Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

The Legal System and Ethics in Information Security

Security plays a big part in today's world of computers, e-commerce and the Internet. Technology however, has brought with it, the evils of crime. We thus need laws to protect those who maybe exposed to these new threats. In this paper, I will discuss the issues faced by the legal system in keeping up with the fast paced development of technology, the ways in which the current laws can help, and I will also enumerate a few of the laws that have been developed specifically to address computer crime in the United States....

Copyright SANS Institute
Author Retains Full Rights

AD
Take control of vulnerability threats Now!
Request a Free Trial
Secunia Stay Secure

The Legal System and Ethics in Information Security

SANS Security Essentials
GSEC Practical Assignment
Version 1.4, Option 1
Amit Raju Philip
15 July 2002.

© SANS Institute 2002, Author retains full rights.

Abstract:

Security plays a big part in today's world of computers, e-commerce and the Internet. Technology however, has brought with it, the evils of crime. We thus need laws to protect those who maybe exposed to these new threats. In this paper, I will discuss the issues faced by the legal system in keeping up with the fast paced development of technology, the ways in which the current laws can help, and I will also enumerate a few of the laws that have been developed specifically to address computer crime in the United States. Finally, the paper describes the role that ethics have to play in the world of computer security, and how they must be developed hand in hand with laws and statutes to govern the rights and wrongs of the computer world.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Table of Contents

1 Introduction 3
2 Security and the Law 4
2.1 Issues With the Legal System 4
2.2 Where the Law Comes In 8
2.3 Laws that apply to Security 10
3 Ethics in Security 11
4 Conclusion 13
5 References 14

© SANS Institute 2002, Author retains full rights.

1 Introduction

You took the advice of the security experts, and hired a full time security administrator/analyst. With his help your company formulated and spelled out a security policy. You analyzed the risks and vulnerabilities prevalent in your environment, and identified your industry's practices for due care. With this in mind, you set up a security infrastructure. You also laid out a plan for conducting periodic reviews and tests to analyze and enhance your security policy and infrastructure [1]. Finally, you set up an intrusion detection system. Just as you start to wonder whether it was all worth it, lo and behold, your security administrator informs you, that after analyzing several suspicious logs and hack attempts, he was able to pin-point an intruder who had been trying to get to the core of the company's data. Had it not been for the security systems in place, the organization could have lost millions. Great; that $100k increase in the total cost of ownership of the IT department seems to be paying itself off [1]. But the question is, now what?

You set up the system and nabbed the intruder, but where do you go from here? What are the laws governing information security? Do such laws even exist, and if so, how and to what extent do they protect you? Will the evidence you provide, hold up in a court of law? Will the legal system even be competent enough to try such a case? How much harm would the case do to your organization's public image? Other issues include geographical location and jurisdiction, as most computer crime today is Internet related, and boundaries for law enforcement agencies are either not well defined in this domain, or most countries do not have laws to prosecute cyber crime. With the absence of the protection that laws provide, the only recourse that exists is to build ones own defenses against external threats, and to depend on internal security, and to a large extent, ethics to minimize internal intrusions.

Since technology is developing a lot faster than the legal system and the law making process, sometimes there is no legal protection offered against the misuse of new technology. In some cases, it is not apparent what is and what is not to be prohibited, and so adequate laws do not exist, or are just not comprehensive enough to deal with most situations that may arise with misuse of a certain technology. In these circumstances, as with society, it is imperative that ethics take over, in order to provide sanity to what would otherwise be a very chaotic situation. It is the responsibility of people who create and use the technology to make sure that it is utilized in a responsible and ethical manner. Of course, this does not offer any tangible protection, but just as with society, social acceptance and peer pressure that are nurtured through the acceptance or non-acceptance of evolving ethics, play a key role in limiting the misuse of technology. Thus, it is vital that healthy security based ethics are cultivated to compensate for and/or collaborate with the legal system.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

2 Security and the Law

This section deals with the interaction of the legal system with information security. A major part of computer and information security today is tied to the Internet, and the since the Internet does not have any geographical boundaries, a discussion of the legal system with respect to computer security would not be complete without mention of legal practices in this regard, followed in every country around the world. Since it is not feasible to study the legal systems of every single country, the focus of this section will be on the computer security laws and statutes of the United States' legal system.

