence. Table 1 gives a summary of the CFAA.

Jurisdiction

In order for prosecution to take place the applicable court must have jurisdiction over the parties involved. "Jurisdiction" simply means the place where the crime was initiated. This concept becomes difficult to define when the offending parties could be scattered around the country, as often happens in cybercrimes. The prosecuting court must have two types of jurisdiction over the parties for a trial to be held: subject matter and personal jurisdiction. Subject matter jurisdiction dictates which type of dispute can be brought before a particular court. Typically, state courts handle any type of lawsuit that pertains to citizens of the same state. Federal courts, on the other hand, handle lawsuits that pertain to federal laws and inter-state lawsuits. However, to complicate matters, there are certain state courts that handle cases of general jurisdiction - i.e., any sort of dispute between any parties. Federal courts thus have only limited jurisdiction. Personal jurisdiction gives the court the power to enforce judgment over specific defendants. In civil cases, the two issues are: which state does the defendant belong to, and what is the constitutional appropriateness of extending the arm of a court to reach into another state to enforce a judgment on a defendant. The first issue above suggests that the offending parties should have committed the offence in the same state. However, this is a problem when the offense is committed through a medium such as the Internet (i.e., not in the same state). The state court thus needs to have the ability to prosecute out of state offenders. The way in which they gain jurisdiction over an out of state entity is by means of the long arm statute. This statute allows the court to impose jurisdiction over a party that had sufficient contact with a resident of their state. What constitutes the adequate level of minimum contact is up to the individual states and is limited by the constitution. This leaves a lot to be determined before a venue can be decided. Traditional crimes (even if done over the internet) are resolved easily. For example, if a hacker is in one state and commits fraud in another state, they are liable in the state they live for hacking and fraud, but they are also guilty of the same offense in the other state and since it crossed state lines the venue could be held in federal court too. It is up to the courts to pick one of the three venues for the trial, usually the court that has the best chance for a conviction is the chosen one. But when new cyber crimes arise that do not meet the criteria new laws need to be changed or adopted to stop these new crimes (adapted from Casey, 2004 pp42-45). The issue of jurisdiction has come up repeatedly in US courts on the issue of pornography, obscenity and child pornography, which we discuss in the next section.

Pornography

In the American legal system, the issue of pornography comes under the freedom of speech, protected under the First Amendment of the constitution. However, it should be noted that pornography is considered different from obscenity, and the latter is not protected under the First Amendment.

Section	*Summary*	*Penalties*
Section (a)(1)	Obtaining unauthorized access to information regarding national defense, foreign relations, and atomic energy.	A fine and/or up to 10 years imprisonment for a first offense and up to 20 years for subsequent offenses.

Section (a)(2)	Obtaining unauthorized access to records from a financial institution, credit card issuer, or consumer reporting agency.	A fine and/or up to 1 year imprisonment for a first offense and up to 10 years for subsequent offenses.
Section (a)(3)	Interfering with government operations by obtaining unauthorized access to their computers or computers that they use.	A fine and/or up to 1 year imprisonment for a first offense and up to 10 years for subsequent offenses.
Section (a)(4)	Obtaining unauthorized access to a Federal interest computer to commit fraud or theft unless the object of the fraud and the thing obtained consists only of the use of the computer.	A fine and/or up to 5 years imprisonment for a first offense and up to 10 years for subsequent offenses.
Section (a)(5)(A)	"Whoever ... through means of a computer used in interstate commerce or communications, knowingly causes the transmission of a program, information, code, or command to a computer or computer system with reckless disregard of a substantial and unjustifiable risk that the transmission will damage, or cause damage to, a computer, computer system, network, information, data, or program; or withhold or deny, or cause the withholding or denial, of the use of a computer, computer services, system or network, information, data, or program" provided the access is unauthorized and causes loss or damage of $1,000 or more over a one year period or "modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals."	A fine and/or up to 5 years imprisonment for a first offense and up to 10 years for subsequent offenses.
Section (a)(5)(B)	Whoever ... through means of a computer used in interstate commerce or communications, knowingly causes the transmission of a program, information, code, or command to a computer or computer system if the person causing the transmission intends that such transmission will damage, or cause damage to, a computer, computer system, network, information, data, or program; or withhold or deny, or cause the withholding or denial, of the use of a computer, computer services, system or network, information, data, or program" provided the access is unauthorized and causes loss or damage of $1,000 or more over a one year period or "modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals."	A fine and/or up to 1 year imprisonment.
Section (a)(6)	Trafficking in passwords that affect interstate commerce or involve the password to a computer that is used by or for the US government	A fine and/or up to 1 year imprisonment for a first offense and up to 10 years for subsequent offenses.

