Japanese and American Computer Crime Policy

A Comparative Study

Ryan J. Handerhan
Carnegie Mellon University
Information Systems
4/30/2010

Contents

Abstract

The development of a strong information-based economy is dependent upon the trust and belief of its users and customers in the integrity and security of information. National policy plays an enormous role in not only bolstering the trust of the people, but can also be effective in deterring cyber crimes and protecting critical data from unauthorized or malicious access, reproduction, or destruction. This thesis compares the American Computer Fraud and Abuse Act and the Japanese Unauthorized Computer Access Law in order to glean knowledge that can be used to make policy recommendations. Subsequently, these recommendations can be used to create more effective information security policy on a national level that will reduce cyber crime and increase people's trust of information systems.

Introduction

In this thesis, I compare the policies of the United States and Japan aimed at preventing the unauthorized and unwanted access, reproduction, or destruction of electronically stored data. Two of the most direct, high-visibility policies aimed at achieving these goals include the American Computer Fraud and Abuse Act and the Japanese Unauthorized Computer Access Law. Therefore, I intend to focus specifically on the comparison of these two national-level legal policies.

For the existence of a strong information-based economy, users' trust in the security of their information is imperative. National policy can play a tremendous role in providing the protection needed to foster this necessary trust and security. Seeing this, the primary research questions were formulated from an extensive literature review of the current Computer Fraud

and Abuse Act and the Japanese Unauthorized Computer Access Law. The questions relate to comparing the areas of strength and areas of concern in both policies and ultimately making recommendations for approaches to computer crime policy from the results. The final research questions are presented in the Research Design section of this paper.

While each country has similar intentions of protecting their critical electronically stored information and creating the necessary faith in security for the development of a strong information-economy, each country's policy substantively and procedurally, behaves differently. By examining the effects of these differences, I will derive key take-aways which can be used to make recommendations to improve each country's information security policy.

The American Computer Fraud and Abuse Act identifies and outlaws seven specific activities involved with the unauthorized access, reproduction, and destruction of electronic data. It is the primary and comprehensive cyber-crime act in United States Federal Law, and it stands as part of the American criminal code. The Japanese Unauthorized Computer Access Law outlines and outlaws one activity, but that activity can be used to prosecute within several more broad contexts. It is not a part of Japanese criminal code and is not as comprehensive in its approach as the American Computer Fraud and Abuse Act. Several other sections of Japanese criminal code also deal with computer crime, and may frequently be used in tandem with the Unauthorized Access Law. These differences will become an important theme in my analysis.

In addition, not only did I review how policy affects trends in the criminal reproduction and destruction of electronic data, but I also investigated how trends in such undesirable activities affect the development these two policies over time. By examining these trends, I

demonstrate the strengths and short-comings of each country's law. From this, I suggest improvements to the current state of information security policy.

Literature Review

Background

Mentioning that the internet and telecommunications landscape is rapidly evolving every day has become a cliché by now. The ways in which people communicate and do business are continuously in flux. Along with that, the ways people find to manipulate information technology to defraud, steal from, or perform any of a variety of acts of selfish gain or malicious intent are constantly proliferating. Along with the problems that the proliferation of computer-related crimes give law enforcement, the traceability and investigation of internet and computer crime remains incredibly difficult. Anyone, anywhere in the world, can perform malicious activity on any computer anywhere else in the world, through the internet. At the same time, while technology changes fast, the law moves very slow, creating many problems for public policy in regulation of cyber activity (Klotz, 2004). In the late 1990s, the internet was much likened to the old American Western Frontier: a vast, law-less landscape where regulation cannot exist, and may not even belong (Cox, 2006).

However, this has turned out to be far from the truth. Lawrence Lessig, who at one point had been seen as an enormous proponent of such a libertarian view of the internet as some un-manageable "frontier," has detected a trend toward more and more regulation, under the influence of policy, through the code that constructs the applications, sites, and networks that make up the internet (Cox, 2006). This is in support of what Grabosky, Smith, and Dempsey refer to as a notion of legal pluralism. In the digital age, where the limits of the state have become increasingly apparent, cyberspace is controlled primarily through the programming and architecture of information systems, as well as market forces and non-state

institutions. The regulation of the computers and computer crime is not handled by the state alone, but by a complex web of inter-dependent non-state organizations, market-forces, and code, all of which are influenced by policy and the state (Grabosky, Smith, & Dempsey, Electronic Theft: Unlawful Acquisition in Cyberspace, 2001).

However, even if governments can exercise influence on different forces of regulation in this web of legal plurality, addressing computer and internet crime with current legal frameworks still faces a barrage of problems. A primary issue at hand is the "state-less" condition of the internet. For example, a computer in France may fall victim to a hacker in Sri Lanka. Tracing such activity is incredibly difficult, and even if accomplished, often times crossing the red-tape of different international justice systems causes great difficulties for prosecutors and raises issues surrounding the sovereignty of nation-states. Within the condition of the global society, it is implausible at this time to consider a completely universal international code to prosecute cyber-crime, or expect the feasibility of some sort of state-less new paradigm of rule and policy creation. Now, and into the foreseeable future, law-makers and governments have been focusing on regulating computer crime with existing legal paradigms. However, considering the global context in which computer activity and crime takes place, a push towards a certain level of international legal harmonization has become prevalent (Klotz, 2004). Within an environment of international pressure for legal harmonization and the betterment of internet regulation and protection, comparing, studying, and understanding different nations' policies becomes more and more critical.

The United States Computer Fraud and Abuse Act

Beginning in the early 1980s, law enforcement began to notice an inability to address a rise in computer-related criminal activity as information systems and information technology advanced. A combination of traditional laws and the wire and mail fraud provisions of the federal criminal code covered some of the malicious activity, but the laws of the time were not sufficient to address the rise in the new, computer-related crime. In answer to the situation, Congress included provisions to make it a felony to access financial records or credit histories stored in a financial institution or to trespass into a government computer, as a part of the Comprehensive Crime Control Act of 1984. However, after enacting these provisions, Congress still continued to hold hearings related to problems in the realm of computer-crime to determine if federal criminal code required further revision. In 1986, these hearings resulted in the Federal Computer Fraud and Abuse Act (CFAA), which amended the previous provisions of 1984, 18 U.S.C. 1030(f). Since 1986, information technology and related crimes have become more sophisticated in their nature, and the Computer Fraud and Abuse Act has consistently been revised to keep pace. The CFAA has seen revisions in 1988, 1989, 1990, 1994, 1996, 2001, and 2002. The most major revisions to the act have occurred in 1996, and in 2001 with the introduction of the U.S.A. PATRIOT Act (Department of Justice, 2007).

In its current state, the Computer Fraud and Abuse Act, 18 U.S.C. 1030, outlaws conduct that victimizes federal computers, bank computers, and computers connected to the internet used in inter-state commerce. It is a computer and information security law. It outlaws

accessing these "protected" computers for the purposes of trespassing, threats, damage, espionage, and from being corruptly used as instruments of fraud. The provision is not entirely comprehensive but fills in the gaps of previous, traditional criminal laws to effectively combat computer-related crime. The act is divided into Subsections (a) through (g). The seven paragraphs of subsection 18 U.S.C. 1030(a) outlaw seven specific computer-related activities, and subsection 1030(b) continues by making it illegal to attempt to commit any of the offenses listed in subsection (a). Subsection 1030(c) outlines the penalties for committing each offense. Penalties range from no more than a year imprisonment for simple computer trespassing to life imprisonment until death for intentional computer damage. Subsection 1030(d) protects the authority of the Secret Service to investigate related crimes. Subsection 1030(e) clarifies common definitions. Subsection 1030(f) disclaims application to what otherwise would be permissible law-enforcement activities, and 1030(g) provides a civil cause of action for victims of these crimes (Doyle, 2008).

The following table presents the offenses outlawed by the CFAA 18 U.S.C. 1030(a), and the penalties for each offense as prescribed by subsection 1030(c).

(Table 1) (Department of Justice, 2007)

Section	Offense	Penalty(Years)
(a)(1)	Obtaining National Security Information	10(20)
(a)(2)	Compromising the Confidentiality of a Computer	1 or 5
(a)(3)	Trespassing in a Government Computer	1(10)
(a)(4)	Accessing a Computer to Defraud and Obtain Value	5(10)
(a)(5)(A)(i)	Knowing Transmission and Intentional Damage	10(20 or Life)
(a)(5)(A)(ii)	Intentional Access and Reckless Damage	5(20)
(a)(5)(A)(iii)	Intentional Access and Damage	1(10)
(a)(6)	Password Trafficking	1(10)

(a)(7)	Extortion Involving Threats to Damage Computer	5(10)

*Maximum penalty for second offense notated in ().

The following section indicates each offense as outlined in the CFAA 18 U.S.C. 1030(a), and provides a brief description of the offense.

Obtaining National Security Information: 18 U.S.C. 1030 (a)(1)

Section 1030(a)(1) punishes the act of obtaining national security information without or in excess of authorization and then intentionally providing or attempting to provide the information to an unauthorized recipient, or willfully retaining the information (Department of Justice, 2007).

Compromising Confidentiality: 18 U.S.C. 1030(a)(2)

The crimes out-lined in the three subsections of 1030(a)(2) punish the unauthorized access of different types of information and computers. Generally, violations of this section are considered misdemeanors unless aggravating factors are proven to exist. Computers protected by this section include any computer connected to financial institutions, any department of the United States Government, or any computer involved in inter-state or foreign commerce(Department of Justice, 2007).

Trespassing in a Government Computer: 18 U.S.C. 1030(a)(3)

"Section 1030(a)(3) protects against "trespasses" by outsiders into federal government computers, even when no information is obtained during such trespasses. Congress limited this section's application to outsiders out of concern that federal employees could become unwittingly subject to prosecution or punished criminally when administrative sanctions were more appropriate" (Department of Justice, 2007).

Accessing to Defraud and Obtain Value: 18 U.S.C. 1030(a)(4)

A violation of this section has occurred when someone knowingly accesses a protected computer without or in excess of authorization with an intent to defraud. The unauthorized access must further the intended fraud and the offender must obtain anything of value, including use of the computer if value exceeded $5000 (Department of Justice, 2007).

Damaging a Computer or Information: 18 U.S.C. 1030(a)(5)

Section 1030(a)(5) outlaws a wide array of offenses that cause computers or computer systems to fail to operate as their owners would like them to operate. Criminals can harm computers in a variety of ways, including, but not limited to, shutting systems down, deleting files, viruses, "denial service attacks," etc. Prosecutors can use section 1030(a)(5) to charge all of these different kinds of acts (Department of Justice, 2007).

Trafficking in Passwords: 18 U.S.C. 1030(a)(6)

"Section 1030(a)(6) prohibits a person from trafficking in computer passwords and similar information when the trafficking affects interstate or foreign commerce, or when the password may be used to access without authorization a computer used by or for the federal government. First offenses of this section are misdemeanors" (Department of Justice, 2007).

Threatening to Damage a Computer: 18 U.S.C. 1030(a)(7)

"Section 1030(a)(7), which prohibits extortion threats to damage a computer, is the high-tech variation of old-fashioned extortion. This section applies, for example, to situations in which intruders threaten to penetrate a system and encrypt or delete a database. Other scenarios might involve the threat of distributed denial of service attacks that would shut down the victim's computers. Section 1030(a)(7) enables the prosecution of modern-day extortionists who threaten to harm or damage computer networks—without causing physical damage—unless their demands are met" (Department of Justice, 2007).

Over the years since its initial enactment, the Computer Fraud and Abuse Act has come across many changes and revisions. The most prevalent and recent of these changes occurred in 2001. "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001," or the USA PATRIOT Act (Patriot Act), proposed several procedural, investigative, and substantive revisions, which are important to consider when analyzing the Computer Fraud and Abuse Act. Some of the largest of these revisions

include defining certain acts of computer crime as acts of "terrorism." Prior to the Patriot Act, no act of computer-related crime could be considered "terrorist" in nature. The Patriot Act increases penalties for certain acts of computer crime, and adds prominence to the concept of "national security" that did not exist before in the CFAA. The revisions also further clarify the definitions of "loss" and "damages" to victims of computer crime. The Patriot Act includes important changes that will increase the power of prosecutors in cases involving computer crimes (Podgor, 2002).

The Japan Unauthorized Computer Access Law

During the 1990s, a sharp increase in high-tech crime, and an increase in pressure from foreign nations to improve international cooperation in fighting high-tech crime lead Japanese law enforcement and law makers to realize the necessity to draft legislation that will empower the Japanese government in the battle against cyber-crime. In the years 1996 through 1998, the Japanese National Police Agency and the Ministry of Posts and Telecommunications conducted a number of studies and produced a number of reports in regards to unauthorized computer access and cyber-related crime. In April of 1999, the cabinet proposed the Unauthorized Computer Access Law (不正アクセス行為の禁止等に関する法律) to the Japanese Diet, under the cooperation of the National Police Agency, the Ministry of Posts and Telecommunication, and the Ministry of International Trade and Industry. In August, the Diet approved the legislation, and in February of the year 2000, the criminalization of unauthorized computer access and other articles came into effect (Saka, 2003).

The Unauthorized Computer Access Law criminalized the act of unauthorized computer access in which another's identification code (such as a password, etc.) is stolen, and security-hole related attacks. The penalty for violating this law is imprisonment with labor for not more than one year, and a fine of not more than ¥500,000[1]. A separate penalty of not more than ¥300,000 is reserved for a third party who gives out someone's identification code to another person.

Beyond the criminalization of unauthorized computer access, the law also stipulates security measures that must be taken by IT professionals and law enforcement agencies. The

[1] Approximately $5,000 U.S.

administrator of a network computer is legally obligated to manage access identification codes and ensure the security of the network's access control functions. When a computer network has been compromised, the local police are responsible for providing advice and assistance to the network administrators of the compromised system. The purpose of police guidance is to prevent recurrence of the crime that compromised the computer network (Grabosky & Broadhurst, Cyber-Crime:The Challenge in Asia, 2005).

The following graph provided by the Japanese National Police Agency, illustrates the structure of the Unauthorized Computer Access Law.

(Graph 1) Unauthorized Computer Access Law – Structure [Saka, 2003]

Major Differences between the UCAL and the CFAA

Both the United States' and the Japanese Governments passed their key pieces of legislature regarding computer and information security with similar purposes in mind: both countries needed to give their law enforcement greater power in preventing computer-related malicious activity, and thus help contribute to the development of a stable and strong information economy. Although both governments developed the American *Computer* Fraud and Abuse Act and the Japanese Unauthorized Computer Access Law with similar intent, a quick overview of the two laws alone will quickly alert any reader to major differences in the interpretation and treatment of computer crime. The differences in these two laws may be derived from differences in the legal systems, or to appropriately address cultural differences in the two different regions; however, such vast procedural and substantive discrepancies in the law are bound to produce vast discrepancies in the law's effects in application. This section intends to overview some of the major differences between the two laws that could lead to discrepancies in effect, interpretation, and application in society.

To start, the age-old conflict between Federalism and States-Rights pokes in throughout the American Computer Fraud and Abuse Act, leaving particularly strong marks on definitions and terms that set the scope of the statute's reach. The Japanese *Unauthorized* Computer Access Law, however, is not altered by the federal-vs.-state tension as the Japanese government is already much more centrist in its operations. An example of how this tension

manifests itself in the American law, appears in the definition of a “protected computer” in 1030 (e)(2).

> *“(2) the term "protected computer" means a computer--*
>
> *“(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or*
>
> *(B) which is used in interstate or foreign commerce or communication;”*

This definition of a “protected computer” limits the scope of the Computer Fraud and Abuse Act to protecting only computers that are part of a federal government agency, a financial institution, or computers involved in interstate or international commerce or communication. Any computer that does not fall into one of these categories is not protected under the federal CFAA, and any involvement in related crime would be handled by varying state laws. On the other hand, the Japanese Unauthorized Computer Access Law does not define any special form of “protected computer” and leaves open the interpretation that all computers that could be considered within Japanese jurisdiction would be protected under the act. These discrepancies in scope are manifestations of the differences in the two countries’ legal structures, legal traditions, and idea of what types of computer “fraud and abuse” are most important to address.

A very concrete difference to note is what activity is specifically outlawed by each of the acts. Although the acts are very similar in their intents, the activity that each outlaws is defined

differently. The Computer Fraud and Abuse Act specifically names several activities which are outlawed. The activities can be summarized as follows:

1) Obtaining National Security Information
2) Compromising the Confidentiality of a Computer
3) Trespassing in a Government Computer
4) Accessing a Computer to Defraud & Obtain Value
5) Knowing Transmission and Intentional Damage
6) Intentional Access and Reckless Damage
7) Intentional Access and Intentional Damage
8) Trafficking Passwords
9) Extortion Involving Threats to Damage a Computer

The Unauthorized Computer Accesss Law, however, only delineates one crime of "unauthorized computer access." The only action needed to be in violation of this law is "trespassing" in a computer or cyberspace beyond permitted access. No differentiation is made between intent, causing damage, or information related to national security. The crime of unauthorized computer access is defined in Article 3 of the statute (provisional English translation provided by the Japanese National Police Agency):

> *2. The act of unauthorized computer access mentioned in the preceding paragraph means an act that falls under one of the following items:*
> *(1) An act of making available a specific use which is restricted by an access control function by making in operation a specific computer having that access control function through inputting into that specific computer, via telecommunication line, another person's identification code for that access control function (to exclude such acts conducted by the access administrator who has added the access control function concerned, or conducted with the approval of the access administrator concerned or of the authorized user for that identification code);*
> *(2) An act of making available a restricted specific use by making in operation a specific computer having that access control function through inputting into it, via telecommunication line, any information*

(excluding an identification code) or command that can evade the restrictions placed by that access control function on that specific use (to exclude such acts conducted by the access administrator who has added the access control function concerned, or conducted with the approval of the access administrator concerned; the same shall apply in the following item);

(3) An act of making available a restricted specific use by making in operation a specific computer, whose specific use is restricted by an access control function installed into another specific computer which is connected, via a telecommunication line, to that specific computer, through inputting into it, via a telecommunication line, any information or command that can evade the restrictions concerned.