The following sub-sections analyze the issues that the legal system faces when dealing with computer based crime, and why it is such a challenge. The field of networking, that brought about a whole new arena for computer crime is now almost three decades old, and the Internet, almost two [7]. Laws have been established in this time, and are still evolving. Section 2.2 describes the areas of computer security that are addressed by laws in the US. The last sub-section describes a few of the actual laws and statutes on computer and information security established in the United States.

2.1 Challenges the Legal System Faces

2.1.1 Rapid Technological Advancement

> It cannot be helped, it is as it should be, that the law is behind the times. (Holmes, p.102 [3])

Developments in computer technology are occurring every day. With every new protocol, product or application that is developed, more doors are opened to computer intrusion and misuse. Most of the time it is not even known that a problem exists until vulnerability is found and exploited. Then it is realized that some sort of law needs to be established to offer protection against misuse, and the process begins to develop a law. Since the legal system is so reactionary in nature, it just does not have the ability to keep up with the rapid development of technology. Laws take time to be formulated, finalized and approved before they go into effect. This however, is a necessary evil, as stated by the Pennsylvania State Legislature:

> Laws influence our environment, economy, education, our families, our health and virtually every aspect of our daily lives, now and for generations to come. To make new laws or change those already on the books, lawmakers follow time-honored Constitutional procedures [4].

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

The good news however, is that efforts are being made to establish laws in the field, and in fact, the U.S. Department of Justice's criminal division has a dedicated department for cyber-crime issues, called the Computer Crime and Intellectual Property Section (CCIPS). Their website at http://www.usdoj.gov/criminal/cybercrime/index.html provides information on cyber-crime related legal and policy issues, as well as instructions on how to report and even help fight cyber-crime. In times of adverse need, changes to laws can be made without much delay, as evidenced by the USA Patriot Act which was signed by President Bush on October 25, 2001, in response to the terror acts of September 11th, 2001. This Act contains a number of substantial changes to the US federal cyber-crime laws since the last major revisions of 1996 [5].

2.1.2 Technologically Inept Legal Personnel

In order to try, prosecute, or make judgments in computer crime related cases, the lawyers, prosecutors and Judges involved need to have a firm understanding of the technologies involved in the crime being tried. Unfortunately, legal personnel of yester-year do not have adequate know-how of computers and computer related technologies [2]. If a jury is required, they too need to be well informed. What is more of a challenge, is keeping people of these professions up-to-date with the latest advancements. While it is true that experts are often called in for opinions, informed decisions cannot be made without basic understanding. This begs the question as to what the best method to tackle this problem would be. Do we make the security experts lawyers, or do we make the lawyers security experts? In the United States, the Computer Crime and Intellectual Property Section (CCIPS) of the US Department of Justice criminal division, has its own attorneys that provide training to federal, state, and law enforcement agents, prosecutors, other government officials, and in some cases to foreign requesters [6]. Thus steps are being taken in the right direction to equip the system with the needed expertise to face the world of computer security.

2.1.3 Multiple Roles of Computers in Crime

Computers can be the subject, the object, or the medium of a crime [2]. It would be great if we could prosecute the computer itself, but unfortunately a computer does only what it is told to do by a human, and if it does not, the fault lies again with the human who built it, or the human who modified it to behave inappropriately. Laws on computer crime need to address all these situations.