Table 1: Summary of the Computer Fraud and Abuse Act of 1986 (From Casey, 2004, pp. 64).

Thus, the issue then becomes how should a court decide which is pornography, and which is obscenity. In the American system, this issue is left to the local standards of the community to which the specific court belongs. Thus, what is considered obscene in one state may not be considered that in another State. This raises a great deal of jurisdictional confusion when pornographic or obscene content is transmitted through the Internet.

The issue of indecent content transmission has been addressed in the US legislature several times, especially via the Communications Decency Act (1996). However, this Act has run into trouble in the form of court challenges because of the lack of a clear definition of the terms "indecent" and "patently offensive." It is also important to note that it is legal to possess "indecent content "in one's computer, but it may be illegal to transmit such content in certain states where that content may be deemed obscene. Thus, there is a likelihood that one would not know if the material falls under pornography or obscenity unless it is transmitted, at which point it is "too late" from the point of view of the transmitter (Miller v. California, in Casey, 2004, p46).

Due to the inherent confusion that reigns with regards to pornography and obscenity, US lawmakers have tried to focus on child pornography, which seems, at least at the outset, more clear-cut in its definition and universal unacceptability. In 1998 the Child Online Protection Act (COPA) was passed. Under this law, it is illegal even to possess child pornography on one's computer. However, this law has also been challenged in the courts by the American Civil Liberties Union, which took issue with COPA's definition of "material that is harmful to minors." The major problem seems, again, to be the issue of which state or community will accept some content, and which will not, under the definitions proposed. The US Supreme Court remarked in Ashcroft vs. ACLU et al (2002) that while the law may be constitutional, it may not be easily implemented and remanded the case to further action by the District Court and Court of Appeals. This leads us to the conclusion that while the US courts are generally moving in the direction of defining and establishing precedents for prosecuting pornography, child pornography and obscenity in the courts. This area is still emerging.

Privacy

Privacy is a tricky issue to deal with. Before the advent of technology, the right to privacy was relatively sound. An individual could expect a reasonable amount of privacy from individuals and privacy from unreasonable searches from the government (4th amendment). The common law "right to privacy" as described by Casey (2004, p. 51) states that,

1. Appropriation of a person's name or likeness for the defendant's benefit.
2. Unreasonable intrusion, defined as intentional interference with another person's interest in solitude and seclusion.
3. Public disclosure of private facts.
4. False light, that is, publicity which presents a person to the public in a false light.

Before the development of computers and Internetworking, an individual would have to be quite intrusive to violate these common laws. So the expectation of privacy was high. The Internet is, however, is a very accessible, ubiquitous technology that can be used to find private information about any citizen. In California v. Greenwood, Greenwood's garbage was searched upon a tip that he was operating a drug business. The trash was left on the curb and was searched without a warrant. The search of the trash turned up drug paraphernalia. With that evidence in hand, a warrant was issued for his home and a drug factory was discovered inside. He was convicted and later appealed saying it was an invasion of privacy to search the trash without a warrant and any choices made on those findings were unconstitutional. The court affirmed that there was no expectation of privacy for things left out that the public could access, and therefore privacy did not apply to the trash left for the public to see. This case is the basis for the reason why privacy is a thing of the past. This ruling is applicable to current computer technology. Private information left out in a public domain is fair game. Whether it is trash on the curb or a web site, it will be viewed as the same.