Article 4 of the statue also makes facilitating or assisting someone else in committing an act of unauthorized computer access illegal.

The actions criminalized by the Computer Fraud and Abuse Act are much more detailed in their description, and allow for much more differentiated penalties based on intent, whether or not damage occurred, and on the type of information that was illegally accessed or damaged. The Japanese act does not make such differentiations, and only applies one flat penalty. The penalties for violations of the CFAA can be summarized by the following chart:

Offense	Section	Sentence (Years Imprisonment)
Obtaining National Security Information	(a)(1)	10 (20) years
Compromising the Confidentiality of a Computer	(a)(2)	1 or 5
Trespassing in a Government Computer	(a)(3)	1 (10)
Accessing a Computer to Defraud & Obtain Value	(a)(4)	5 (10)
Knowing Transmission and Intentional Damage	(a)(5)(A)(i)	10 (20 or life)
Intentional Access and Reckless Damage	(a)(5)(A)(ii)	5 (20)
Intentional Access and Damage	(a)(5)(A)(iii)	1 (10)
Trafficking in Passwords	(a)(6)	1 (10)
Extortion Involving Threats to Damage Computer	(a)(7)	5 (10)

The Japanese *Unauthorized Computer Access Law* penal code is much more straightforward:

> *A person who falls under one of the following items shall be punished with penal servitude for not more than one year or a fine of not more than 500,000 yen:*
> *(1) A person who has infringed the provision of Article 3, paragraph 1;*
> *(2) A person who has infringed the provision of Article 6, paragraph 3.*
>
> *A person who has infringed the provision of Article 4 shall be punished with a fine of not more than 300,000 yen.*

It is important to note that the penalties outlined by the American statute are in general, more severe than those listed in the Japanese provisions. This may be due to the fact that several other pieces of Japanese legislation exist within that Japanese criminal code that address slander (第２３０条), fraud (第２４６条、第２４６条の２), destruction of digital data causing interference in work (第２３４条の２), and distribution of obscene materials (第１７５条), separately. In cases involving the Unauthorized Computer Access Law, interaction and involvement of the above criminal codes may be frequent, which would intensify the penalties faced by the defendant. These differences between the American and Japanese penalties may also be a result of trends in malicious computer activity and the situations leading up to the drafting of the two different pieces of legislation. Ultimately, the differences in penalty may have large affects in acting as deterrent to computer-related crime.

Another critical difference to note is an aspect that the Japanese law covers and the American law completely leaves out. The Japanese Unauthorized Computer Access Law identifies reasonable responsibilities for network administrators and local to which must be adhered. Network Administrators are required to ensure regular maintenance and functionality of a computer or network's "access control function." Local specialized police are

required to provide assistance to administrators in the case of a breach of the U.A.C. in order to prevent re-occurrence of the violation. No "reasonable requirements" are identified for computer administrators or police in the American act. Only provisions are provided to protect police and the Secret Service in investigating crime related to the *Computer* Fraud and Abuse Act. These differences may manifest in variations in prevention of computer fraud and unauthorized access between the two countries.

Current Trends

The Computer Fraud and Abuse Act

This section provides a high-level overview of recent violations and trends related to the American Computer Fraud and Abuse Act. Data is summarized from the United States Department of Justice Internet Crime Complaint Center, the Department of Justice Intellectual Property and Cyber Crime Division, along with some reports of academic studies. This section presents what is known about the general state of computer crime and the role of the Computer Fraud and Abuse Act in the United States, then provides some background as to which aspects of the CFAA are most frequently violated. Finally, some general problems and concerns surrounding the act and its enforcement are explored.

According to the Federal Bureau of Investigation's Internet Crimes Complaint Center (IC3), numbers in computer crime complaints have been steadily rising over the past decade. In 2008, the IC3 received 72,940 complaints. Of these complaints, the vast majority were about activities which were fraudulent in nature, involving financial loss. In 2008, the total dollar loss

from all referred cases totaled at approximately 264.6 million dollars, with a median of 931 dollars lost per complaint. These numbers are from the reported 239.1 dollars lost in 2007. Amongst the perpetrators, 77.4% were male, and 66.1% were from the United States. Large numbers of foreign perpetrators were reported to be from the United Kingdom, Nigeria, Canada, China, and South Africa (2008 IC3 Annual Report, 2008).

The number of cases actually convicted under the CFAA seems relatively small compared to the number of complaints received by the IC3. Considering the distribution of cases convicted under the CFAA, the majority of cases dealt with monetary fraud. Of convicted cases, 54% represented violations of subsection a(4), "General Fraud," and 24% represented violations of subsection a(2), "Accessed Financial Information." These results further the belief that the most common motivation for violations of the CFAA is monetary gain. The next largest convicted offense was "Password Trafficking," making up 12% of convicted cases (Nwokoma, 2008).

Similar to the Japanese Unauthorized Computer Access Law, major problematic trends include resistance from organizations to reporting criminal activity, and a lack of investigative resources. "In addition, fearful of negative publicity, corporations have an annoyingly schizophrenic attitude toward punishing offenders especially when the crime is committed by an employee," writes Professor Anele Nwokoma of Gambling State University. "There are cases where companies dismissed computer criminals but threw a lavish farewell party for the perpetrators to cover up the true reason for their departure. Even though computer crime is immoral, offenders are presently evading justice" (Nwokoma, 2008). Law enforcement also does not currently have the resources to properly and thoroughly investigate computer crime.

Without personnel who are trained in the collection of computerized evidence, important evidence to a case may be lost or destroyed. Both of these reasons can contribute to the seemingly low number of prosecutions in comparison to the high number of complaints related to computer-crime. The *Berkeley Technology Law Journal* has claimed evidence that the CFAA has done little in its existence to deter computer crime. It refers to the CFAA as "an overly punitive and largely ineffective approach to combating computer crime" (Skibell, 2003). The reference further indicates the complete dearth of attention paid to prevention and investigation by United States cyber-crime policy. The CFAA is frequently criticized for problematic trends related to its inability to address preventative and investigative measures.

The Unauthorized Computer Access Law

This section summarizes violations and trends related to the Japanese Unauthorized Computer Access Law, briefly summarizing what is currently understood of its effects in Japanese society. This is a short summary of statistics released by the Japanese National Police Agency, the Japanese Information-Technology Promotion Agency, the Ministry of Economy Trade and Industry, and the Ministry of Public Management, Home Affairs, Posts and Telecommunications. I first place the Unauthorized Computer Access Law in context with other computer crime in Japan, to understand the scope of occurrences. I then go into further details about the types of violations occurring within the Unauthorized Access Law itself. Finally, I comment on the state of reporting and prevention of crime related to the Unauthorized Computer Access Law.

Computer crime in Japan, following trends with the rest of the world, continues to be an increasing problem. When compared to the first-half of 2008, the first-half of 2009 saw a 76.6% increase in cyber-crime related arrests. Arrests due to violation of the Unauthorized Computer Access law increased 1151.6% in the first half of 2009 when compared to the first half of 2008. In addition, arrests due to violation of the U.A.C. contributed to 50.8% of all Cyber-Crime related arrests in 2009. As 1,965 arrests were made in relation to charges of Unauthorized Computer Access, one can definitely say the law is having impact on society (警察庁, 2009).

Interesting and important details also appear when one views the varieties of violations occurring within the Unauthorized Computer Access Law. Of 2289 total cases of Unauthorized Access known in 2008, 214 cases were suspects from foreign countries, 1193 of the suspects were Japanese citizens, and in 82 cases, the point of access was never uncovered. While the vast majority of reported incidents are Japanese suspects, a substantial international presence does exist, and may have implications on the importance of international legal harmonization. The top actions accomplished after the suspect achieved illegal computer access, included the manipulation of internet auctions and manipulation of on-line game systems. The overwhelming motivation was for the purpose of the illegitimate obtainment of money. The vast majority of suspects arrested were under the age of thirty, and more than 40% of the time, the victim was, at the very least, an acquaintance of the suspect (国家公安委員会, ２００９).

Despite the fact that the Unauthorized Computer Access Law, unlike the American Computer Fraud and Abuse Act, contains provisions to require network administrators to maintain their security access control functions, and for local police to provide support to

prevent cyber-crime (不正アクセス行為の禁止等に関する法律, 2000), the fallacies relating to reporting and preventing crime in regards to the U.A.C. are particularly notable. Small and medium size companies in Japan are lagging far behind in the creation of security policies for their information. As Harada (2003) explains, in 2003, less than 10% of small to medium sized companies claimed to have any security policy at all. In 2003, only about half of large Japanese firms had implemented any sort of security policy, and even within the firms that had implemented a policy, no group had demonstrated beginning a policy more than four years prior. A very limited number of Japanese companies even show awareness of security audits, as in 2003 only 20% of large firms, and 7.2% of small to medium size firms participated in such activity. In addition, the violation statistics provided only show the tip of the ice berg in terms of actual Unauthorized Access activity, as studies show that less than 10% of small to medium sized companies reported incidents, unless major damage was suffered. Individuals and home users show similar attitudes (Harada, 2003). This could be due to a fear of possible negative publicity, and the trouble of an investigation deters users from reporting incidents.

This summary illustrates the state of the Unauthorized Computer Access Law. While known cases and arrests related to the law are growing, reporting and prevention remain a major problem. In the field of cyber-law today, where the limits of government and law enforcement are so clearly restricting, reporting and prevention becomes even more important. In the field of cyber crime, problems in these areas could be particularly detrimental to the safety and protection of a high-performing information society.

Research Design

Overview

Comparing two broad policies and each policy's effects in two separate nations, is an enormous task. The number of variables and stakeholders to measure is seemingly uncountable. Not to mention, "effectiveness" in policy is very subjective to different stakeholders; perspectives; as well as moral, ethical, and cultural backgrounds. This research design section provides an overview of the methods used to collect data and the procedures used to analyze to draw meaningful conclusions. This section also introduces the three types of data collection employed (interviews, surveys, and document analysis), explains why each method was chosen, and also demonstrates how the different pieces of data collection complement one another and work together to produce a comprehensive collection of information from which conclusions and results are drawn.

Research Questions

The research questions explored in this thesis were formed from the analysis of previous research conducted during the literature review process. Through this research and writing process of the literature review, I identified that two primary purposes of both the American Computer Fraud and Abuse Act and the Japanese Unauthorized Computer Access Law are to deter and enable the prosecution of various computer-access and computer-fraud related crimes, as well as to provide for the growth of a prosperous information economy in each law's respective country. Hence, the research questions were formed in a way to both

guide the research to measure each law's performance in achieving both of these goals, as well as to encourage analytical comparison of findings related to both pieces of legislation. The research questions are as follows:

1) How effective is the Computer Fraud and Abuse Act, including its revisions in the 2001 Patriot Act, in protecting American electronically-stored data from unwanted access, reproduction, or destruction?
    a. In what ways is it effective?
    b. In what ways is it ineffective?
    c. How does it interact with other American laws in achieving its aims?
2) How effective is the Japanese "Unauthorized Computer Access Law" in protecting its electronic data from unwanted access, reproduction, or destruction?
    a. In what ways is it effective?
    b. In what ways is it ineffective?
    c. How does it interact with other Japanese laws in achieving its aims?
3) Do these two policies build users' trust in the security of information, thus promoting a sound information economy?
4) Based on the comparison of the policies of the two nations, what recommendations can be made to policy makers to improve the current legislation?

Methodological Approach

Overview

In order to determine and compare the effectiveness of the American Computer Fraud and Abuse Act, and the Japanese Unauthorized Computer Access Law, I conducted a policy analysis on each law then drew comparisons from the results. The research questions identified two major goals of the CFAA and the UCAL as the prevention and prosecution of computer crime as well as the promotion of a sound information economy. In order to complete a manageable comparative study of the two policies, I investigated several varying "cross-sections" of stakeholders of each policy and then aimed to triangulate the findings to recurring themes related to the research questions. When performing an analysis of policy with an immeasurably wide scope and influence, it is helpful to take such cross-sections of stakeholders across the wide spectrum of the policies' influence and then compare and triangulate findings from each cross-section in order to prevent errors associated with having a limited perspective (Dunn, 1994). Research was conducted in both the United States and in Japan. Research methods used include interviews, surveys, and document analysis. Each method of research was used to target a separate stakeholder group. Once data was collected, the results of the different methods of investigation were analyzed and compared in order to identify what policy-makers in each country could learn from the other county's experiences.

Once the research data was collected, I used this comparative analysis to produce recommendations and considerations for future policy making.

Multiplism/Triangulation

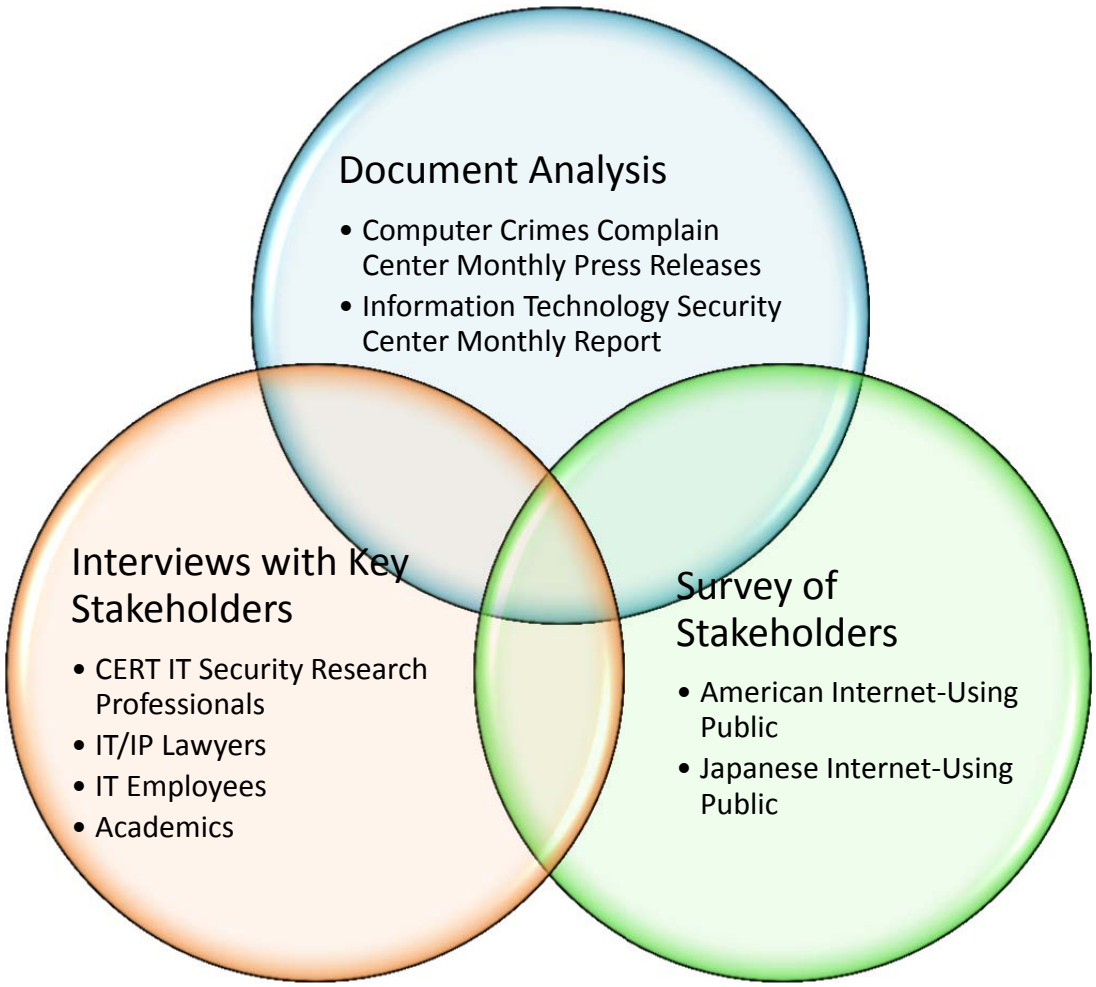
Due to the complexity of the scope and effects of public policy, as well as to limit errors due to limited perspective, I used a method of analysis referred to as "Critical Multiplism." Critical Multiplism represents a creative synthesis of a broad range of research and analytic practices advocated and used by a cross section of the policy science community. Inductive plausibility, as opposed logical certainty, is central to the method of multiplism (Dunn, 1994). In order to prevent the most common errors of limited perspective within policy analysis, multiplism focuses on synthesizing and critically assessing multiple methods, operations, hypothesis, perspectives, and variables.

Multi-Aspects

The research methodology applied theories of critical multiplism in the following ways:

Multi-Method Research

The multiple methods of research can be quickly visualized through a simple venn diagram. Several methods of research are conducted. The results of each method are then compared in order to find intersections and points of interest from which conclusions can be drawn.