- Computers maybe stolen or they maybe damaged. In these cases they will be considered tangible property, and their value will be sought. However, what about the value of the data on the computer?
- Breaking in to somebody's house and stealing is considered burglary. However how should unauthorized access to computer systems be handled? Not only could someone steal valuable data, they could also use the machine to gain access to other trusted machines.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Computer systems maybe used to develop destructive code for viruses and Trojans that could cause widespread damage to other systems.
- Computers hold valuable information, the misuse of which could aid in a number of other crimes such as fraud, identity theft etc.
- There is also the issue of copyrights and illegal use of software programs.

These are just few of the ways in which computers are used as a tool to cause harm, create losses, or to gain unjust profits. It is the responsibility of lawmakers to identify these methods, and inhibit them with adequate laws and punishments for people who resort to using computer systems in inappropriate ways.

2.1.4 Jurisdiction

Jurisdiction is a major stumbling block for the legal system when it comes to dealing with computers, networks and their security. In the US, the court must have jurisdiction over the person or the subject matter of a lawsuit in order to be able to try it [8]. This works well with the current setup of law enforcement agencies that are very territorial and operate within distinct district, city, county, state or country lines. All of this however, gets thrown out the window when there are no physical boundaries to go by when determining jurisdiction, as is the case when it comes to computer networks and the Internet.

A person could be sitting in country 'A', remotely logged in to a computer in country 'B', and committing a crime on systems in country 'C'. Of course in committing the crime, the perpetrator could be sending packets that traverse routers in countries 'D', 'E' and 'F' [9]. Under which country's laws should this person be prosecuted? The crime was committed on a computer in country 'C', from a computer in country 'B'. Law enforcement officials from these two countries do not have the authority in most cases to go to country 'A' where the individual is physically located, and bring him or her back to their respective countries for prosecution. This is not a fictional scenario as illustrated by the following excerpts quoted from an article on CNET News.com.

> Perhaps no case highlights the confusing thicket of jurisdictional issues on the Web more than the Yahoo imbroglio. The saga began two years ago when two French human rights groups sued Yahoo, arguing that the posting of historical Nazi items on the company's U.S.-based site violated French law prohibiting the display of racist material. A French judge sided with the groups, ordering Yahoo to block French citizens from accessing the site or face steep fines. However, Yahoo turned to the U.S. courts and asked a judge to declare the French law unenforceable here. He did.
>
> Now, the company is facing another set of charges that it, along with former CEO Koogle, violated the country's war crime laws by displaying the items. In perhaps the most curious aspect of the

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

case, the American Yahoo site at issue had no physical presence in France. (Bowman [10])

Suggestions have been made to make cyberspace a separate jurisdiction of its own with its own laws and regulations [8, 11]. However, this will take a great deal of time, agreement and co-operation between countries. Until such a move is justified and agreed upon, it is up to cyber communities such as ISPs to maintain their own laws and codes of conduct so that the misuse of computers over their networks is kept to a minimum. Various countries are in turn trying to establish treaties to sort out these very cross-border Net issues.

2.1.5 Computer Crime kept Quiet

In this day and age where companies hold large amounts of personal information about its customers or clients, keeping the information private is top priority. Thus the security of networks and databases is a big deal. If an intrusion does occur, and data is lost or leaked, companies find it in their best interests to keep the matter quiet and out of courts, even if the intruder is identified. A court case and media attention would cause unwanted negative publicity, which would in turn scare off potential clients, and perhaps even cause current clients to consider competitors instead. It could also cause enough furor among the current client population that they would look to sue for damages as well. These possible repercussions are enough incentive for most companies to deal with security intrusions internally, which in turn hurts the legal system, since it will never become aware of the kind of threats that need to be protected against. Moreover, it may seem as motivation for individuals to indulge in such criminal behavior under the pretext that they will not be answerable to the law if caught.

2.1.6 Inadequate Precedence

Since computers, networks and the Internet are a relatively new evil in the legal system, not many cases have been tried in these fields. Modern day court rulings are based to a large extent on precedence from old cases. This once again is a stumbling block for the legal system when it comes to cases related to computer security. Since there is no precedence established, rulings on current cases will become precedence for future cases. Thus, a great deal of thought and care has to be taken to make sure that correct decision is made and appropriate punishments are handed out.