Another case that illustrates the loss of privacy is Kyllo v. United States. It was believed that Kyllo was operating a drug factory. The agents used thermal imaging devices from the street to detect any hot spots in his home. Once the hot spots were seen they were issued a warrant and the premises were searched. Kyllo was found to be growing marijuana and the hot spots were the sun lamps used to grow the drugs. Kyllo appealed his conviction saying that it was unreasonable to be issued a warrant on the basis of the thermal imaging. The appeal was overturned and it was stated that the thermal imaging was in general public use and available to anyone therefore it can be used by the agents. This case shows how public technology can be used to gain information about private individuals. Over time the US government has gained even more leeway when conducting warrant-less searches. The USA Patriot Act allows government and state entities to monitor and search to a large degree before needing a warrant. "While it is important to understand that the 'right of privacy' is protected by common law and statutes, for the purposes of criminal law, ... the focus is on our privacy protection as it is embodied in the US Constitution. The word 'privacy' does not appear in the Constitution and the right of privacy in this context is largely a separate body of law

developed over many years through interpretations and analysis of the Fourth Amendment, which prohibits 'unreasonable searches and seizures.' It turns out that our right of privacy has a lot to do with our expectations and how reasonable they are." (Casey, 2004 pp52).

The previous cases help illustrate the direction in which the American legal system is going. Since these cases were affirmed a new precedent was set and the government can follow suit by applying these to emerging technologies. Despite this gradual loss of privacy in the US, a case can be made that the loss of privacy does have some benefits. It is harder for criminals to go unnoticed when privacy is low. This is the basis of cybercrime prevention.

There has been a long debate in the US legislature on how to thwart cybercrime and there is no clear answer. Laws are adopted and shaped as crimes progress into new areas, or new crimes emerge. It is the proverbial cat and mouse game and law enforcement has to be one step ahead of the game. The United States is one of the foremost experts in the prevention of cybercrime and the vast majority of foreign nations look to America as an example on how to protect a nation's infrastructure.

Copyrights and Intellectual Property Protection

The protection of intellectual property (IP) is enshrined in Article I Section 8 of the US Constitution. The US Copyright Act of 1976 grants several rights to the owner of a copyright. A copyright is automatically created if a work is an original expression that is fixed in a tangible form. With the advent of the Internet, violations of digitized data have become easy. Copyright laws have been invoked in several cases by owners of copyrights to prove that the posting of copyrighted images on public-access or subscription based web sites exceed the "fair use" doctrine (e.g., Playboy Enterprises Inc. v. Ferna). In this instance Ferna provided copyrighted images from Playboy on a member-only bulletin board which could be downloaded by the members. In other cases, copyright laws have had to be augmented to in order to prosecute new types of copyright violations that have emerged along with the Internet. For example, in 1994 David LaMacchia of MIT was indicted for running an electronic bulletin board which aided the copying of proprietary software. His case was dropped, however, because David did not charge for the use of the bulletin board. In response, the No Electronic Theft Act was passed in 1997 which removed the requirement of profit motive in prosecuting copyright violations. In the year 2000, Napster, a service that enabled members to share copyrighted music, was shut down by a federal district court, because Napster users were not engaging in personal use of the music they owned, but were trading them with thousands of strangers.

Thus we notice that laws concerning copyrights have had to change along with developments in technology. In the next section we will examine cyber crime laws in the European context.

THE EUROPEAN CONTEXT: CYBER LAWS AND PENALTIES

The European Union was officially created in 1992 with the signing of the treaty of the European Union (the Maastricht treaty). As of May 2004, the EU had twenty five countries in its membership. The EU was created to oversee health and economic policy, foreign affairs, and defense. In the EU, laws are voted upon and once the law is adopted it is up to the individual country to enforce that particular law. This process allows for continuity among member states but they retain a unique independence.

The Legislative System under the EU

The EU has many divisions similar to the American legislative system but the three main legislative branches of the EU are the European parliament, European court of justice, and the European commission. These three entities are primarily responsible for the creation of law and policy. The European parliament currently has 732 members that are elected democratically every five years. The European parliament works in conjunction with the council of ministers to impose legislation. The European parliament cannot create new legislation but it can amend or reject legislation brought upon it for review. The European court of justice consists of 25 judges and 8 advocate generals. The court of justice is similar to the US supreme court, where appeals are sent up to the court of justice for review. In addition to the review of cases the court of justice monitors the member states to ensure its compliance with EU laws and regulations. The European court of justice has many other functions but these are the main parts for the construction of law. The last major component to the law making process of the European Union is the European commission. The European commission creates legislation for EU member states. The commission has 25

members (one from each member state). These three parts are the main components to the creation and management of EU law and policy.