Document Analysis
• Computer Crimes Complain Center Monthly Press Releases
• Information Technology Security Center Monthly Report
Interviews with Key Stakeholders
• CERT IT Security Research Professionals
• IT/IP Lawyers
• IT Employees
• Academics
Survey of Stakeholders
• American Internet-Using Public
• Japanese Internet-Using Public

Multi-Analytic Analysis

Multi-Analytic Analysis was partly achieved through the comparison of the American and Japanese policies. In addition, research on similar policies and their effects within each country are cited as a part of the document analysis.

Multiple Stakeholder/Perspective Analysis

Multiple Stakeholder/Perspective analysis was achieved though the inclusion of a broad spectrum of stakeholders in the interview and survey process. Questions were designed to capture different ethical, political, organizational, economic, social, cultural, psychological, and technical perspectives.

Multiple Communications

As Policy Analysis does not end with simply the results, measures were taken to ensure that information is disseminated in a way that it may become policy-relevant knowledge. Beyond the standard academic thesis, a simple, easy-to-access, web publication of the major results has been created and can be accessed at: http://ryanhcmu.wordpress.com/

Research Methods Table

Evidence from the multiple research methods, analyses, and perspectives were appropriately triangulated to communicate policy-relevant knowledge as results. The following table summarizes how this triangulation occured. The table separates each research method, identifies the target stakeholders of the research method, the topics covered by the research method, the perspectives that the method helps analyze the policies from, and finally what qualitative "metric" the method addresses. It is an easy-to-reference map of the types of research conducted, why each method was used, and how the different methods relate with one another to produce a cohesive set of data from which to draw inferences.

Method	Who	Topics	Perspectives	"Metrics" Addressed
Surveys	Internet Using Individuals (Ages 18+) US and Japan	*Knowledge of Law *Feeling of Safety *"Policy's" effect on personal usage	*Personal -Cultural -Social -Ethical -Psychological	*Feeling of Security *Awareness
Interview	Law/Policy Professors US and Japan	*Background *Problems with Information Security Policies/Issues *Success with I.S. Policy *General Questions about Cyber-Law Theory *Ethics of CFAA and UCAL *Identifying other sources	*Personal *Organizational -Cultural -Social -Ethical -Political -Economic	*Prosecutorial Power *Use in Defense *Interactions with other laws *Awareness
Interview	Lawyers	*Procedural Questions *Differences in working with CFAA/UCAL in comparison with other Laws	*Personal *Organizational *Technical -Cultural -Social	*Investigative Power *Prosecutorial Power *Use in Defense

		*Trends in Cases *Interaction with "Other" Laws *Identifying other Sources	-Ethical -Political -Psychological	*Interaction with other laws *Awareness *Reducing crime
Document Analysis	Press Releases	*What kind of cases get attention? *Who hears about these cases? *How are the "stories" portrayed? *Number of Press Releases	*Organizational *Personal -Cultural -Social -Political -Psychological	*Awareness *Feeling of Security *Reducing crime *Investigative Power

Data Analysis Approach

In the process of data analysis one tries to "discover patterns and themes in the data and to link them with other patterns and themes," and turns raw data into results" (LeCompte & Schensul, 1999, p. 3). Qualitative data analysis commonly entails first coding collected data; next, adding memos containing comments and reflections; afterwards, going through the codes to identify patterns, themes, sequences, similarities and differences between sub-groups, and relationships; and finally, making generalizations that cover consistencies in the data and linking them into formal constructs and theory (Robson, 2002). In order to identify patterns and themes and turn the raw collected data into meaningful knowledge-building results, I followed a very similar pattern to that described by Robson. In the following section, which details the specific purposes and logistics of each of the three major types of data collection conducted in this study, I provide the specifics for the methods of coding and identifying themes and patterns in the data that I employed while conducting this study.

The rest of this section explains the methods of research used, the target stakeholder groups for each method of research, and to what purpose each method of research was conducted in detail. The explanations are divided by research method.

Interviews

Method	Who	Topics	Perspectives	"Metrics" Addressed
Interview	Law/Policy Professors US and Japan	*Background *Problems with Information Security Policies/Issues *Success with I.S. Policy *General Questions about Cyber-Law Theory *Ethics of CFAA and UCAL *Identifying other sources	*Personal *Organizational -Cultural -Social -Ethical -Political -Economic	*Prosecutorial Power *Use in Defense *Interactions with other laws *Awareness
Interview	Lawyers	*Procedural Questions *Differences in working with CFAA/UCAL in comparison with other Laws *Trends in Cases *Interaction with "Other" Laws *Identifying other Sources	*Personal *Organizational *Technical -Cultural -Social -Ethical -Political -Psychological	*Investigative Power *Prosecutorial Power *Use in Defense *Interaction with other laws *Awareness *Reducing crime

Purpose

The primary purpose of the interview phase was to gain insight into the "expert" stakeholders' views on the CFAA and the UCAL. In addition, the interviews allowed me to

gather expert opinion related to the laws' promotion of investigative and prosecution power, awareness of policy in the professional realm, as well as how the CFAA and UCAL interact with other pieces of legislation to either achieve, or not achieve, their intended goals.

Logistics

Interviewees were recruited primarily through networking of professional contacts, using e-mail and phone calls. A few of the candidates were identified because of their publications, and were then e-mailed or called to be invited to participate in an interview.

Interviews of stakeholders primarily took place on the Carnegie Mellon University campus during the fall of 2009, and on the Temple University of Japan Campus, where I studied during the spring of 2010. Interviews of experts took place in public settings, and at Carnegie Mellon and Temple University Japan Campus sites. I used Skype video calling to converse with interviewees when a physical meeting was not possible.

Interview guides were developed and based on a semi-open ended interview form. Interview guidelines were preferred to highly-structured interview scripts and questionnaires so as not to overlook important details that might relate to each specific interviewee's field of expertise. The interview guides are included in Appendix I.

Participant Demographics

Research consisted of individual interviews of both "expert" stakeholders in the field of cyber-law and computer forensics. Research consisted of United States CERT Computer Security research specialist, a United States CERT affiliated technology and an intellectual

property lawyer. In order to protect the privacy of respondents, aliases have been selected to represent the names of each interviewee. The descriptions of their positions and experiences, as well as their responses to interview questions, have been preserved accurately. The following table provides an at-a-glance overview of the participants in the interview process and can be used to quickly understand what perspectives each interviewee brought to the discussion.

Alias	Educational Background	Work Experience
David Filp	PhD. Information Studies	Assistant Teaching Professor of Information Systems 3 Years at CERT[2] (USA) Navy Information Warfare Officer
Jessica Anderson	Masters Electrical Engineering	Senior Researcher/Member of Technical Staff (CERT) Former Deputy Director of SEI[3]
Alex Moot	Masters Computer Science	Senior Member of Technical Staff (CERT-SEI) Computer Security Researcher at US Naval Research Laboratory
Susan Connelle	J.D., MBA	SEI Counsel – Director of Business Development Background in Contracts and IP Law

[2] CERT stands for "Computer Emergency Response Team." It is a government established information security research, response, and coordination organization established in 1988.
[3] SEI stands for "Software Engineering Institute" and is affiliated with Carnegie Mellon University.

Samples of interview guides used are attached in Appendix I.a.

Data Analysis Procedure

To analyze the data collected through the interviews, an iterative, bottom-up, inductive approach to coding and theme identification was used. An inductive analysis "produce[s] items in the form of those events, behaviors, statements, or activities that stand out because they occur often; are crucial to other items; are rare and influential; or are totally absent, despite the researcher's expectations" (LeCompte & Schensul, 1999, p. 69). Due to the nature of the interview data collected being voice recordings and manually typed MS Word document notes, this inductive coding procedure was done manually. Each interview recording and associated notes were reviewed several times, and reflective notes were taken on text or ideas that came up more than once, that stood out as a rare or emotionally charged response, or on ideas or items that were totally absent from the data set despite my expectations. These reflective notes were then again reviewed to identify repetition and patterns, upon which themes could be identified and used to draw meaningful conclusions.

Surveys

Method	Who	Topics	Perspectives	"Metrics" Addressed
Surveys	Internet Using Individuals (Ages 18+) US and Japan	*Knowledge of Law *Feeling of Safety *"Policy's" effect on personal usage	*Personal -Cultural -Social -Ethical -Psychological	*Feeling of Security *Awareness

Participants in this aspect of the study were asked to complete a web-based survey about their feeling of safety while using the internet and their awareness of federal information security policies. The survey took approximately 10 minutes to complete. Questions included behavior and feeling of security on-line. Questions also covered awareness of current policy. A copy of the questions of this survey can be found in Appendix B.

Purpose

Surveys of general internet users were conducted to gauge public awareness of the CFAA and the UCAL, gauge general internet users' feeling of security using networked computers, as well as determine if the laws being studied had an effect on that public sense of confidence. The assumption is that Internet user's feelings of security and behavior play a role in the development of an "advanced information economy," so if users do not feel safe using networked computers, that would be detrimental to the development of a sound information economy will indicate room for improvement in policy.

Logistics

Participants were largely gained through professional and academic contacts who distributed the survey materials on paper by hand. In addition, many participants were gained through on-line e-mail and social networking solicitation. Participants who took the survey in a classroom setting all took the survey by hand with paper, while about half of the participants took the survey on-line through a personal computer.

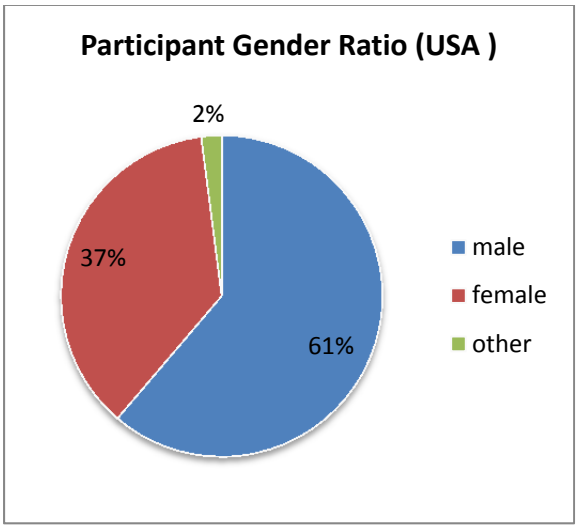
Participant Demographics

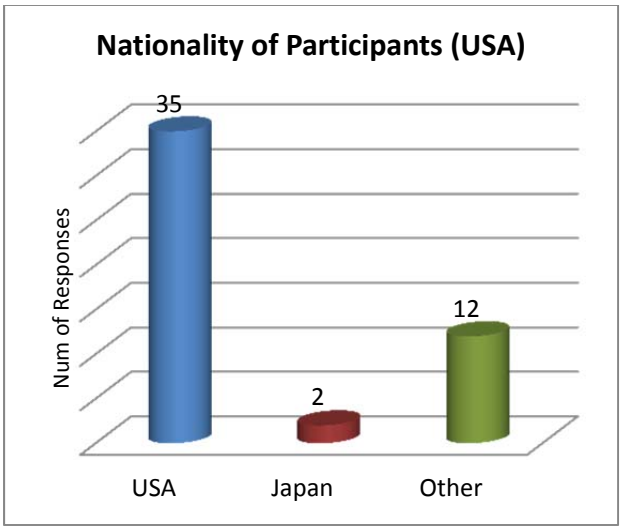
No one was intentionally excluded from this study on the basis of race, gender, religious beliefs, sexual orientation, disability, etcNo one was excluded from this study on the basis of race, gender, religious beliefs, sexual orientation, disability, etc. Participation in this study was open to anyone over the age of 18. No person under the age of 18 participated in this study.

Data related to participant demographics are included in the charts below.

United States Survey Demographics

Total Responses: 49
Average Age of Respondent: 19.27

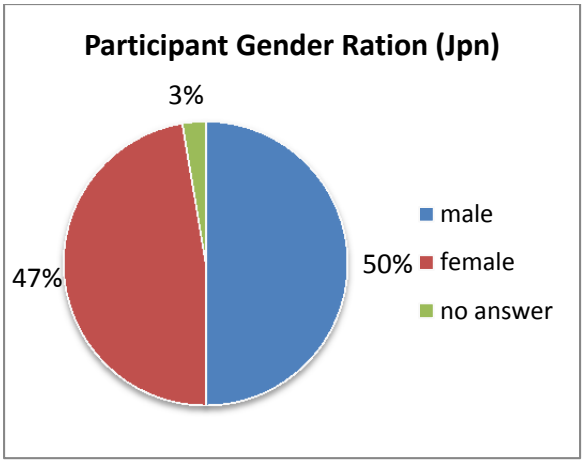


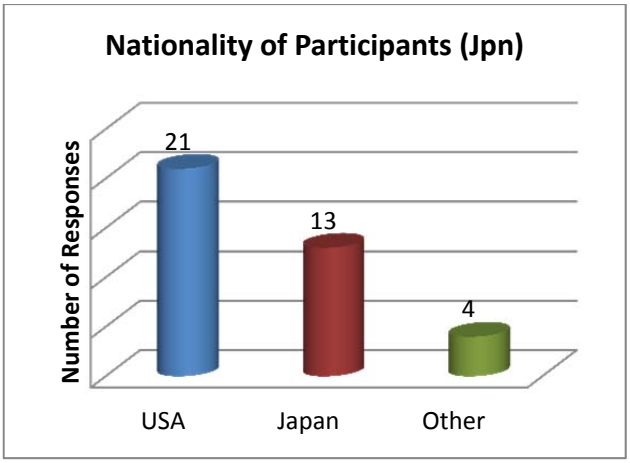


Nationalities Represented by "Other" Category: India, South Korea, China, Taiwan, Sudan

Japan Survey Demographics

Total Responses: 38
Average Age of Respondent: 23.06





Nationalities Represented by "Other" Category: Vietnam, Sweden, Taiwan

Data Analysis Procedure

Once survey responses were collected, similar to the other methods of data analysis, a bottom-up method of analysis was used to first identify patterns in the data, group identified patterns into themes, and then match those themes to research questions. To review the data and identify patterns and points of interest, the data collected from paper surveys was imported into Microsoft Excel. Excel was used to calculate sums, averages, and create visual representations of the data for comparison. The graphs and calculations created from the surveys are included in the Data and Findings section of this report.

Examples of the surveys used are attached in Appendix I.b.

Document Analysis

Method	Who	Topics	Perspectives	"Metrics" Addressed
Document Analysis	Press Releases	*What kind of cases get attention? *Who hears about these cases? *How are the "stories" portrayed?	*Organizational *Personal -Cultural -Social -Political -Psychological	*Awareness *Feeling of Security *Reducing crime

This part of this research consists of conceptual document analysis, in which through selective reduction, categories of words, sets of words, and phrases are identified, and the presence and frequency of these words are coded in a set of chosen documents that relate to decided research questions. Through conceptual content analysis one is able to reveal international differences in communication content; detect the existence of propaganda; identify the intentions, focus or communication trends of an individual, group or institution; describe attitudinal and behavioral responses to communications; and even determine the psychological or emotional state of persons or groups. Because of what one is able to learn about social conditions through conceptual analysis, it is an appropriate methodology to address my research questions.

This section identifies the process I employed for the conceptual analysis in my research. I identify which documents were included in the dataset and why these documents were selected. I identify the process with which I encoded the documents. By making explicit these

details of the techniques employed, I mitigated risks of inconsistency in document coding that could lead to reliability and validity issues in results. As a whole, this section provides an explanation of how I employed conceptual analysis to address the research questions.

Purpose

By comparing how major research institutes release their findings, and how they frame their public notices, I investigated public awareness of the CFAA and UCAL. In addition, I gained insight into how secure the public may feel, as feelings of security may translate into network and internet usage behavior, which would certainly have effects on "the development of a sound information economy."

Sources

From every other year since 2003, I will select one document per quarter from the following two sources.

1st quarter: Jan-Mar

2nd quarter: Apr-Jun

3rd quarter: Jul-Sep

4th quarter: Oct-Dec

Document Source/Type	Topics Addressed	Perspectives	Research

			Questions
IC3 Press Releases **http://www.ic3.gov/media/default.aspx**	(American) *What does the IC3 value as important enough to report *What impression is the public being given of cyber-crime *How is "law" portrayed in these reports (if at all)	*Personal *Organizational	1(a,b), 3, 4
Japanese Information Technology Promotion Agency Monthly Reports **http://www.ipa.go.jp/security/english/monthly_vir_backnum.html** **(Part I "Reminder" sections only)**	(Japanese) *How is cyber-crime portrayed to the "public"? *How is the "law" portrayed in these reports. (Is it at all?) *What does the IPA value as important enough to report.	*Personal *Organizational	2(a,b), 3, 4

Coding Procedure

As opposed to the surveys and the interviews, a more top-down approach to selecting themes was applied to the document analysis. First, from what I determined as the purpose of the document analysis I chose a simple set of major themes to detect. I then identified words that would represent the presence of these themes in a bottom-up fashion, by manually reading through each article and collecting a list of words that appeared in each article that related to each theme in question. Next, qualitative analysis software was used to perform

word searches through all documents with all of the words in the previously assembled lists. Finally the qualitative analysis software was used to group results from different groupings in articles to see if any trends appeared over time. Themes, word lists, and results identified are available in the Data and Findings section of this report.

QSR N6 Qualitative Research Software was used to conduct the analysis of the texts. Texts were copied into .txt format from their published html format in order to be analyzed.