2.1.7 Motive and Age of Offenders

In searching for criminals, law enforcement agencies usually look for means, motive and opportunity to build a strong enough case [12]. With the Internet, means and opportunity are always available, however, finding a motive is difficult in most cases. This is because most cyber-crime is done not out of spite or hate, but for the adventure and challenge it offers. In fact, juveniles commit a number of these crimes. The problem with this is that these are seen more as childhood pranks, and if not 'nipped in the bud' early, the same juveniles, with more

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

experience, technology, and quest for adventure will commit more serious offenses [2].

2.1.8 Anonymity Offered by the Internet

It is possible for people to remain anonymous while communicating or performing other activities over the Internet. This brings a sense of security, and in turn, in some cases, gives individuals the courage to do the outrageous, and sometimes even resort to illegal activities. The sense that their actions cannot be associated with them makes people indulge in activities they would not ordinarily do. With respect to computer crime, individuals may seek to play pranks, or in more extreme cases steal, cause loss or harm or commit fraud. It sometimes takes days, weeks or even months before acts of cyber-crime are detected, and by that time the perpetrators are able to cover their tracks and maintain their anonymity, and so in a lot of cases, will never be caught [13].

2.2 Where the Law Comes In

The previous sections seem to paint a dreary picture of the state of the legal system with regard to computer technology and its ability to offer protection from misuse of the latter. However, even in light of the fact that the laws are slow to develop, and often take years to take form and be approved, legal systems have to, and do offer some sort of respite. Laws do exist for more traditional crimes, and while they may not fit very well with the computer world, they can be adjusted to provide some, if not thoroughly adequate protection. This is not to say that no laws exist exclusively for computer crime. As a matter of fact, Section 2.3 describes actual laws and statutes that have been passed in the United States to prosecute computer crime. The purpose of this section however, is to describe the situations where the law can and does extend its hands into the realms of computer and information security, be it through laws expressly developed for computer crime, or through pre-existing laws used to prosecute more traditional crimes such as theft, fraud, abuse etc.

Attorney and consultant, Ronald B. Standler, in his article “What is Computer Law?”, states that computer law should at least cover copyrights, contracts, trademarks, patents, tort, computer crime and utilities [14]. It is evident that there have existed laws covering all these topics with the exception of computer crime, since the expansion of computers and the Internet into the public domain. Thus, with minor modifications these have been used to regulate the use of computer technology.

Existing copyright laws are geared towards the protection of expression of ideas. They do not protect the idea itself, but merely the way the idea is expressed. Thus works of art, literature, books, songs etc. are protected, and cannot be copied under this law. In terms of computers, programmers would want to copyright their programs. The US copyright law of 1976 was amended in 1980 to

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

include computer software [2]. This however, may not be the most suitable protection that programmers would be looking for. The program is the expression of the idea. The actual idea in this case is the algorithm, and in the computer world, it would make more sense to protect the algorithm. This cannot be done under the traditional copyright laws, and so until another law is developed this is the only protection offered.

There have been some cases of the Patent Office issuing software patents as an alternative for software programmers. These too, however, do not protect the underlying algorithms for programs that programmers would like to do. Further, justification for a patent for a computer program is difficult, and is often challenged. Patents are meant to protect inventions, or in other words, the process for carrying out an idea; once again not the idea itself. So, while this from of protection is available, the time, effort and expense involved in obtaining and maintaining a patent may not be the most suitable for software writers [2].

With the recent boom in E-commerce, the need arose for laws to protect and uphold contracts, business transactions, data processing and development over the Internet. The United Nations adopted a model law for electronic-commerce in 1996 based on which a number of countries have developed their own laws. The United States too passed its own electronic law in the year 2000 through the US Electronic Signatures in Global and National Commerce Act ("E-SIGN"). This is used in conjunction with the Uniform Electronic Transactions Act of 1999 to encompass electronics transactions conducted over the Web [15, 16].