The members of the EU are obligated to adopt laws agreed upon, but developing the laws can be an arduous task. All members of the EU have to ratify a treaty in order for the legislation to take affect. This is far from a simple process. There are twenty five members of the EU all with similar but still different goals. So legislation can take years to pass. This means that EU imposed law is difficult to pass but this does not mean the country doesn't already have a cybercrime law in effect.

EU Cybercrime Laws and Privacy

Most European nations have a version of cybercrime law but it may be below the standard required to maximize protection. The EU is focused on the citizens' right to have fluid movement of communication and privacy. This is good for freedom but it allows for criminals to prosper. "Protection of privacy is a key policy objective in the European Union. It was recognized as a basic right under Article 8 of the European Convention on Human Rights 20 (Hellenic Resources Institute, 1995). Articles 7 and 8 of the Charter of Fundamental Rights of the European Union 21 also provide the right to respect for family and private life, home and communications and personal data" (COMMISSION OF THE EUROPEAN COMMUNITIES, 2001, pp. 24). One of the major goals of the EU is to create an interconnected network among member states. This goal has in its core, the matters of economics and defense. But the member countries have been slow to adopt cybercrime laws, which is quite problematic. The Internet is inter-connecting the EU so that the differences between the members become completely transparent to its citizens. This is a goal of the EU but the absence of a universal cybercrime law allows criminals to remain in a gray area and remain hidden. The EU values privacy, and thus deemed that privacy would eventually be beneficial to economic development. But it could be argued that tightening the privacy laws in conjunction with a new founded cooperation among EU member states will work better at securing the rights of the EU citizens and further facilitate growth. E-commerce is at an all time high and securing systems will raise the confidence in this technology, which in turn will foster further economic development. But as it stands now the EU is in litigation over an imposed cybercrime law and it is up to the individual countries to develop the law and share information. "To date, national laws have been developed autonomously. This means that, while some countries have preferred to amend their penal or criminal code, other countries have decided to pass specific laws on cybercrime (not included in the penal/criminal code). There are even some countries that do not have legal provisions regarding cybercrime at all – either in their penal/criminal code, or in the form of special laws. (Rand Europe, 2002, pp23" The legal framework existing at an international level in the area of cybercrime remains confused. There is wide agreement on the need to harmonize national legal provisions and to enhance judicial and police cooperation, but there are still many obstacles that hamper the achievement of concrete results. Nonetheless, the need to prevent and control cybercrime in order to enhance the development of an Information Society is a priority on the agendas of almost all national and international institutions. Therefore, there are good prospects for improved harmonization and cooperation in coming years" (Rand Europe, 2002, pp16). Once universal cybercrime legislation is in place the interconnection between member states will increase due to increased security and communication.

Jurisdiction

According to the European Convention's (2001) article 21 (Council of Europe, 2001), each "party" (i.e. nation or state) has an implied jurisdiction over any offence established in Articles 2 through 11 of the Convention (please see "Convention on Cybercrime," November 2001, referenced by Council of Europe (2001) when the offence is committed:

1. in its territory
2. on board a ship flying the flag of that Party
3. on board an aircraft registered under the laws of that Party; or
4. 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.

Each party, however, has the right not to apply or to apply, in specific cases, the jurisdiction given by the above paragraphs. In cases where an offender sought by another party (i.e., an extradition request has been made) is present in its territory, and it does not extradite him/her based on his/her nationality, then it is its responsibility to adopt whatever measures are required to establish its jurisdiction over the offenses concerned.

This Convention includes any criminal jurisdiction exercised by a Party in accordance with its domestic law. The Convention further states that 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.