More information regarding the QSR N6 software can be found at:

http://www.qsrinternational.com/FileResourceHandler.ashx/RelatedDocuments/DocumentFile/90/N6_features_and_benefits.pdf

Data and Findings

Overview

The following section provides a detailed summary of the data that was collected via the methods described in the Research Methodology Chapter. The research findings here are organized by the research method through which they were collected. These methods included interviews, surveys, and document analysis.

Interviews

Overview

The responses of the interviews of American experts can largely be associated with research questions 1 and 3:

1) How effective is the Computer Fraud and Abuse Act, including its revisions in the 2001 Patriot Act, in protecting American electronically-stored data from unwanted access, reproduction, or destruction?
    a. In what ways is it effective?
    b. In what ways is it ineffective?
    c. How does it interact with other laws in achieving its aims?
3) Do these two policies build users' trust in the security of information, thus promoting a sound information economy?

A major piece of this data, is the relation to question (1.c.), "How does it [the CFAA] interact with other American laws in achieving its aims?" Though each is an "expert stakeholder" in the field of information security and computer crime, each interviewee has his or her own unique field of expertise, and unique vantage point from which he or she looks at the relationship between the law, organizations, and standard internet users. Each expert interviewed mentioned different experiences with different government bureaucracies and policies, and thus each gave a unique and informed perspective on how the CFAA might fit into the puzzle of an overall governmental "cyber law strategy," and how the CFAA interacts with other United States policies. Interviewees also revealed, sometimes indirectly and sometimes directly, how these relationships between the CFAA and other policies affect the efficacy of the CFAA in achieving its stated goals.

Also, in relation to question (3), all interviewees expressed either a lack of knowledge, and/or a belief that some measures related to a policy critically tied to the success of the CFAA, was suffering some sort of short-falling, and thus rendering the CFAA short of its potential. This demonstrates a short-falling in either the CFAA policy itself, or in the advertisement and application of the law.

Federal Law System and Confusion

Professor David Filp brought an interesting point to attention in his interview that was previously predicted as a possible point of interest in the previous literature review section of this paper, and thus it has been highlighted as a theme for analysis. As predicted in the

literature review, Professor Filp, in response to the question, "What do you believe to be the purpose of the CFAA within the United States Government's approach to cyber-law?", responded by sharing his opinion about the CFAA's role as a federal law in relation to state and local law, and how that relationship relates to the efficacy of the CFAA.

First, Professor Filp emphasized that it is hard to see the CFAA's direct impact on cyber-crime and the theft and destruction of electronic data because of the multi-tier federal system of laws in the United States. Professor Filp mentioned that many state laws exist relating to cyber-security, and many computer criminals could be prosecuted under these state laws. However, Doctor Filp also mentions that "states don't track that information very well." Beyond this, Doctor Filp adds that it is often times easier to prosecute a computer-related crime under a non-computer related statute at the state or federal level. It is also almost impossible to gather how many crimes could have been prosecuted under the CFAA that instead were prosecuted under different state laws. With so many possible layers of applicable legislation, and with record keeping that makes it difficult to gather and compare prosecution from all states and the federal level, it is hard to understand what the CFAA is really achieving in the greater picture of cyber-crime in the United States.

Importance of Response Team and Forensics

The importance of response teams, forensics, and law enforcement to the success of the CFAA arose multiple times throughout almost every interview. Through each interviewees perspectives on the importance of response teams and enforcement to the success of the CFAA, one can also gain a better perspective on the dependence of the CFAA on the policies and laws

of various other government bureaucracies and institutions, as well as the CFAA's dependence on foreign government's policies and law enforcement infrastructures in order to operate effectively as a protector of Americans from computerized crime. These relations go towards addressing research question 1.c., "How does it [the CFAA] interact with other laws in achieving its aims?"

Mr. Alex Moot first touched on this issue when he mentioned that evidence collection problems can frequently lead to an inability to prosecute within an organization. Mr. Moot graciously divulged the contents of his research, which is part of the Software Engineering Institute's CERT (Computer Emergency Response Team), a federally funded institution for research and coordination of computer crime emergency response and forensics. Mr. Moot's research is related to a specific set of commuter crime activity classified as "insider threat." Insider threat refers to crimes in which the perpetrator is an employee, business partner, contractor, or any person who already has legal access to an organization's systems, who then either uses that access or exceeds that access in order to perform fraudulent activity such as stealing, reselling, or destroying digitally stored data. The purpose of Mr. Moot's research is to understand the risk of insider threat to prevent the crime in the first place but also to provide law enforcement with what sorts of evidence they can and should look for in a computer crime case and also inform organizations on how they can properly design their systems to legally and ethically maintain necessary evidence in the case of a disaster. Mr. Moot's words and his federally funded research are one testimony to the important connection between response team/law enforcement policy and the CFAA.

To add to Mr. Moot's testimony, Mz. Jessica Anderson, the former Deputy Director of Mr. Moot's organization, explained how their organization came to be and also came to be funded, which also demonstrates an interdependent relationship between certain government bureaucracies and the CFAA. According to Mz. Anderson, the institution that both Ms. Anderson and Mr. Moot research for was founded and funded in reaction to the 1988 Morris Worm, which is said to have "taken down" 15 to 25 percent of research centers on the ARPA Net (predecessor to today's internet). The FBI established an emergency response center in 1988, and CERT was formed as an operational response center. CERT continues to serve as a response center which is critical for coordinating law enforcement and collecting evidence which is critical in Computer Fraud and Abuse Act cases. Since CERT is dependent on funding from federal bureaucracies, and since CFAA cases rely on the work of CERT and computer-crimes response teams, Ms. Anderson's explanation about CERT's relationship to federal bureaucracies further illustrates how the CFAA is affected by other government institutions' policies.

Professor Filp added an additional level to this theme by introducing the international aspect of the importance of a well-coordinated response team to collect evidence for prosecution. In Professor Filp's opinion the most difficult part of dealing with an international computer crimes case is working with response teams at the national level. In an ideal case, national response teams would provide liaisons to facilitate law enforcement coordination between the two countries. However, a country may not even have a central coordination center to help facilitate this action. This would make collecting evidence much more difficult, and perhaps make prosecution of a case nearly impossible. Hence, Dr. Filp emphasizes the

importance of proper training of law enforcement in all countries, which in his opinion is currently underperformed even within the United States. As internet crime knows no physical borders, and a suspect may live just about anywhere in the world, this situation demonstrates the great interdependence of the CFAA upon foreign governments' institutions, policies, and laws in order to be successfully implemented in protecting Americans from computer crime and for appropriately prosecuting computer criminals.

Interference with Evidence Collection

Ms. Connelle, an intellectual contracts and property lawyer working for CERT, raised some interesting points related to research question 1.c. "How does it [the CFAA] interact with other laws?" I have chosen to raise Ms. Connelle's point here as a theme for analysis.

Ms. Connelle mentions that Wiretap and Employment Laws often make it more difficult to collect evidence and prosecute under the CFAA. Organizations are prohibited from certain kinds of on-line monitoring conduct without employee permission. Employment law, for example, protects certain minority classes from targeted monitoring, so organizations have to be very careful about their policies or any action taken against an "insider threat case" may be rejected in court due to an organization's violation of employment law. Ms. Connelle states,

> *"There is policy debate with respect to not just cyber-crime, but there is a pull between 'right to privacy' and protecting everyone for cyber-crime, just like terrorism. How far are we going to go to protect classes before we are all in danger? "*

An effective wire-tap and employee law help protect from unethical discrimination, but may also hinder the CFAA from being effective against true cyber crime. Striking an appropriate balance between safety, freedom, and privacy seems to be a constant struggle, and is extremely difficult to achieve in all cases.

The Technology Issue

Another opinion that appeared repeatedly throughout all of the interviews was that the territoriality and jurisdiction issues that the CFAA and other forms of cyber-law face will not be resolved in the future by additional policy changes and legislation, but by technology changes. Several interviewees re-iterated the position that the problem may not be one of policy, but one of technology.

For example, Ms. Connelle explained her stance on the matter with an analogy. She stated:

> *"In poor countries in Africa, they just skipped and went to cell phones. The Internet is the 'land line' infrastructures. We need to skip to some new kind of technology to make us more secure. The Deputy Director for Intelligence for the Navy says that 'everything' can be broken into. Technology will be the answer."*

From Ms. Connelle's perspective, it sounds as if only a new networking infrastructure will be able to resolve the borderless crime problems of today.

Dr. Filp and Ms. Anderson also support this point with their stances on the relation of law and technology. Dr. Filp mentions that "legislators often want to be seen as doing

something," and thus they "re-actively address a problem they felt as growing." Ms. Anderson also adds that law is "rarely a catalyst." "Law lags action," she says. Both Dr. Filp and Ms. Anderson suggest that law is too slow and reactionary to serve as a primary actor in a solution to the border problem.

Ms. Connelle also provided an example of her own idea which addresses the technology issues she had addressed. She suggested that "governments may fund 'ideas' that may jump the technological leap to solve these issues."

Lack of Awareness

Lack of knowledge or awareness of the Computer Fraud and Abuse Act came up consistently in every interview, despite the fact that each of the interviewees may be considered an "expert" in the field of information security. Professor Filp seemed to be one of the most aware interviewees of the Computer Fraud and Abuse Act and its contents, claiming to have been exposed to it during courses about cyber-law that he had taken. Mr. Moot, when asked if he was familiar with the CFAA responded with,

> *"Not Really. Heard of it before today though. [The law was] often cited in the cases as what the insiders [suspects in my insider threat research] are prosecuted under."*

Mr. Anderson also responded that she only knew of the CFAA at "a very high level." It is clear that even these experts in the field of information security are unfamiliar with what is explicitly legal or illegal as outlined by the CFAA.

Summary

As the experts that were interviewed had various different backgrounds of expertise, a wide variety of themes were identified within the interview data. Several of the themes provided strong insight into how the Computer Fraud and Abuse Act was effected by and worked with other policies to achieve its aims. Several of the experts' responses indicated that some policies actually make it harder for the CFAA to be utilized as an effective tool for prosecuting computer crime. The importance of government bureaucracies both domestically and abroad at being efficient and establishing proper computer crime response and forensics teams was emphasized multiple times by multiple interviewees. The federal system of law in the United States also makes understanding the CFAA's role within the legal framework of the entire nation more complicated, and it also makes it harder to measure and assess the CFAA's importance. It also became clear that even amongst the information security and information security policy experts interviewed there was little collective familiarity with the CFAA and its contents. Finally, several of the experts asserted that the CFAA or any legal policy will not be the answer to alleviating issues of cyber-crime, and instead the answer will come through future technological advancement.

Surveys

Overview

The surveys conducted brought results that can be related to three of the primary research questions:

1) How effective is the Computer Fraud and Abuse Act, including its revisions in the 2001 Patriot Act, in protecting American electronically-stored data from unwanted access, reproduction, or destruction?
    a. In what ways is it effective?
    b. In what ways is it ineffective?
    c. How does it interact with other American laws in achieving its aims?
2) How effective is the Japanese "Unauthorized Computer Access Law" in protecting its electronic data from unwanted access, reproduction, or destruction?
    a. In what ways is it effective?
    b. In what ways is it ineffective?
    c. How does it interact with other Japanese laws in achieving its aims?
3) Do these two policies build users' trust in the security of information, thus promoting a sound information economy?

A primary focus of the surveys conducted was to identify how the CFAA and the UCAL have been working to achieve success related to building users' trust in the security of information,

thus promoting a sound information economy. This directly relates to research question number three. Questions on the survey were designed to measure both feelings of safety when performing certain activities on networked computers, as well as measure actual activities performed by users on networked computers. In addition, the survey asked questions related to awareness of the CFAA and the UCAL so that conclusions could be drawn in relation to whether the feelings of safety or insecurity that users experienced while working online had anything to do with the policy or not.

In addition, measuring awareness of the policy has an additional effect that relates to research questions one and two. If the policy is effective in deterring people from committing computerized crime, then people would have to be aware of the policy and related punishments. Thus, measuring public awareness of the law also can serve as an indicator as to whether the law is affecting the public's behavior.

Knowing Who's on the Other Side

Through results of the surveys, it is clear that internet users in both the United States and Japan do not have trust in the law or the limits of technology to protect them or their personal information. However, this is not scaring users away from using on-line mediums to make economic transactions entirely. The results of this survey show that, in both the United States and in Japan, the most important factor of whether a user has trust in the security of his or her information, and whether or not that user will engage in economic interaction on-line,

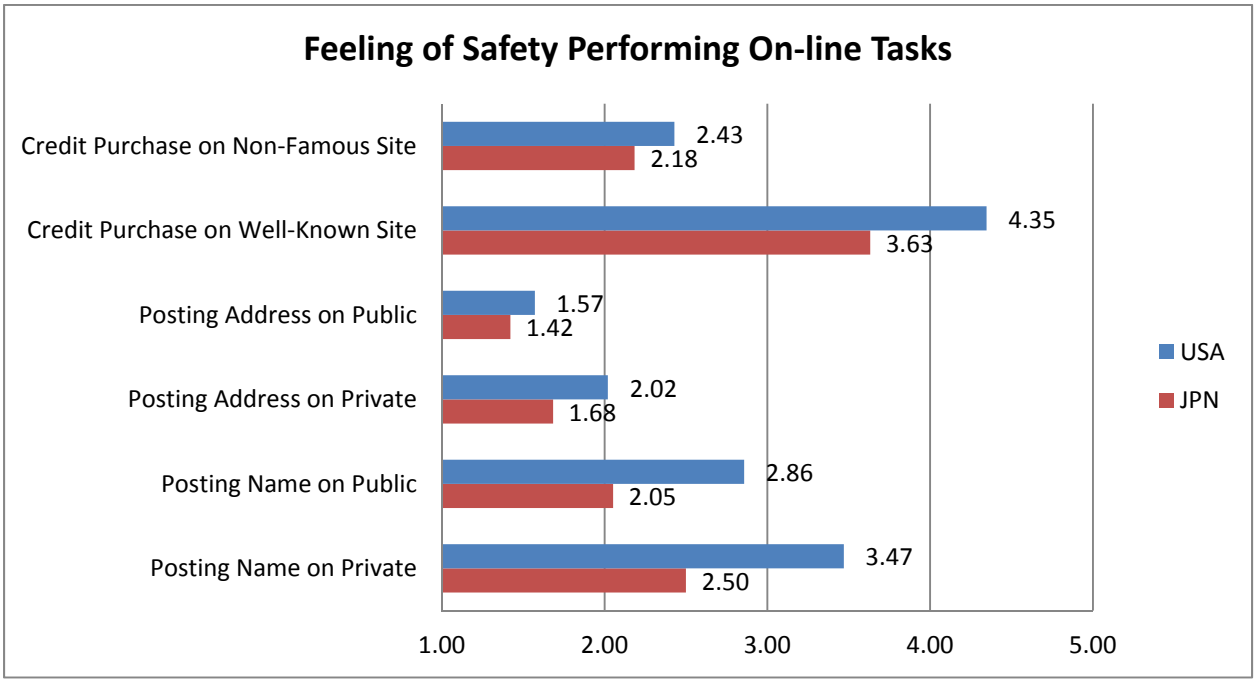
involves whether or not that user has knowledge of and trust in the other user, business, or organization on the other side of the network or system. Survey results relating to how safe users feel on-line, what qualities of a system make a user feel safe, and answers regarding on-line behavior, all contribute to this conclusion. This conclusion has direct relevance to research questions one, two, and three.

How to Feel Safe On-Line

Part of the first series of questions asked to participants in the survey involved requesting of participants to rank how safe they felt on a scale of one to five ("1" representing feeling the most unsafe, "5" representing feeling completely safe), how safe he or she felt performing certain activities on-line. The activities asked are as follows:

1) Posting your full-name on a social networking service or private blog
2) Posting your full-name on-line on a public blog or open forum
3) Posting your address on-line on a social networking service or private blog
4) Posting your address on a public blog or open forum
5) Making purchases with your credit card information on-line at a well-known on-line store
6) Making a purchase with your credit card on-line at a site that you have not been to or heard of before

The answers users provided on a scale of one to five were averaged, and those results are displayed in the charts below.