A trademark is a word, phrase, symbol or design, or a combination of words, phrases, symbols or designs, that identifies and distinguishes the source of the goods of one party from those of others [17]. Trademarks hold significant value to organizations, especially once they are established and well recognized. In the computer world, domain names can fall into this category. There is also the issue of the illegal distribution and use of established trademarks to gain profits. The World Intellectual Property Organization (WIPO) has undertaken an international process to develop recommendations concerning trademark issues associated with Internet domain names, including issues pertaining to the resolution of domain name disputes [18].

Utility law is something that refers to regulation of Internet Service Providers, telecommunications companies, and domain name providers. These are relatively new, and there is still debate as to whether ISPs should be treated as regular utility companies, such as electricity, water and cable companies. A number of countries have strict laws for ISPs controlling the kind of websites that users should be allowed to access. Such laws are not prevalent in the US so far, but there have been attempts to have laws to regulate indecency and obscenity on the Internet, but these have been struck down by the courts as unconstitutional [19].

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

A tort is a form of wrongful conduct that results in a harmful consequence, normally personal injury or property damage. Tort law is the body of legal rules that govern the various tort actions that can be brought in the event of personal injury or damage. In terms of computer security, tort law addresses the following, according to Ronald B. Standler, in his article "What is Computer Law?"[14]:

- Duty to maintain secure data (i.e., confidentiality)
- Privacy issues in databases
- Use of Social Security Number by businesses as identifier, allowing different records to be merged into a comprehensive database
- Liability for errors or harmful information in content of databases
- Repetitive motion injuries from computer keyboards or mice
- Products liability involving computer hardware or software
- Y2K problem

Laws that directly address computer crime also do exist, and some of the more important statutes of the US legal system are discussed in the next section.

2.3 Laws and Statutes that apply to Security

Computer related laws and statutes have a direct effect on computer security. They determine how computer security intrusions should be handled and investigated, and what kind of evidence is required in order to prosecute perpetrators. Very often security policies will be based on the kinds of laws available, since due diligence and due care form an important part of today's legal systems.

In the following section, are described some of the federal computer crime laws and statutes of the US Department of Justice [20]. They are listed with the statute number, and title, followed by a very brief description of what the law encompasses. It is not feasible for the scope of this paper to go into the details of each of the laws; however, the actual text of the law can be reviewed by clicking on the title.

- 18 U.S.C. § 1029. Fraud and Related Activity in Connection with Access Devices - Describes prohibitions and penalties associated with unauthorized possession and fraudulent use of access tokens, passwords, and other access devices.

- 18 U.S.C. § 1030. Fraud and Related Activity in Connection with Computers - Describes prohibitions and penalties for the unauthorized access and fraudulent use of electronic systems.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- 18 U.S.C. § 1362. Communication Lines, Stations, or Systems - Describes prohibitions of malicious or willful destruction or intent to destroy or disrupt communications systems within the U.S.

- 18 U.S.C. § 2511. Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited – Describes prohibitions of monitoring cellular voice channels, cordless phones and eavesdropping on electronic transmissions of data.

- 18 U.S.C. § 2701. Unlawful Access to Stored Communications - Describes prohibitions and penalties associated with unauthorized and/or overdue access to electronically stored information.

- 18 U.S.C. § 2702. Disclosure of Contents – Describes prohibitions for electronic communication service providers, and remote computing service providers from knowingly divulging personal information, or communications of subscribers that they have electronic possession of.

- 18 U.S.C. § 2703. Requirements for Governmental Access – Describes the requirement for electronic communication service providers, and remote computing service providers to disclose to government entities information regarding subscribers or customers.

3 Ethics in Security

We deal with the vast expanses of the Internet, a domain that knows no geographical boundaries or national or cultural lines. While on it, we interact with people from different parts of the world, with different values and beliefs. Apart from laws to regulate the on-goings of the Internet, its users also need to have a certain amount of responsibility and etiquette while using it. This does not apply only to Internet use, but also to general use of computer resources, hardware and software.