Problems of Implementing Cybercrime Laws in the EU

One of the most recent measures to adopt new cybercrime law in the EU is the recommendation from the council of Europe (COE) convention on cybercrime. The COE makes recommendations on the safety and well being of European nations. The COE made several recommendations to the EU on how to solve the cybercrime issue. This recommendation was made in 2001 and still has not been ratified by the all the members of the EU. This illustrates how having a network of nations can severely inhibit the legislative process. "In 2001, the Council of Europe completed drafting a Convention on Cybercrime. As of September 15, 2005, the treaty had been ratified by only 11 countries, mostly in Eastern Europe. The number of ratifications has been sufficient for the convention to enter into force, on January 7, 2004. As of September 15, 2005, the convention had not been ratified by most Western European countries, nor had it been ratified by the United States, which played a major role in its drafting and had been invited to ratify it. As a model, the convention has some positive and some negative elements. The convention is very broad, reaching far beyond computer crime as such. And having taken on the issue of government access to computer data (for all crimes), the treaty fails to address half of the issue (the privacy and human rights half). Accordingly, developing countries must be very cautious in approaching the COE convention as a model" (GIPI, 2005, pp. 4).

The EU values the right to privacy arguably more then the US. So there are many aspects of the COE convention that will reduce the level of expected privacy. This is a double edged sword. While it is beneficial to reduce privacy (as the US has) to reduce cybercrime, it also hurts the social well being of the community to be monitored closely and not have absolute privacy. Table 2 provides a summary of the Convention on Cybercrime.

As can be noticed from the table below, the European Convention on Cybercrime addresses fraud, jurisdiction, child pornography and IP protection issues, similar to the US laws.

DIFFERENCES BETWEEN US AND EU LAWS

The first and most obvious difference between the US & EU is the fact that the US is one nation that governs itself and the EU is a coalition of European countries that cooperatively work together to achieve a common goal. In terms of ease of passing and implementing legislation, the US has the advantage. The US needs only to govern itself and only needs to deal with one legislative system. In the EU many nations have to ratify a treaty in order for it to take effect. This is quite problematic. Even though the EU members have a common goal they often have different agendas on how that goal should be achieved. That is why some legislation takes years to pass all the steps in the EU.

The second difference between the US and the EU is the expected level of privacy. The US has many laws that protect privacy but it is less concrete than what the EU has in place. Recently with the Patriot act and Homeland Security act Americans have lost a great deal of what is considered privacy. The EU is still upholding their charter to protect privacy. Everyone expects and enjoys a life without unnecessary intrusion but with a decrease in some privacy rights cybercrime will decrease. It is harder for criminals to commit a crime if the level of investigation is at a higher level. With the decrease of freedom and the forward thinking of legislation the US has one of the most secure infrastructures in the world. The following figure gives a comparison of secure web servers in the US and the EU.

Table 2: Article summary of the Convention on Cybercrime and the Framework Decision on Attacks Against Information Systems

COUNCIL OF EUROPE CONVENTION ON CYBERCRIME	COUNCIL OF THE EUROPEAN UNION FRAMEWORK DECISION ON ATTACKS AGAINST INFORMATION SYSTEMS
Illegal access (Article 2): Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	**Illegal access to Information Systems (Article 2):** 1. Each Member State shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases which are not minor. 2. Each Member State may decide that the conduct referred to in paragraph 1 is incriminated only where the offence is committed by infringing a security measure.
Illegal interception (Article 3): Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	
Data interference (Article 4): 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**Illegal data interference (Article 4):** Each Member State shall take the necessary measures to ensure that the intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system is punishable as a criminal offence when committed without right, at least for cases which are not minor.
System interference (Article 5): Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.	**Illegal system interference (Article 3):** Each Member State shall take the necessary measures to ensure that the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data is punishable as a criminal offence when committed without right, at least for cases which are not minor.