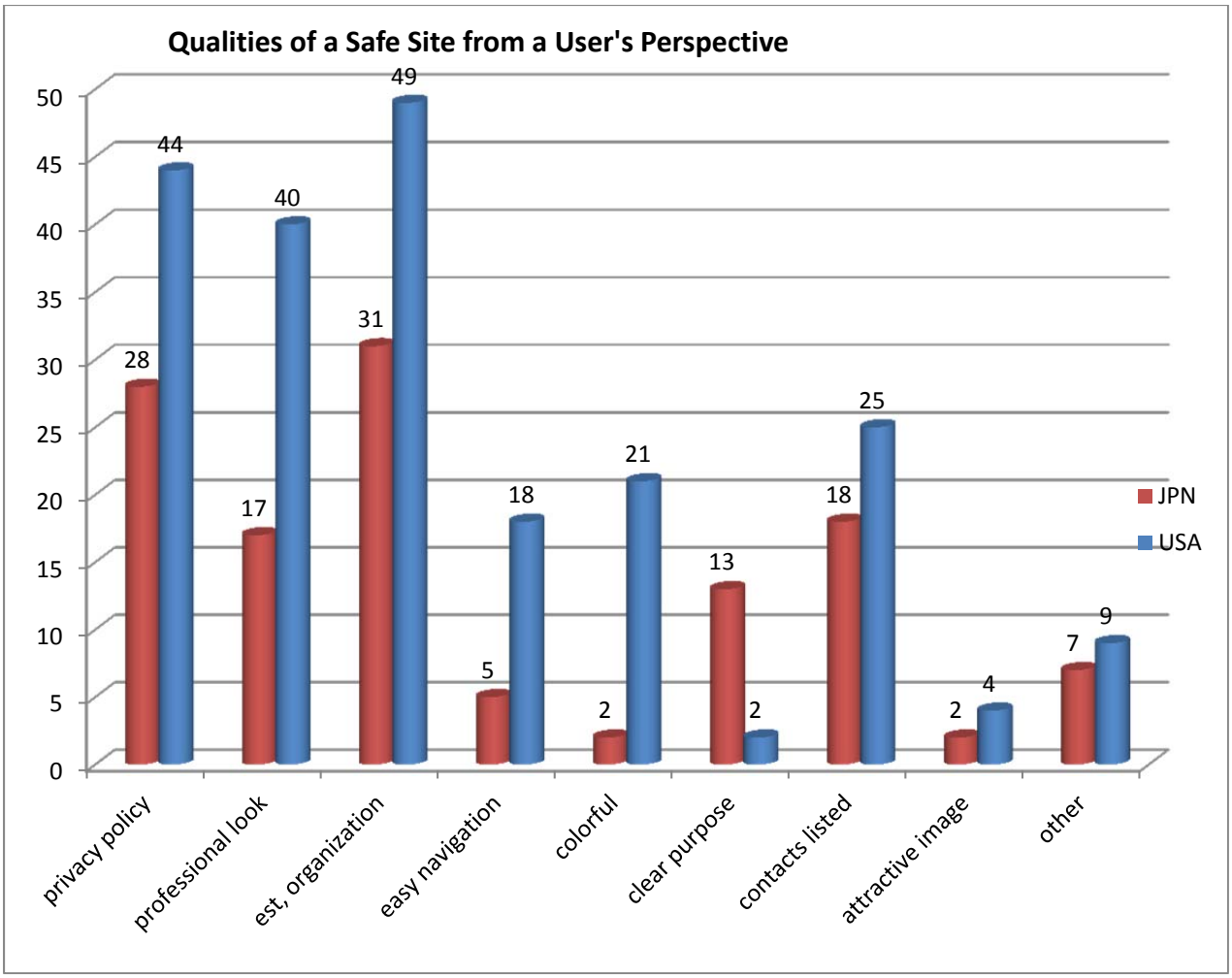


The aggregated results above help demonstrate that the most important factor in whether users trust a networked system in both the United States and in Japan is whether or not the person trusts the people using the system on the "other side." Universally, users ranked posting their names or addresses onto a private blog or private social-networking page approximately half-a-point higher on the scale of "feeling safe" than they ranked posting their names on publicly-viewable blogs or forums. Private blogs and private social networking pages frequently allow users to control which other users can view the information they post, and therefore there is additional control over who the user on the "other side" is that views the posters information. However, in a public blog or forum, these kind of controls are either unemployed or do not exist, and thus any on-line user can easily view the information that is posted. In addition, by far the highest-ranked activity in terms of feeling of safety was "making

purchases with your credit card information on-line at a well-known on-line store." On average, making purchases at a well-known store was ranked almost two full points higher in the United States, and almost 1.5 points higher in Japan, than making purchases at a store without a well-known reputation. These results are one hint that the most important factor to consumers making economic transactions on-line is whether or not they know and trust the person, business, or organization on the other end of the system. It also supports the idea that users and consumers do not trust the technology or the law to keep their information safe and keep those who would use their information maliciously accountable, and instead rely on trusting whether or not they know and/or trust the user on the other end of the system directly with their information.

An additional section of the survey also supports the conclusive theme that the most important factor for users in determining whether to interact with or trust a system is whether they trust or know who is viewing their information on the other side. In the second half of the survey, users were presented a checklist and asked to check all of the qualities listed that they believed were indicators of a site being trustworthy and safe.

The total number of checks for each item on the checklist from all users were aggregated and totaled, and these totals are presented in the following graphs for both the United States and Japanese surveys.



It is very clear from these numbers that the most commonly selected trait for whether a site is trustworthy or not according to users is whether or not the site is in affiliation with or created by a recognized organization. In the United States survey, one hundred percent of participants selected this criterion as an indicator that site is trust-worthy and/or safe. Beyond a clear connection with a well-known organization, other indicators that the organization on the other end is well-established and can be trusted were widely selected. The number two most selected qualities in both countries was the existence of a privacy policy on the site. A

privacy policy may serve as an indicator that the organization on the other end of the site has a promise and some form of internal sense of accountability in relation to how it will treat the information the users of its systems provide. Other commonly selected traits in both countries include whether the site has a professional look or not and whether contact information is listed for the creators or operators of the site or system. Users could possibly view a "professional look" as an indicator that the site is operated and maintained by "professionals" whose business reputation could depend on the proper handling of user information. Contact information listed could be one additional indicator to users that they themselves could contact and hold others affiliated with the site or system accountable for their information. The traits that participants in the survey selected as indicators that a site is safe act as another support to the conclusion that internet users rely on trusting the actual person or persons using the site or system on the opposite end rather than expecting technology or some outside force like the law to keep them safe.

On-Line Behavior

Following the questions where users were asked to rank how safe he or she felt performing certain activities on-line, each user was then requested to identify whether he or she had actually performed the activity. Respondents could either choose to answer "yes," "no," or "unsure." The activities each user was requested to identify are listed here below:

1) Posting your full-name on a social networking service or private blog
2) Posting your full-name on-line on a public blog or open forum

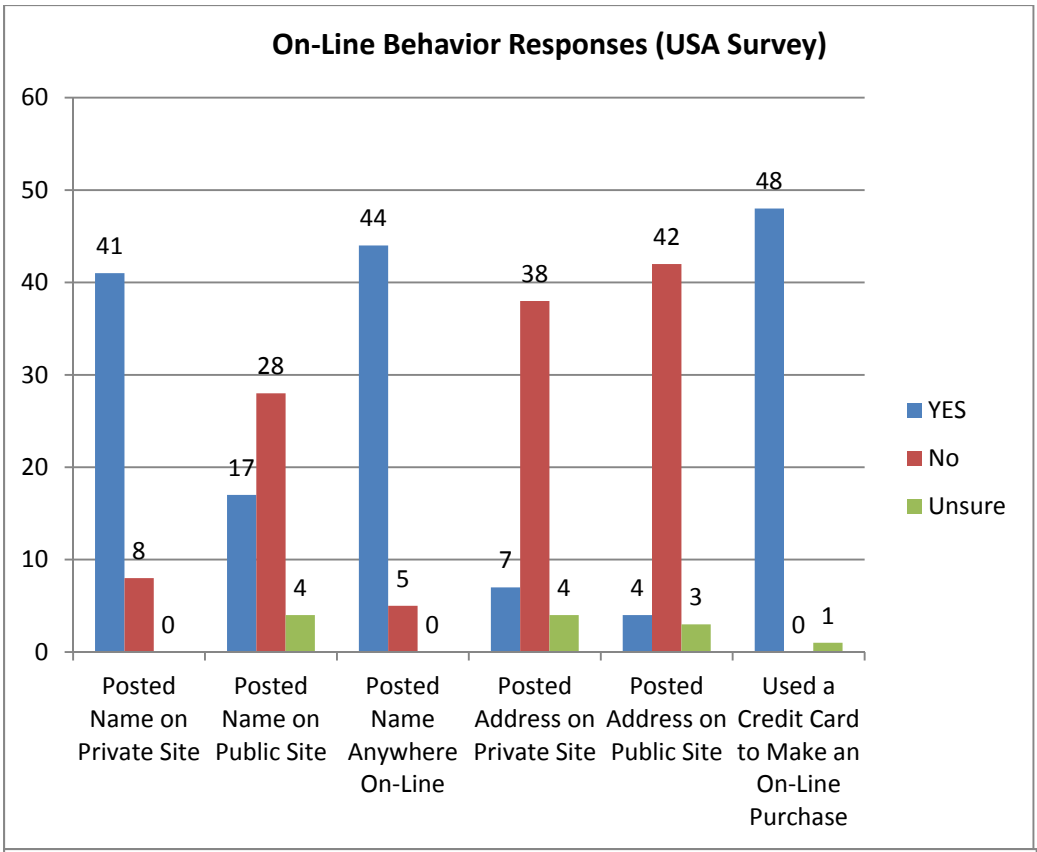
3) Posting your full-name on any on-line medium

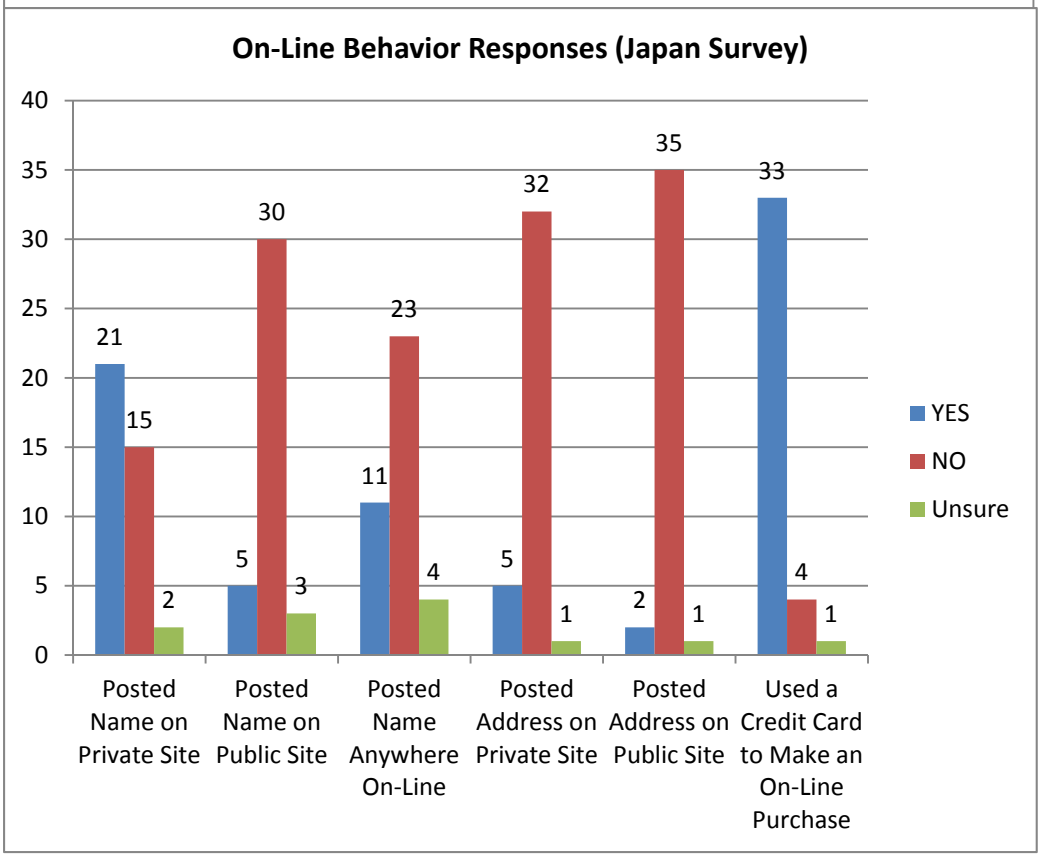
4) Posting your address on-line on a social networking service or private blog

5) Posting your address on a public blog or open forum

6) Making a purchase with a credit card on-line

The responses to each of these activities have been totaled and summarized in the charts posted here below:


On-Line Behavior Responses (USA Survey)
60
50
40
30
20
10
0
41
8
0
17
28
4
44
5
0
7
38
4
4
42
3
48
0
1
YES
No
Unsure
Posted Name on Private Site
Posted Name on Public Site
Posted Name Anywhere On-Line
Posted Address on Private Site
Posted Address on Public Site
Used a Credit Card to Make an On-Line Purchase


On-Line Behavior Responses (Japan Survey)
40
35
30
25
20
15
10
5
0
21
15
2
5
30
3
11
23
4
5
32
1
2
35
1
33
4
1
YES
NO
Unsure
Posted Name on Private Site
Posted Name on Public Site
Posted Name Anywhere On-Line
Posted Address on Private Site
Posted Address on Public Site
Used a Credit Card to Make an On-Line Purchase

One primary purpose of these behavioral questions and results is to confirm the accuracy of the "feelings of safety" questions proposed in the previous section of the survey. The results presented in the above charts confirm that how the users responded about how safe they felt performing certain activities on-line is accurately reflected in the users' actual activities on-line. More users claimed "yes" to performing activities that were ranked highly in the "feeling safe" section of the survey than to activities that were ranked low on the "feeling safe" scale. The highest rank activity in terms of "feeling safe," was using a credit card to make a purchase at a reputable on-line store. Coincidentally, using a credit card to make an on-line purchase was ranked the highest performed activity in both the United States and Japan. In both countries the most-performed activities followed in order in coincidence with how each activity was rated in terms of feeling in the previous section. User's posted name and address information more frequently once more on private blogs and sites where the receiving user is thought to be more familiar as opposed to posting on public systems where anyone could get an access to the data. This coincidence is a help to confirming the accuracy of the claims to be made with the "feeling of safety" data that states that users choose to rely on trust of users on the other end of a system as opposed to trusting technology, the law, on another outside force in order to feel safe.

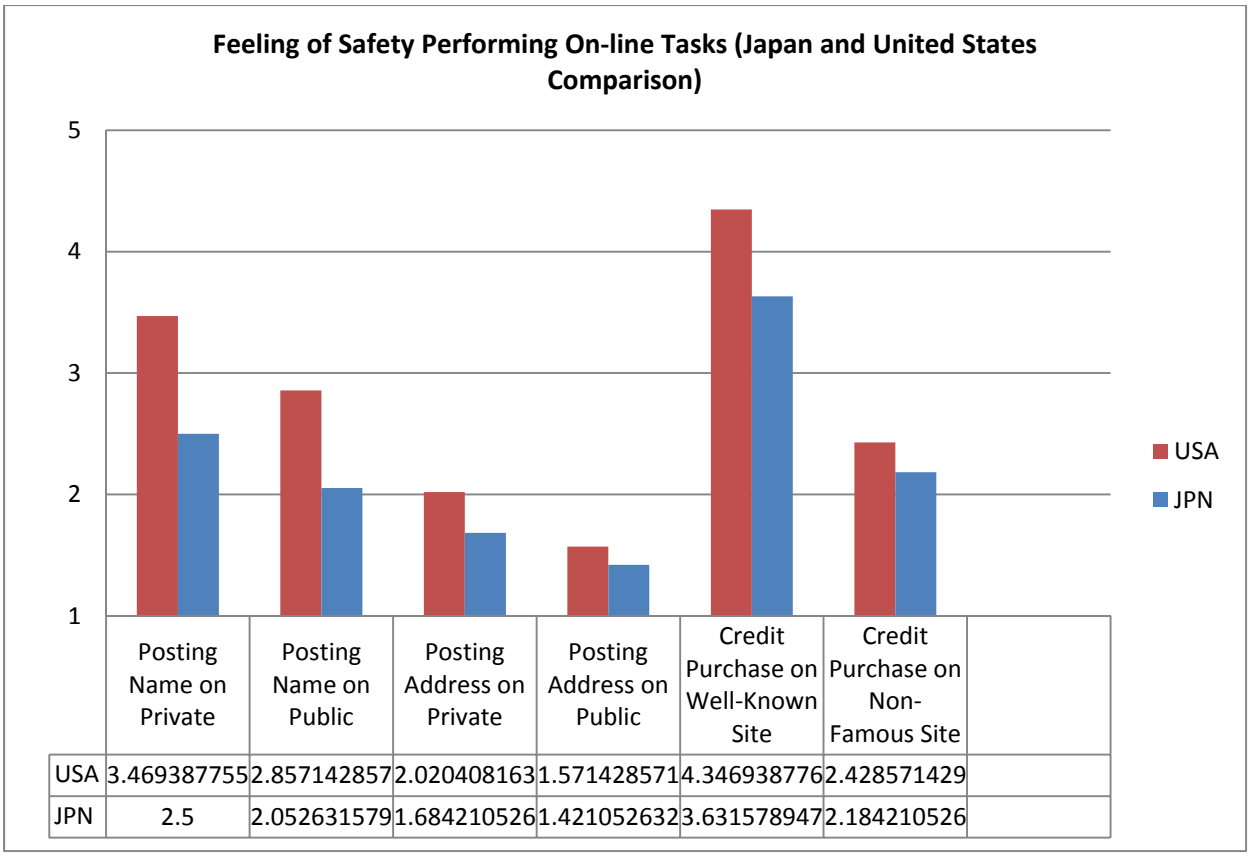
Summary

The results of the survey serve as an indicator that the most important factor of whether a user has trust in the security of his or her information, and whether or not that user will engage in interaction on-line, involves whether or not that user has knowledge of and trust

in the other user, business, or organization on the other side of the network or system. Since users seem to be more apprehensive about conducting on-line interaction with users or organizations they do not already have an established trust relationship with, they may not be trusting in technology or an outside force such as the law or law enforcement to keep handlers of their information on-line accountable.