It is impossible to formulate laws to enforce all sorts of behaviors acceptable to society. Instead, society depends on ethics to build awareness of socially accepted behavior. Ethics are objective [2]. Unlike laws, they cannot be forced on individuals. In fact different individuals may have different ethical beliefs. The point however, is that some sort of social standard needs to be set with regard to the use of computer resources. Unlike laws, ethics can be molded and modified to suit the situation much more easily. Thus it is the responsibility of groups, companies, organizations, service providers, and even countries to establish codes of ethical behavior that people should strive to achieve and live by. In a utopian world, only ethics would be enough to have society function smoothly. With everyone striving to reach certain moral standards, there would be no need

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

for laws. However, in the real world, ethics and laws have to operate hand in hand.

> The Internet was a highly useful medium and worked extraordinarily well as long as professional scientists and engineers dominated the user community. The Internet began to experience problems when other groups of people (e.g., college students who were away from parental supervision for the first time in their lives, people who were not professionals) joined the Internet, but did *not* honor the unwritten rules of etiquette for polite professionals. (Standler [21])

It is because of this change in the user community that the need for ethics in the computer world has increased many fold. Today most organizations have written codes of ethics for its members to abide by. In a similar effort, the Computer Ethics Institute has developed it's own Ten Commandments of Computer Ethics which it believes computer users should abide by [22]:

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that insure consideration and respect for your fellow humans.

Encouraging users to abide by some kind of ethical standard however needs to be a collaborative effort. Regardless of which country we call home, most of us know that it is wrong to break into our neighbors' houses and steal things or damage their property. Yet, it doesn't seem that our youth today are being taught that the same principles apply to their behavior on computers and the Internet. Indeed, in certain instances, unethical online behavior has been glorified. In the United States, the Department of Justice is working with the private sector in an effort to rectify this situation. Approximately a year ago, in a joint private-public effort, the Cybercitizen Partnership was formed, an initiative designed to educate and raise awareness of computer responsibility [23]. Relatively new terms, "cyber-citizenship", "cyber ethics", and "netiquette" refer to responsible cyber social behavior [24]. It is important for all countries to think about how they, too, can encourage ethical cyber-behavior among their citizens.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

As Julie Van Camp says in her article, “Computer Ethics: Codes, Commandments, and Quandaries” [25],

> Ethical behavior comes from an ability to reason through new problems as they arise continually in any profession. It grows from a continuing understanding of principles and how to apply them to new and varied situations, which we cannot even imagine, let alone predict at the present time. Only with a reasoned and thoughtful response to ethical problems are people likely to behave ethically.

It is for this very reason, that a culture of ethical abidance needs to be developed. Perhaps then we will not be so dependant on laws anymore.

4 Conclusion

Computer technology has revolutionized the world. It has removed restrictions of geographical proximity in communication and business. However, with every great invention, also come its follies. Given the kind and amount of information stored on computer systems that travel over networks, there came the need for computer security. With the development of security for computers, came the need for a legal system to prosecute perpetrators. The limitations of the law brought the need for ethics.

The legal system is an integral part of society. We have seen that it has its limitations, but nevertheless it plays a vital part in the upholding a secure computing infrastructure. It is important that security administrators understand the support they have from the legal system in order to adequately protect their computer systems. At the same time, it is important that companies develop healthy computer ethics to minimize intrusions from within. It is a well-known fact that most instances of computer crime occur from the inside, and thus creating a culture of ethical computer behavior is vital deterrent to underhand computer related activities.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

5 References

[1] Northcutt, Stephen. Network Intrusion Detection: An Analyst's Handbook, Second Edition. Indianapolis: New Riders, September 2000. 387, 390.

[2] Pfleeger, Charles. Security in Computing, Second Edition. Upper Saddle River: Prentice-Hall, Inc., 1996. 494-499, 511-512, 517.