	Instigation, aiding and abetting and attempt (Article 5): 1. Each Member State shall ensure that the instigation of, aiding and abetting and attempt to commit an offence referred to in Articles 2, 3 and 4 is punishable as a criminal offence. 2. Each Member State shall ensure that the attempt to commit the offences referred to in Articles 2, 3 and 4 is punishable as a criminal offence. 3. Each Member State may decide not to enforce paragraph 2 for the offences referred to in Article 2.
Misuse of devices (Article 6): 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a. the production, sale, procurement for use, import, distribution or otherwise making available of: i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Article 2–5; ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offences established in Articles 2–5; and b. the possession of an item referred to in paragraphs (a)(i) or (ii) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2–5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this Article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3. Each Party may reserve the right not to apply paragraph 1 of this Article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1(a)(ii).	Not defined within the Framework Decision.

(Rand Europe, 2002, p. 19)

As can be noticed from the table below, the European Convention on Cybercrime addresses fraud, jurisdiction, child pornography and IP protection issues, similar to the US laws.

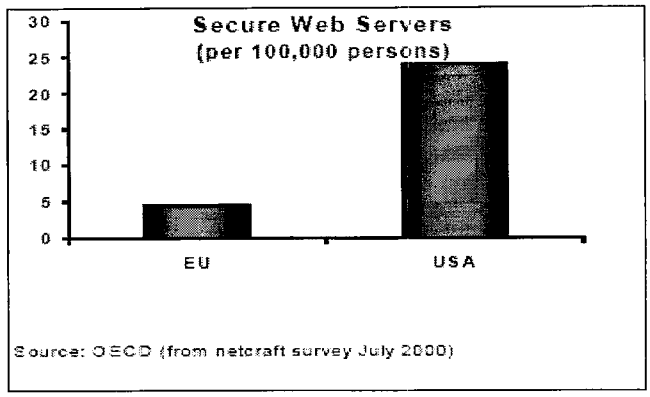

Figure 1: From the Commission of the European Communities, 2001)

Another major difference between the US and EU cybercrime laws focus on the issue of pornography. While the US laws and lawsuits focus a lot on what is pornographic and what is obscene, there seems to be no such issue in the EU laws. Both the EU and the US have similar laws concerning child pornography. But the issue of what is obscene, and thus what is harmful to minors and the larger society is focused on much more seriously in the US. Indeed, even within the US, there exists currently a complicated field of lawsuits and judgments pertaining to the issue of what is protected and what is not. In the EU, the problems are likely to be even more severe, due to the differing nature of culture, societies and communities within the members of the EU.

Since the US is currently considered to be one of the foremost experts in cybercrime prevention, many other nations rely on advice from the US in framing cybercrime laws. This cooperative effort is beneficial for global cybercrime prevention. Since the EU is looking to the US for a framework the laws (once adopted), it is likely that EU cybercrime laws will eventually mirror US laws in some aspects. "The EU cybercrime treaty generally adopts the approaches taken by the United States in the Computer Fraud and Abuse Act of 1986, Title 18 United States Code Section 1030, and the U.K. Computer Misuse Act and the laws. It calls on member states to adopt laws to punish unauthorized access to computers, unauthorized damage to, alteration of information in, or disruption of service to computers or computer systems, and the unauthorized interception of electronic communications" (Rasch, 2001). The differences between the US and EU are more procedural than functional. This opens the possibility of future cooperation between foreign nations. Once the laws are harmonized and the 'players' are on the same page, international cooperation will follow suit and cybercrime will be a thing of the past.

CONCLUSION

Cyber-criminals take advantage of the speed of propagation, global reach, anonymity and transience of the Internet to perpetrate crimes. Cybercrimes are currently an important global issue that has the potential of adversely affecting international economics, commerce, security and human rights. Criminal justice systems have responded with criminal prosecutions of cybercrime under old, existing laws, or by enacting new "cybercrime laws." These actions have mostly emerged from technically advanced countries, namely the United States, countries of the European Union, Australia, New Zealand, etc. Other countries have also started framing cybercrime laws, using mostly the US laws as the basis. Cyberlaw is a comparatively new field, and is continuously evolving and "catching up" with innovations in technology. However, as the analysis in this paper shows, despite some progress, cybercrime laws are often inadequate – they contain loopholes that make the prosecution difficult, suffer from a lack of understanding of the technical nuances of rapidly emerging technology, and suffer from vague and conflicting interpretations. Further, cyberlaws enacted in one country may counteract with another's notions of national sovereignty, jurisdiction, human rights and privacy. Given this it is useful to further study the development of cyberlaws and the role that they play in the convergence of information, innovation and technology. It is also important for IT professionals to take an active part in shaping cyberlaws, so that they are consistent, have minimal loopholes, are reasonably easy to prosecute, safeguard the essential openness and freedoms of the Internet, and not open to interpretation.