A Gap in Use between the United States and Japan

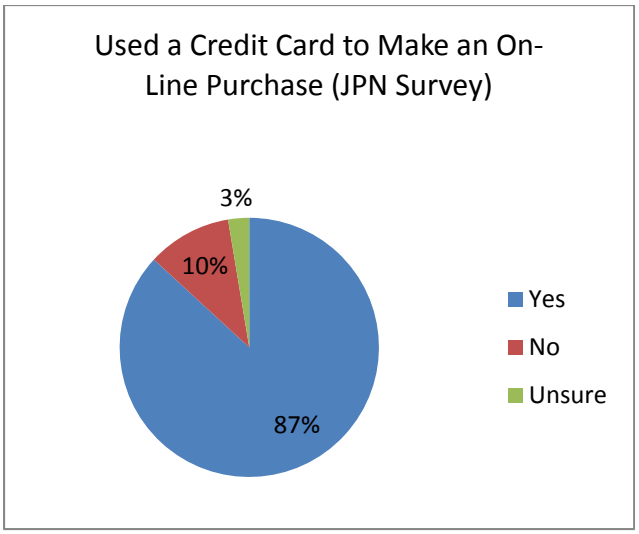
Viewing the results presented above in regards to feeling of safety on-line and internet usage patterns, one may see that, in general, the United States respondents felt safer performing the activities in question, and in addition, more users in general claimed to have performed the activities questioned than Japanese respondents. As the survey sampling population has been small and limited to mostly college students, this variation may not necessarily be caused by the difference between the United States and Japan, as much as on the difference between the types of students and the environment of the two universities, or on other variables. However, since the gap in the pattern of behavior and feeling of safety is very clearly defined in this survey, and since it may be impossible to determine the exact variables causing this gap without additional surveying, I would still like to bring forth this pattern in the data as a theme for analysis.

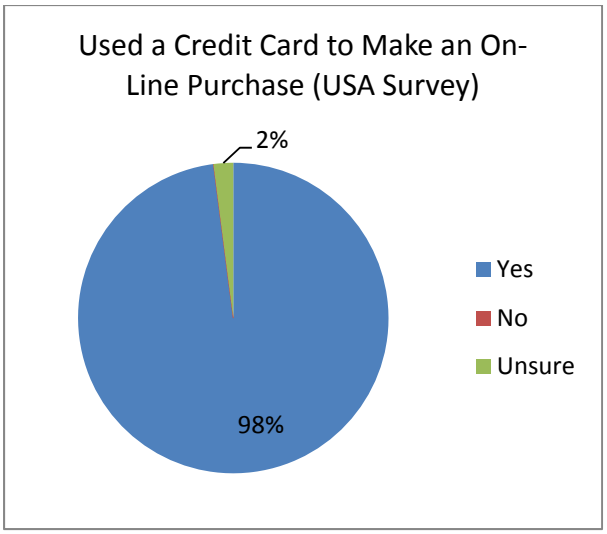


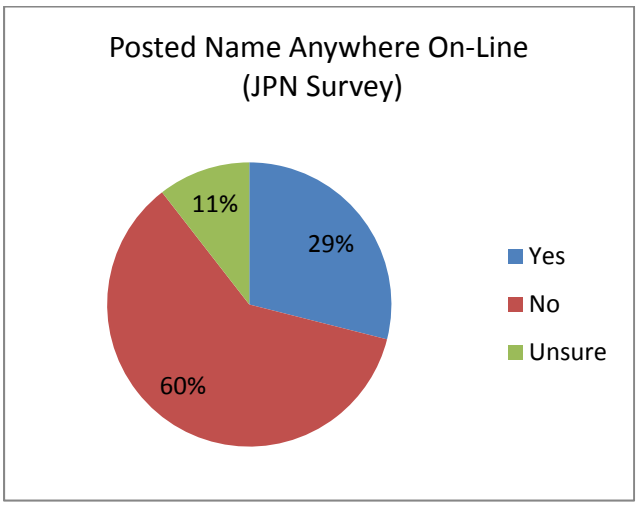
	Posting Name on Private	Posting Name on Public	Posting Address on Private	Posting Address on Public	Credit Purchase on Well-Known Site	Credit Purchase on Non-Famous Site	
USA	3.469387755	2.857142857	2.020408163	1.571428571	4.346938776	2.428571429	
JPN	2.5	2.052631579	1.684210526	1.421052632	3.631578947	2.184210526	

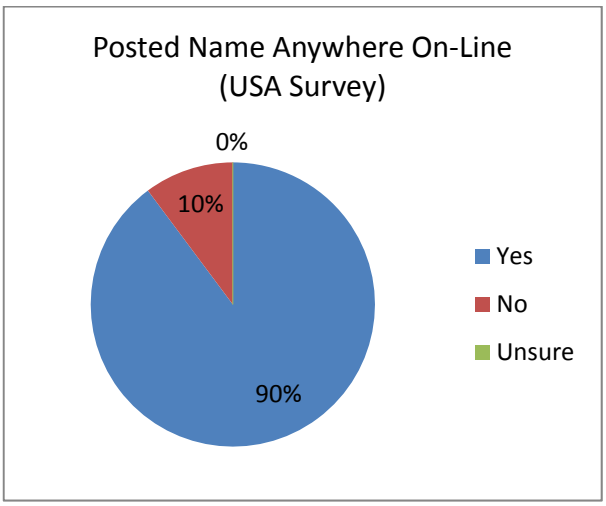
The above chart illustrates the comparison between how safe the American survey participants felt performing certain on-line tasks versus how safe the Japanese participants felt. It is clearly visible that the American participants claimed to feel more comfortable performing every activity in this survey.

Patterns in how participants actually claimed to behave on-line further demonstrated the gap in comfort level between the American and Japanese survey participants. The following several graphs illustrate the percentages of respondents who answered “yes” “no” or “unsure” to several activities in the United States and Japan.



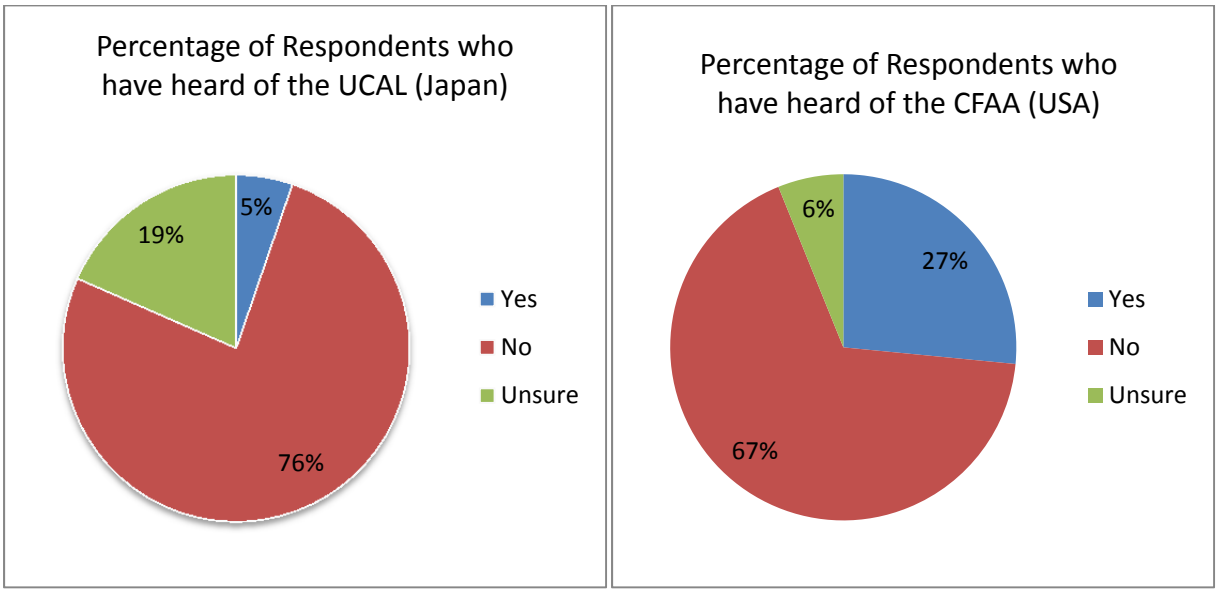






The above charts showed that the percentage of American participants who claimed to have used a credit card to make an on-line purchase before was slightly higher in comparison with the Japanese participants who claimed to do the same. However, there is a very large difference in the percentage of American respondents who are set to have posted their full name on-line in comparison with the number of Japanese respondents. While based on a relatively small sample size, these numbers may show a trend in greater trust in posting information on the web in the United States in comparison with Japan.

Finally, on simple comparison, the numbers show that slightly more American respondents admitted to at least hearing of the Computer Fraud and Abuse Act in comparison with the number of Japanese survey respondents who claimed to have heard of the Unauthorized Computer Access Law, even if neither group had an understanding of the components of the law.



While it may be difficult to tell from the small sample size, the numbers could point towards a trend where those in America, for whatever reason, are at least slightly more aware of what laws exist in regards to the internet and internet-related crime.

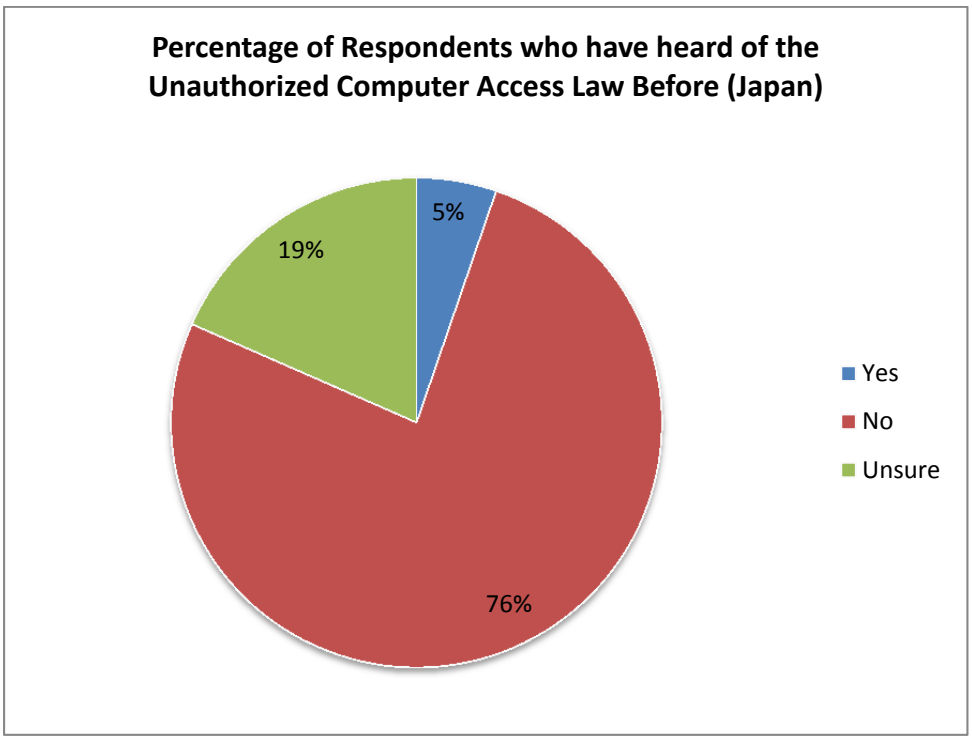
Lack of Knowledge of the Law

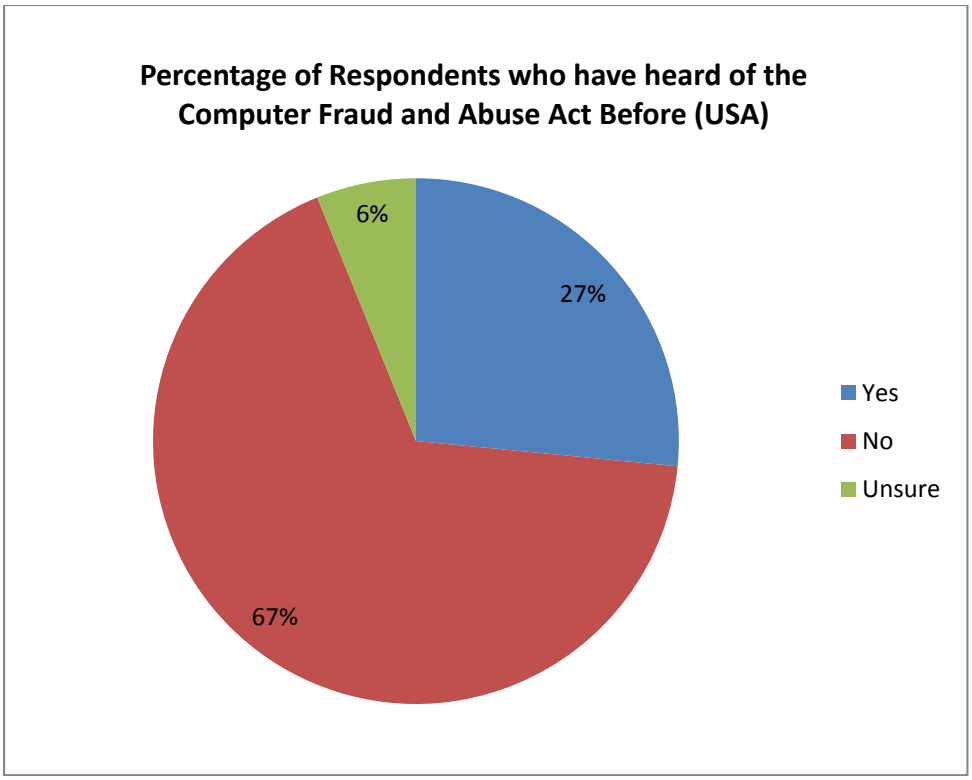
A recurring pattern that became clear through the survey is that most of those surveyed had never heard of the Computer Fraud and Abuse Act or of the Unauthorized Computer

Access Law. Most had some idea that certain activities were illegal on-line, but there was discrepancy amongst those surveyed in regards to what was thought to be illegal. It would be hard for the public to trust in the law or be deterred by the law when the public does not even know for sure that a law exists, or if they do, they do not know what the specifics of the law.

Simply Not Knowing

In one question of the survey, respondents were requested to identify simply whether or they had heard of either the Computer Fraud and Abuse Act (on the United States survey), or the Unauthorized Computer Access Law (the Japanese survey). The results of the question are summarized in the charts immediately below:





In both surveys the majority of respondents admitted to being unfamiliar with the law. In the United States survey, 73% of respondents admitted to having never heard of or being unsure if they had heard of the Computer Fraud and Abuse Act before the survey. In Japan, 95% of respondents admitted to having never heard of or to being unsure if they had heard of the Unauthorized Computer Access Law. This data seems to fall directly in line with the findings of the interviews, where even experts in the field of information security seemed to be significantly out of the loop on what was considered legal, and of what the law consisted.

Perceptions of Legality

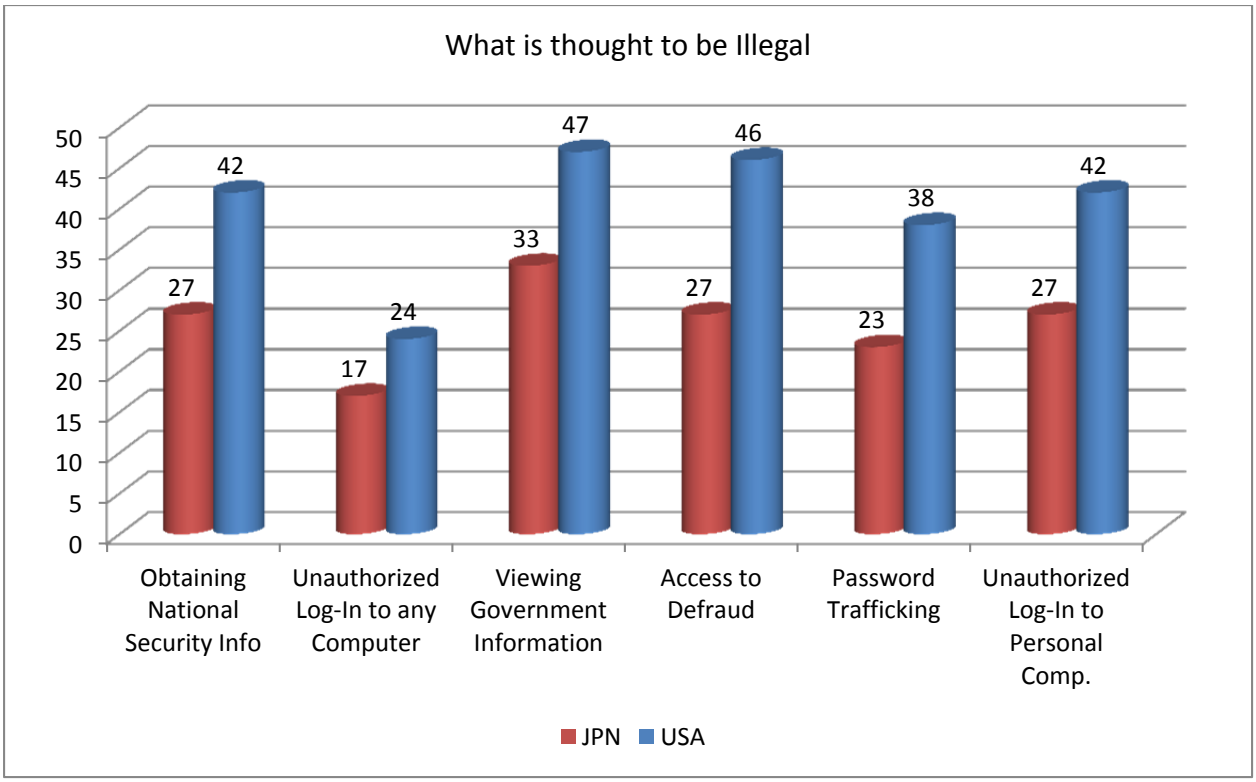
Beyond just being questioned about their awareness of their existence of the law, participants were questioned their perceptions of what the law might contain. This questioning

could help qualify the relevance of the prior question which gauged whether users were aware of the law. Perhaps if users innately knew what the law consisted of, then perhaps they would be able to make informed network-usage decisions without specific awareness of the law. However, the responses that returned were varied among the participants, and the responses were also not always "correct."