[3] Holmes, O. W. Speeches, 1934. 102.

[4] Commonwealth of Pennsylvania. "Making Law in Pennsylvania." URL:http://www.legis.state.pa.us/WU01/VC/visitor_info/making_law/intro.htm.

[5] Reilly, Bill. "The Impact of the USA Patriot Act on Network Security Practice." 15 November 2001. URL:http://packetstormsecurity.nl/papers/legal/patriot.doc.

[6] U.S. Department of Justice. "Inviting CCIPS Attorneys to Speak to You." 21 March 2001. URL:http://www.usdoj.gov/criminal/cybercrime/speaker.htm.

[7] Internet Society. "All About the Internet." 18 November 2001. URL:http://www.isoc.org/internet/history/cerf.shtml.

[8] Oberding, Juliet. "A Separate Jurisdiction for Cyberspace?" URL:http://www.ascusc.org/jcmc/vol2/issue1/juris.html.

[9] Burk, Dan. "Jurisdiction in a World Without Borders." Virginia Journal of Law and Technology, Volume 1. Spring 1997. URL:http://vjolt.student.virginia.edu/graphics/vol1/home_art3.html.

[10] Bowman, Lisa. "Enforcing Laws in a Borderless Web." 29 May 2002. URL:http://news.com.com/2100-1023-927316.html.

[11] Johnson, David. "Law And Borders--The Rise of Law in Cyberspace." Stanford Law Review 1367, 1996. URL:http://www.cli.org/X0025_LBFIN.html.

[12] Rogers, Larry. "Cybersleuthing: Means, Motive and Opportunity." InfoSec Outlook, June 2000. URL:http://interactive.sei.cmu.edu/news@sei/columns/security_matters/2000/summer/security-sum-00.pdf

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

[13] Auchard, Eric. “World's Computer Laws Lag Behind Internet Changes.” 11 May 2000.
URL:http://www.expressindia.com/ie/daily/20000511/ibu11016.html.

[14] Standler, Ronald. “What is Computer Law?” 30 May 1999.
URL:http://www.rbs2.com/cdefn.htm.

[15] Baker & McKenzie. “Electronic and Digital Signature Definitions.” 14 November 2000.
URL:http://www.bmck.com/ecommerce/countrycomp.htm.

[16] Global Internet Policy Initiative. “E-Commerce / Digital Signatures” 2001.
URL:http://www.gipiproject.org/e-commerce/.

[17] United States Patent and Trademark Office. “Basic Facts About Trademarks.” 16 October 2001.
URL:http://www.uspto.gov/web/offices/tac/doc/basic/trade_defin.htm.

[18] Guillot, Gregory. “All About Trademarks.” 17 January 2002.
URL:http://www.ggmark.com/#Trademarks_In_Cyberspace.

[19] Cole, Raywid & Baverman LLP. “Becoming an ISP.”
URL:http://www.crblaw.com/faqs/becomeisp.html#8.

[20] U.S. Department of Justice. “Federal Computer Intrusion Laws.” 4 June 2002. URL:http://www.usdoj.gov/criminal/cybercrime/cclaws.html.

[21] Standler, Ronald. “Response of Law to New Technology.” 12 August 1998. URL:http://www.rbs2.com/lt.htm.

[22] Computer Ethics Institute. “The Ten Commandments of Computer Ethics.” 16 April 2001. URL:http://www.cpsr.org/program/ethics/cei.html.

[23] Robinson, James. “Internet as the Scene of Crime.” 31 May 2000.
URL:http://www.usdoj.gov/criminal/cybercrime/roboslo.htm.

[24] The Cyber Citizen Partnership. “What is Ethics?”
URL:http://www.cybercitizenship.org/ethics/ethics.html.

[25] Van Camp, Julie. “Computer Ethics: Codes, Commandments, and Quandaries.” June 2001.
URL:http://cobolreport.com/columnists/julie/062701%20-%20VanCamp_6_2001.rtsf.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**