It is also important to note that even though this paper addresses only US and EU cybercrime laws, those are not the only countries considering or enacting such laws. Cybercrime is becoming increasingly recognized in other parts of

the world, and several countries have legislated or enacted their own versions of the cybercrime laws based on the US and EU experience. In a continuation of this study, we plan to study cybercrime laws of other countries, especially where they deal with international cooperation, to study similarities, differences and possible gaps in cybercrime laws. A future study will also address the experiences, issues problems of implementing cybercrime laws around the world.

REFERENCES

Casey, E. (2004). *Digital Evidence and Computer Crime.* San Diego, CA. Elsevier.

Commission of the European Communities. (2001). COM(2001)298 final, *Communication From The Commission To The Council, The European Parliament, The European Economic And Social Committee And The Committee Of The Regions, Network and Information Security: Proposal for A European Policy Approach.* Retrieved April 1, 2006 from http://europa.eu.int/eur-lex/en/com/cnc/**2001**/com**2001**_**0298**en01.pdf

Legislative Branch (2006, May 1). Federal government of the United States. In *Wikipedia, The Free Encyclopedia.* Retrieved 18:20, May 1, 2006 from http://en.wikipedia.org/w/index.php?title=Federal_government_of_the_United_States&oldid=50820243.

State, Tribe and local governments (2006, May 1). Federal government of the United States. In *Wikipedia, The Free Encyclopedia.* Retrieved 18:20, May 1, 2006 from http://en.wikipedia.org/w/index.php?title=Federal_government_of_the_United_States&oldid=50820243.

Rasch, M. (2001). *Cybercrime treaty flawed, but needed.* Retrieved March 13, 2006 from http://www.securityfocus.com/columnists/11

Rand Europe. (2002). *Handbook of Legislative Procedures of Computer and Network Misuse in EU countries Study for the European Commission Directorate-General Information Society 2002.* Retrieved April 1, 2006 from http://**eu**ropa.**eu**.int/information_society/**eeu**rope/2005/doc/all_about/csirt_**handbook**_v1.pdf

PC World Staff (1999). *The Digital Century: Software and the Internet.* Retrieved April 1, 2006 from http://www.cnn.com/TECH/computing/9911/23/digital.century2.idg/index.html

Hellenic Resources Institute. (1995). *The European Convention on Human Rights 1950*, Retrieved April 1, 2006 from http://www.hri.org/docs/ECHR50.html#C.Art20

Council of Europe (2001). *Convention on Cybercrime.* Retrieved April 1, 2006 from www.interpol.int/Public/TechnologyCrime/Conferences/6thIntConf/Convention.pdf

Cybercrime. (2006). *Wikipedia, The Free Encyclopedia.* Retrieved 14:28, April 3, 2006 from http://en.wikipedia.org/w/index.php?title=Cybercrime&oldid=46548752.

Global Internet Policy Initiative. (2005). *Trust And Security In Cyberspace: The Legal And Policy Framework for Addressing Cybercrime* Retrieved on April 2, 2006 from http:// www.internetpolicy.net/cybercrime/20050900cybercrime.pdf

Cases Cited

California v. Greenwood. (1987). US Supreme Court, Case number 86-684. Available online at http://laws.findlaw.com/us/486/35.html.

Kyllo v. United States. (2001). US Supreme Court, Case number 99-8508. Available online at http://laws.findlaw.com/us/000/99-8508.html.

Miller v. California. (1973). Supreme Court, California. Case number 70-73. Available online at http://laws.findlaw.com/us/413/15.html.

Playboy Enterprise Inc. v. Ferna. (1993). District Court, Florida, Case number 93-489-Civ-J-20.