User awareness was gauged in two ways. First, a check-list of activities both legal, illegal, and also questionably either, was presented to each participant, and participants were asked to check any and all items on the list that they thought to be considered illegal under the Computer Fraud and Abuse Act in the United States, and the Unauthorized Computer Access Law in Japan. The items on the checklist were as follows:

- ☐ Obtaining National Security Information from a Government Computer
- ☐ Logging into any computer to which you do not have access
- ☐ Viewing information stored in a Government Computer to which you do not have access
- ☐ Accessing a Computer to Defraud and Obtain Value
- ☐ Transferring/communicating passwords of protected computers to unauthorized persons
- ☐ Logging into someone's personal computer without permission.
- ☐ Unauthorized access to and intentional damage of electronic data.

The following graphs illustrate the summation of responses provided by both American and Japanese Survey participants according to the above check-list.



Trends in what was believed to be illegal were very similar in both countries. A number or participants actually anticipated the law to be more restricting or protective that it actually is, as almost half of the respondents in both surveys responded that they believed unauthorized access to any computer was illegal. The activity of password trafficking was seemingly underestimated as a criminal activity, as both countries have provisions to make many forms of aggregation and transferring password data illegal, but only 38 out of 49 respondents in the United States, and only 23 of 38 respondents in Japan marked that they believed such activity was illegal on their surveys.

Second, participants were presented a free-space with which they were asked to write very briefly what they believed either the CFAA or UCAL consists of. User responses to both

questions were inconsistent and varied, further demonstrating a lack of knowledge of the law, which would be detrimental to the goals of deterring the unauthorized theft and destruction of electronic data as well as promoting the trust of users in systems for the establishment of a sound information economy.

The descriptions that participants listed as what they believed to be the content of the two different laws further demonstrates the potential obliviousness of the internet-using public to what is considered a crime and how they may be protected under the law. A full table of quotes listed by participants is available in the appendix. However, I summarize the important patterns and bring forth particular points of interest that came through participant's responses here.

First, in both surveys, many people chose not to answer this final question, and the majority of participants that did choose to answer, answered in vague terms that demonstrated the extent of their knowledge of the law was as deep as guessing what the law might be about based on hearing the name in the question stem. For example, in the Japanese survey, some claimed that the law "outlaws unauthorized access into a site that requires a password," or "outlaws the unauthorized entry of a password and unauthorized access to personal information." The American side also had similar vague responses such as, "hacking and breaking and entering computer systems," as well as "tries to protect computers from fraud and data theft." Others also just claimed flat-out ignorance of the law. A Japanese participant wrote "I'm sorry, I don't know," and another American participant wrote "I have no clue."

Some users also put in simply wrong interpretations of what the law consists of. One participant wrote on the Japanese survey "no one can access a computer they don't own or have permission to use." This interpretation is actually far stricter than the actual law's extent. Another Japanese participant responded that the law would protect individual accounts such as e-mail and Facebook, as well as outlaw child pornography on the web. An American participant suggested the law involves "protecting the right to privacy." Another American participant suggested the law involves "illegal downloads." Twisted or misinformed interpretations of what is legal and what is protected under the law may be very detrimental to the purposes of the CFAA and the UCAL.

Summary

The user surveys conducted in both the United States and in Japan produced very similar results in both countries. The results can be grouped into two major themes. First, the CFAA, the UCAL, or any other law, technology, or outside force does not seem to be promoting additional user trust in the internet, information systems, or the information economy. Instead, users seem to rely on trusting the user directly on the other end of the system when making transactions on a network. Participants stated sense of security when performing certain tasks on-line, as well as the records of what they claim to have actually done on-line help support this claim. Second, there is a lack of knowledge amongst the participants in regards to the existence of the law, and what is actually considered legal and illegal. For one, the vast majority of

respondents to the survey claimed that they had no prior knowledge, or had not even heard of the CFAA or the UCAL before participating in the survey. In addition, participants' interpretations of what they believed to be considered legal and illegal were varied and often incorrect. The lack of knowledge and misunderstanding of the law could be great impediments to the CFAA or the UCAL serving as either deterrents or promoters of trust in on-line economic transaction.

Document Analysis

The results from the Document Analysis segment of data collection can be related to three of the four primary research questions:

1) How effective is the Computer Fraud and Abuse Act, including its revisions in the 2001 Patriot Act, in protecting American electronically-stored data from unwanted access, reproduction, or destruction?
    a. In what ways is it effective?
    b. In what ways is it ineffective?
    c. How does it interact with other American laws in achieving its aims?
2) How effective is the Japanese "Unauthorized Computer Access Law" in protecting its electronic data from unwanted access, reproduction, or destruction?
    a. In what ways is it effective?
    b. In what ways is it ineffective?
    c. How does it interact with other Japanese laws in achieving its aims?
3) Do these two policies build users' trust in the security of information, thus promoting a sound information economy?

The results of the document analysis procedures tended primarily as a way of re-iterating what was identified in the survey section of the data collection and analysis. The data analysis provides a perspective of how government bureaucracies, both American and Japanese,

present information regarding computer crime and the law to the public. What was identified as being presented to the public through content analysis related surprisingly well to what the public identified as their feeling of security when using the internet as well as their awareness of computer and cyber-crime related law.

The "Fear" Effect – Japan vs. the USA

A major theme tested through the document analysis was how reporting agencies like the Computer Crimes complaint Center in the United States and the Information Technology Promotion Agency in Japan represented computer crime to the public, and whether or not they were increasing or decreasing fear of computer crime. This measurement of a feeling of fear was then compared with how many times law or policy or one of the two acts studied in the report were mentioned, and then again with how many times those laws were mentioned in relation to a resolution of the problem. This first section will explain the measurement of "fear" detected in these promotion agencies reports to the public.

Based on a preliminary reading of the documents in the data collection the following list of words were compiled due to their connotation of fear or uneasiness in relation to computer and network security. QSR N6 software was then used to perform word counts of all of these words across all documents to identify the number of lines of text that "fear words" appeared in. It is assumed that a greater the number of "fear words" appearing in the documents would indicate a greater degree to which "one should fear computer crime" is implied by the C3 or the IPA in their reporting to the public.

Fig. List of "Fear Words" Counted (36 Words)

Damage	Attack	Illegal
Unknown	Vulnerability	Unauthorized access
Defect	Remote	Incident
Fraudulent	Weakness	Victim
Spam	Exploit	Victims
Hoax	Hole	Identity theft
Virus	Infect	Theft
Scam	Exploits	Complaint
Malware	Critical	Threat
Compromised	Unresolved	Extortion
Unauthorized	Criminal	Warning

The final word count came out as follows. A "text unit" refers to one line of text within a given document. The following table presents the total number of text units, the number of text units in which a "fear word" was found, and the percentage of text units in which a "fear word" was found for both United States C3 documents, Japanese IPA documents, as well as combined totals.

	USA	JPN	ALL
Total Text Units	1028	1578	2606
Text Units containg "Fear Words"	108	278	386
Percent containing "Fear Words"	10.5%	17.6%	14.8%

A significant portion of both documents were counted as containing "fear words" in both sets of documents from both countries. In the United States, approximately 10.5% of text units contained one or more "fear words," and in Japan, the number of fear-word containing units exceeded 17.5%. While "fear words" appeared in a significant portion of both sets of

documents, it is interesting to note that fear words made a significantly higher appearance in the Japanese documentation. These data sets are small, and for exploratory purposes only, so these trends cannot be generalized too far. However, the presence of such a pattern may indicate an interesting starting point for future study.

In addition, the rate of occurrence of the "fear words" over time was considered. The results are illustrated in the following tables:

USA	2003	**2005**	**2007**	**2009**	**Total**
Total Text Units	269	121	405	233	1028
Text Units containing "Fear Words"	22	14	49	23	108
Percent containing "Fear Words"	8.2%	11.6%	12.1%	9.9%	10.5%

JPN	2005	**2007**	**2009**	**Total**
Total Text Units	270	530	778	1578
Text Units containing "Fear Words"	28	69	181	278
Percent containing "Fear Words"	10.4%	13%	23.3%	17.6%

Once again, the sample size may be too small to draw any truly concrete conclusion, but as an exploratory measure, from the sample taken, one sees that in the United States, over the sampled period there was no significant change in the rate that "fear words" appeared in the text. In the Japanese documents, however, one sees an increasing trend in the appearance of "fear words." In particular, the 2009 documents saw an appearance rate of over 23%. This could indicate that in more recent years the Japanese IPA has written its reports to the public in a more alarming, or fear-inducing tone than previously.

Lack of Presence of the Law

The second step in the document analysis process was to gauge the presence of reference to law within the documents, and then compare those references to the law with references to the words "prevention," "resolution," "solve," and "solution." The results from this analysis can be summarized very quickly. There simply was a dearth of reference to the law, or the legality of the malicious activity being reported by the American C3 or the Japanese IPA. In the Japanese documents, not only did no specific mention of the UCAL appear, the word "law" or derivatives of it did not appear once throughout any of the text. In the American collection of documents, no specific mention of the CFAA was made, but the word "law" did appear in six text units across three different documents. Every time the word law appeared though, it referred to the word "law enforcement," specifically in regards to reporting activity to law enforcement. Below are the six lines of text in which the word "law" appeared in the American documents:

[JUN13_2007 : 35 - 35]

"activity to law enforcement."

[JUN30_2003 : 29 - 29]

"type of fraud is reported to law enforcement, the average individual is "

[JUN30_2003 : 138 - 138]

"law enforcement, the perpetrator has replaced the spoof site with a"

[NOV29_2007 : 21 - 21]

"warrants were served in the U.S. and by overseas law enforcement partners "

[NOV29_2007 : 65 - 65]

"law enforcement agencies that led to the success of Bot Roast II. Through"

[NOV29_2007 : 154 - 154]

"of Law Enforcement, and the Panama City Beach Police Department"

In addition, the references to the law that did appear were then compared with the words "resolution," "solve," "prevention," and conjugations of those words, to determine if the law was being conveyed to the public as a means of prevention and resolution, and thus promoting trust in law. An analysis was run using the N6 software to determine if the any of the words "resolution," "solve," "prevention," or conjugations thereof appeared within five text units of the word "law." In the end, only one document came back positive for this combination. However, the resulted combination was a "false positive." The words "prevent" and "law" were within five text units of each other, but were used in different contexts. The passage where this occurs is listed here.

> *"The FBI also wants to thank our industry partners, such as the Microsoft Corporation and the Botnet Task Force, in referring criminal botnet activity to law enforcement.*
>
> *Cyber security tips include updating anti-virus software, installing a firewall, using strong passwords, practicing good email and web security practices. Although this will not necessarily identify or remove a botnet currently on the system, this can help to prevent future botnet attacks."*
> *– June 2007*

Thus, in this sample set, there are no references to law in overt relation to words associated with prevention and solution to the reported computer crimes.

Summary

The document analysis of the American Computer Crimes Complaint Center reports and the Japanese Information Technology Promotion Agency reports turned up two major findings. First, these reports had a fairly large occurrence of words that contained connotations of fear, which may actually reduce trust in internet and networked systems. Japan showed a higher occurrence of "fear words" than did the American results. In addition, despite the high rate of "fear" related words, references to the law or anti-crime policy was complete non-existent in Japanese reports, and limited to references to Law enforcement in American reports. Thus, it would appear through this document analysis that major computer crimes complaint, alert, and research centers in the United States and Japan are doing very little to promote trust in an outside force like the law to influence the safety of networked systems, or people's behavior on those systems.

Recommendations and Conclusion

Overview

This final chapter presents policy recommendations that may improve both the American Computer Fraud and Abuse Act and the Japanese Unauthorized Computer Access Law in achieving both policies' aims of reducing theft and destruction of electronically stored data as well as promoting trust in network technologies for the advancement of a healthy information economy. The recommendations presented in this chapter are supported by themes presented in the previous chapter, "Data and Findings." The recommendations presented here are not recommendations for direct, specific changes to the CFAA or the UCAL, but instead are broad alternative policy recommendations for additional policy that could address the issues discovered in the themes of the "Data and Findings" chapter. As was discovered in the "Data and Findings" section, the usage and effectiveness of the CFAA and the UCAL are greatly affected by outside policy, so even if the policy recommendations are not for direct edits to the CFAA and the UCAL, they are still relevant to the workings of the CFAA and the UCAL. This chapter is organized by policy recommendation. This chapter directly addresses the final research question:

4) Based on the comparison of the policies of the two nations, what recommendations can be made to policy makers to improve the current legislation?

The Recommendations

1. Coordinate state internet law in the United States.

A common theme raised in the interviews is the importance of unifying and streamlining law enforcement response to computer crimes in order to effectively be able to collect the necessary information to prosecute under the CFAA. Mr. Moot, and Ms. Anderson both re-iterated this point in their interview responses, but Professor Filp particularly commented on the necessity of communication, coordination, and streamline of process across borders. While people may have established physical, social-political boundaries, the internet and cyber-crime knows no boundaries, so if legal response to cyber crime is to be effective, the response must not be hampered by such boundaries.

As initially stated in the literature review section, simply by nature of existing as a federal governmental system, the United States has internal boundary problems that limit the scope of the CFAA and make tracking computer crime cases that might otherwise be tried under the CFAA difficult to follow because each state employs its own computer-crimes laws and tracks its cases differently. Professor Filp supported the point that the various state laws complicate the recording and measuring of internet crime cases when he added that "states don't track this information very well." Thus, the complication of the existence of a variety of state laws, state law enforcement, and state court record-keeping methods create boundaries on a boundary-less world of computer crime, and thus hamper the ability to prosecute under, or simply even study, the CFAA.

Thus, this is one area where the United States could take away a lesson from Japan's policies. By nature of Japan existing as a unitary political system, it avoids the complication of various state and local laws. However, beyond this, as mentioned in the literature review section, Japan makes official data gathering and reporting policies to not only uniformly study and understand computer crime trends across the entire country, but also to direct and unify law enforcement response practices across the entire country. For example, written directly into the UCAL are directives for yearly studying and reporting of trends in crime related to the UCAL and additional directives for how law enforcement should respond to cases of unauthorized access. This could make for faster response and more effective data collection for prosecution.

While it is unfeasible to imagine the United States moving to a more unitary system, it may be reasonable for the United States central government to pass legislation to coordinate the laws and reporting practices of the various states related to computer crime. While the central government is not supposed to direct commerce policy of individual states, the government should realize that the internet does not know the political boundaries of the states, and that having too much variety in individual states' policies could in fact diminish the effectiveness of not only the CFAA, but all attempts at legal action against computer criminals. Thus, in order to improve the ability to prosecute accurately with the CFAA, it is recommended that the United States take more action to coordinate the policies of its individual states in regards to computer crime.

2. Continue to push for international cooperation in establishing computer-crimes response teams.

As prior mentioned, the internet knows no physical, social, or political boundaries, and neither does computer crime. Investigation is a major hindrance to accurate prosecution under the CFAA or the UCAL, particularly in international cases. Professor Filp mentioned from his experience that the most difficult problem in dealing with an international computer crimes case is coordinating different national-level response teams. Both the United States and Japanese governments currently participate in several international organizations that aim at promoting international legal and response harmonization to computer crime. It is critical for both governments to continue working for promoting this international cooperation in order for computer crimes to be able to be prosecuted under the CFAA, the UCAL, or any law or statute that tries to hold the performers of malicious on-line activity accountable for their actions.

3. Place national security importance on information security and network research.

A theme that arose in both the literature review and interviews involved the sloth of the law and policy in comparison with the speed of technological change. Several of the experts interviewed re-iterated that law is not going to be enough to deter or protect anyone from computer crime. Law cannot be the driver of the solution because it is usually reactive and rarely, if ever, proactive. Thus, an additional recommendation to the Japanese and American governments would be to place great importance on information security research and development, and to promote and environment where information and network technological advancement is supported and promoted. A stronger helping hand in the promotion of such

research would be a positive step towards greater information security for everyone, and hopefully someday lead to technological alleviations to the policy problems today that the CFAA and UCAL do not and cannot address alone.

4. Increase education about information security and related law.

The CFAA and UCAL are acceptable on the books as prosecuting tools, but aren't being used to the extent they could be. Neither will serve as a deterrent to crime if their existence is unknown, and they can't be used effectively as prosecuting tools if the means of collecting evidence is obstructed by a poor response team structure (such as in an international case), or if a victim does even know that he or she should or could pursue repercussive action in the first place. You can see this possibility by comparing the number of complaints groups like the Japanese IPA and the American C3 receive in a year with the number of cases that actual go to court, and collaborate that data with the dearth of knowledge of the law made clear by interviews and surveys. There seems to be a lack of common knowledge or consensus as to what is "illegal." People might not respond, and they might not know how to protect themselves if they do not understand what was done to them, and that what was done might be illegal.

Thus, it is recommended to increase education in both the United States and Japan regarding computing safety, computer crimes, and the law. Simply educating citizens that laws like the CFAA and the UCAL exist could go miles for increasing both policies' power in serving as a deterrent for computer crime. It could be wise to teach computing security and personal

computer network safety practices in school computer lab courses. It may also be possible to increase ad campaigns, much like a previous "identity theft" campaign existed in the United States or the "Furi-komi sagi" (ATM Wire-Transfer Fraud) campaigns in Japan aimed at educating citizens about certain technology related crimes, how to protect themselves, and how to respond. It could also be wise to increase the prevalence of federally funded research and response organizations like CERT who work with troubled organizations to mitigate their security risks. In addition, according to the data collected in this study, Japan seems to need to take greater steps in just about all of these areas than the United States. No law can serve as a deterrent to computer crime if people are not given the opportunity to know the law and its penalties.

Suggested Areas of Future Work

A short-coming of this particular research is that as an exploratory honors thesis, much of the research lacks detail, statistical analysis, and scientific detail to ensure the credibility of all findings. However, from this exploratory approach, areas for future research and improvement can be suggested to verify and expand upon the findings presented in this thesis. These suggestions are mainly to expand the methods begun in this exploratory analysis to a greater scope, a greater depth, and to a greater degree of scientific accuracy. First, I recommend in the literature review, pursuing a more concrete line-by-line document analysis of the two laws themselves. As far as the interviews and surveys go, it is of course important to obtain a larger, more diversified sample size. It would be wise to interview more lawyers,

specifically lawyers who have worked on direct cases with the CFAA and the UCAL, and also more Japanese professionals. It would be wise to also capture a wider age range in the demographics of the survey. Finally, more statistical analysis on the larger samples to determine to a greater degree the scientific accuracy of the samples would be beneficial.

Concluding Remarks

From researching the Computer Fraud and Abuse Act and the Unauthorized Computer Access Law in both the United States and Japan, it appears that both countries face very similar challenges in relation to computer crime and related law and policy. Having both laws on the books in both the United States and Japan is important to allow certain kinds of malicious computer crime activity to be prosecuted. However, neither law is very useful by itself for the stated purposes reducing the amount of data maliciously stolen or destroyed, or for promoting trust in information networks and thus promoting the growth of a sound information economy due to a lack in policies and practices that would be related to the laws here in question. In order for the CFAA or the UCAL to be effective in achieving either of the two stated goals more attention needs to be paid both in the United States and in Japan to prevention and investigation of computer crime. Research and development in new information security technologies and education of the public would be steps in the right direction. In addition, working to streamline investigation processes across borders will allow for a more proper and accurate collection of evidence. This would be necessary in order to more accurately hold

actual computer criminals accountable for their actions. A public that has never heard of computer crimes law will not likely be deterred by its stated punishments or have faith in the laws ability to provide protection. If there are political, organizational, or technological hindrances to investigation of cyber crime, which by nature is already extremely difficult to investigate, the CFAA and UCAL will be useless as prosecuting tools. The CFAA and UCAL are important pieces of the puzzle in the war against computer crimes, but they need more support from some surrounding pieces of the policy puzzle in order to be more effective in achieving their stated goals.

Appendix

Appendix A

Professor and Lawyer Interview Guideline

Japanese and American Computer Crime Policy: Comparative Study

Overview

The following is an example of a set of questions that served as a guide for interviewing respondents. It is important to note that each interview used the same interview guideline initially, but as the conversation developed naturally and occasionally drifted from the exact guideline, not all of the same questions were asked to all of the respondents. Exact data records are kept by the principal investigator.

The Guide

Carnegie Mellon University, Information Systems
Principle Investigator: Ryan Handerhan
Name:
Age:
Sex: M/F
Position Held:
Affiliated Organization (If Applicable):
How long have you been affiliated with _____ ?
Other Positions held in the field:
Educational Background:
How would you define "Cyber-Law"?
Do you believe that Cyber-Law should be treated or considered differently than traditional law?

What kinds of computer-crime cases are you familiar with/have you dealt with?

(Lawyers) What is your role in the process?

Are you familiar with the Computer Fraud and Abuse Act (CFAA)?

(How are you familiar with it? What do you know about it?)

Are you familiar with any cases involving the CFAA?

What do you believe to be the purpose of the CFAA within the United States Government's approach to cyber-law?

(How does it interact with other laws?)

(How is it used in court?)

(Why did the government enact this legislation?)

In what aspects do you believe the Computer Fraud and Abuse Act is successful? In what aspects do you believe it to be unsuccessful?

(Do you believe the CFAA is successful in deterring computer-related crime?)

(Do you believe the CFAA is successful in empowering law enforcement and prosecutors in appropriately finding and prosecuting computer criminals?)

(Do you believe that the various sentences/punishments involved with the CFAA are appropriate?)

Do you find that the CFAA frequently interacts with other legislation when prosecuting possible criminals? If so, which laws are frequently used in tandem with the CFAA in prosecution?

Do you believe the CFAA is effective in dealing with internet crime as a global phenomenon?

(How do you see the CFAA fitting in the push for international legal harmonization relating with information security policy?)

(Have you ever dealt with an international case involving the CFAA?)

(What was the most challenging part of dealing with an international case?)

What is the timeline of a typical computer-crimes trial?

(How long are you involved in a typical trial?)

(How does a computer-crimes trial compare with any other "regular" criminal trial?)

(Does trial time vary greatly per case, or is it generally standard?)

When reading the language of the CFAA, is there anything unusual about this act in comparison with other criminal code?

In the language of the CFAA, does any passage appear to be a possible issue for prosecution, defense, or law enforcement?

Appendix B

日本と米国の情報セキュリティに関する法律の比較

日本アンケート

これは、カーネギーメロン大学の情報システム学部のライアンハンダーハンの四年生研究に関するアンケートです。参加することは随意です。

問い合わせ：rhanderh@andrew.cmu.edu.

本日はご参加いただき、ありがとうございます。

氏名：

男性
女性
その他

年齢：

国籍：　米　日　その他　_____

名前と苗字をＳＮＳやプライベートなブログに書き込むことは安全だと思いますか？

（全然安全ではない　１　２　３　４　５　とても安全）

名前と苗字をＳＮＳやプライベートなブログに書き込んだことがありますか？

はい　　いいえ　　分からない

名前と苗字をネット上のブログやオンライン掲示板に書き込むことは安全だと思いますか？

（全然安全ではない　１　２　３　４　５　とても安全）

名前と苗字をネット上のブログやオンライン掲示板に書き込んだことがありますか？

はい　　いいえ　　分からない

ネット上で名前と苗字を書き込んだことがありますか？

はい　　いいえ　　分からない

住所をＳＮＳやプライベートなブログに書き込むことは安全だと思いますか？

（全然安全ではない　１　２　３　４　５　とても安全）

住所をＳＮＳやプライベートなブログに書き込んだことがありますか？

はい　　いいえ　　分からない

住所をネット上のブログやオンライン掲示板に書き込むことは安全だと思いますか？

（全然安全ではない　１　２　３　４　５　とても安全）

住所をネット上のブログやオンライン掲示板に書き込んだことがありますか？

はい　　いいえ　　分からない

有名なオンラインストアでクレジットカードを使って物を買うことは安全だと思いますか？

（全然安全ではない　１　２　３　４　５　とても安全）

有名なオンラインストアでクレジットカードを使って物を買ったことがありますか？

はい　　いいえ　　分からない

よく知らないサイトでクレジットカードを使って物を買うことは安全だと思いますか？

（全然安全ではない　１　２　３　４　５　とても安全）

よく知らないサイトでクレジットカードを使って物を買ったことがありますか？

はい　　いいえ　　分からない

ネットでクレジットカード使って物を買ったことがありますか？

はい　　いいえ　　分からない

使ったことがなければ、なぜネットでクレジットカードを使って物を買ったことがありませんか？
あてはまる項目すべてにチェックしてください。

「」クレジットカードや売掛勘定がないから
「」ネットで者を買う意思はないから
「」ネットでお買い物するのが不安全だと思うから
「」その他_____

他のサイトと比較するとより安全だと思うサイトはありますか？

はい　　いいえ　　分からない

どのような特徴がサイトが安全である条件だ思いますか？
あてはまる項目すべてにチェックしてください。

「」プライバシーポリシーがあること
「」サイトのデザインがきれいでプロフェッショナルであること
「」サイトが有名な会社や団体と関係があること
「」サイトのナビが使いやすいこと
「」サイトの目的がはっきりしていること
「」サイトの作者の連絡先の情報が書いてあること
「」サイトのデザインがカラフルであること
「」サイトが魅力的であること
「」その他　_____

どのような特徴がサイトが安全でない条件だと思いますか？
あてはまる項目すべてにチェックしてください。

「」プライバシーポリシーがないこと
「」サイトの内容には文法や漢字の間違いがあること
「」サイトのナビが使いにくいこと
「」サイトの作者の連絡先の情報が書いていないこと
「」サイトの目的が不明であること
「」サイトのデザインがカラフルであること
「」その他　_____

以下の行為の中で、どれが法律違反だと思いますか？
あてはまる項目すべてにチェックしてください。

「」政治と関係があるコンピューターから国防に関する情報を盗むこと
「」アクセス権のないコンピューターにログインすること
「」アクセス権のない政府のコンピューターの情報を見ること
「」詐欺や営利目的でコンピューターにアクセスすること
「」制限されているコンピューターのパスワードを集めて販売すること
「」不正アクセスしてわざとデータを破壊すること

今までに、「不正アクセス行為などの禁止に関する法律」について聞いたことがありますか？

はい　いいえ　わからない

できるだけ、「不正アクセス行為などの禁止に関する法律」はどのような行為を禁止すると思うかをお書きください。

Japan Survey

This is a survey for the Senior Thesis Research of Ryan Handerhan, a fourth-year student of the Information Systems Department of Carnegie Mellon University. Participation in the survey is completely voluntary and all questions are **OPTIONAL**.

Please address questions you may have to the survey proctor or to *rhanderh@andrew.cmu.edu*.

Thank you for choosing to participate!

Demographic Information

Age:

Sex:

☐ Male ☐ Female ☐ Other

Nationality/Country of Citizenship:

Primary Survey

How safe do you feel posting your full-name on a social networking service or private blog?
Please circle a number from 1 to 5 on the following scale.

NOT Safe at All *1* *2* *3* *4* *5* *Very Comfortable/Safe*

Have you ever posted your full-name on-line on a social networking service or private blog?
Please circle one option.

Yes *No* *Unsure*

How safe do you feel posting your full-name on-line on a public blog or open forum?
Please circle a number from 1 to 5 on the following scale.

NOT Safe at All *1* *2* *3* *4* *5* *Very Comfortable/Safe*

Have you ever posted your full-name on-line on a public blog or open forum?
Please circle one option.

Yes *No* *Unsure*

Have you ever posted your full-name on any on-line medium? (Any form of website, blog, etc.)
Please circle one option.

Yes *No* *Unsure*

How safe do you feel posting your address on-line on a social networking service or private blog?
Please circle a number from 1 to 5 on the following scale.

NOT Safe at All *1* *2* *3* *4* *5* *Very Comfortable/Safe*

Have you ever posted your address on-line on a social networking service or private blog?
Please circle one option.

Yes *No* *Unsure*

How safe do you feel posting your address on a public blog or open forum?
Please circle a number from 1 to 5 on the following scale.

NOT Safe at All *1* *2* *3* *4* *5* *Very Comfortable/Safe*

Have you ever posted your address on a public blog or open forum?
Please circle one option.

Yes *No* *Unsure*

How safe do you feel making purchases with your credit card information on-line at a well-known on-line store? *Please circle a number from 1 to 5 on the following scale.*

NOT Safe at All *1* *2* *3* *4* *5* *Very Comfortable/Safe*

How safe to you feel making a purchase with your credit card on-line at a site that you have not been to or heard of before? *Please circle a number from 1 to 5 on the following scale.*

NOT Safe at All *1* *2* *3* *4* *5* *Very Comfortable/Safe*

Have you ever used your credit card to make a purchase on-line?
Please circle one option.

Yes *No* *Unsure*

If you have not used your credit card to make a purchase on-line, why have you never used your credit card to make a purchase on-line? *Please check one option.*

- ☐ I HAVE made a purchase with a credit card on-line.
- ☐ I do not own a credit card.
- ☐ I have never desired to purchase anything on-line.
- ☐ I feel unsafe making purchases on-line.
- ☐ Other: _____

Are there certain sites that you feel are more trust-worthy/safe than others?
Please circle one option.

Yes *No* *Unsure*

What traits/characteristics lead you to believe that a site is trust-worthy/safe?
Please check all that apply.

- ☐ The site has a privacy policy.
- ☐ The site looks clean and professional.
- ☐ The site is associated with an established, well-known organization.
- ☐ The site is easy to navigate.
- ☐ The site has a clear purpose.
- ☐ The site is colorful.
- ☐ The site lists the contact information of its authors/editors/sponsors.
- ☐ The site has attractive images.
- ☐ Other: _____

What traits or characteristics lead you to believe that a site is un-trustworthy/un-safe?
Please check all that apply.

- ☐ Lack of a Privacy Policy
- ☐ The site has spelling/grammatical errors.
- ☐ The site is NOT associated with an established, well-known organization.
- ☐ Navigating the site becomes confusing/is unclear.
- ☐ Contact information is not listed for the sites authors, editors, or sponsoring organization.
- ☐ The site does not have a clear purpose.
- ☐ The site is colorful.
- ☐ The site does NOT have attractive images.
- ☐ Other: _____

For which of the following computer-related activities would you attempt to take legal action against the perpetrator, if you believed that you had been a target of the activity? *Please check all that apply.*

- ☐ You believe someone remotely logged into your personal computer without your permission.
- ☐ You believe that someone intercepted your credit card number during an on-line purchase.
- ☐ You believed that someone electronically accessed your banking/financial data without your permission.
- ☐ I would not pursue legal action if I believed that someone had had accessed any information of mine without permission.
- ☐ Other: _____

Which of the following activities do you believe to be illegal according to Japanese law?
Please check all that apply.

- ☐ Obtaining National Security Information from a Government Computer
- ☐ Logging into any computer to which you do not have access
- ☐ Viewing information stored in a Government Computer to which you do not have access
- ☐ Accessing a Computer to Defraud and Obtain Value
- ☐ Transferring/communicating passwords of protected computers to unauthorized persons
- ☐ Logging into someone's personal computer without permission.
- ☐ Unauthorized access to and intentional damage of electronic data.

Until now, have you heard of the Japanese "Unauthorized Computer Access Law?"
Please circle one option.

Yes *No* *Unsure*

To the best of your knowledge, please write a brief summary of what you believe the Unauthorized Computer Access Law consists of:

Appendix C

Quotations – Japanese Survey

パスワードが必要なサイトに不正に入るなどの行為

You can take legal actions more easily when people access your information by the help of a computer. Japan making it illegal to access unauthorized computer info.

Recently I have heard that some Korean people sent cyber terrorism against a Japanese website, 2 channel, because of radical comments about Kim Yonai figure skator who competed with Mao Asada by some Japanese. I think people who always doing internet tend to probably misunderstand the virtual world for the real world so, people tend to be too aggressive against unreliable comments or info which is stupid.

Having absolutely no knowledge of Japanese law (let alone computer law), I would have to guess that the law denies access to government computers but does not protect the general public.

Logging onto computers to which you have not been granted formal access is illegal.

I would assume the violation of privacy – viewing, sharing, etc. of any found information that you do not have permission.

No one can access a computer they don't own or have permission to use

パスワードなどを不正に入手し、個人情報にアクセスすること。

分かりません。すみません。

Accessing or obtaining data/info without permission especially if considered "sensitive" or private.

他のコンピューターに不正にアクセスして（パスワードも解除して）、他の人のデータや情報を見たり、盗んだりすること。ウィルス目的に不正にアクセスする人もいるし、ただ情報を集めて詐欺目的でアクセスする人もいるので、それを禁止する方法。上の質問で聞かれたもの、全てが不正アクセス行為にあてはまると思います。

他の人のアカウントに入って、勝手にアカウントをいじったりする事。（メールのアカウントや、Ｆａｃｅｂｏｏｋなど）、ハッキング、児童ポルノ

Haven't a clue.

An individual that uses a computer containing information that is sensitive.

Appendix D

Quotations – American Survey

Makes online fraud and abuse illegal

I don't know

Heard of it, not sure of content. Illegal to access or spread information to which you have no right to access

To hold hackers accountable for their online interactions

Do not know what the act is

No idea really, just heard of it

What the name explicitly says… ? (Computer Abuse = Illegal unauthorized actions against privacy in IT-field)

Using information for illegal purposes

It states that it is illegal to use computers in unjust ways

A guideline to privacy infringement

No idea

Guidelines that tell you what is computer fraud and how you can abuse certain things like using someone else's computer to get their information.

Hacking and Breaking and Entering Computer Systems

Don't steal people's info

No idea

I think it protects the right to privacy

I would assume that it helps protect against computer fraud and abuse.

It consists of the laws that deal with computer privacy.

Fraudulent use of someone's computer –related services without his or her permission.

Prevents logging into other people's accounts

Computer fraud and abuse act consists of all that was listed on the previous page as illegal.

Clarifies laws related to computer fraud and abuse.

I haven't heard of the computer fraud and abuse act.

Laws that prevent people from breaking personal privacy laws.

It's a way to protect people who have traditionally lacked protection after becoming victims of identity theft or abuse.

Tries to protect the computer user from fraud and data theft.

Computer Fraud and Abuse Policies

Don't know what it is, but would guess not stealing data that isn't yours and not going on computers that aren't yours

Laws to protect Americans from computer fraud and abuse.

I have not heard of this act, but I'm guessing it has to with mostly illegal downloads.

I have no idea what it is, but from the name I assume it is an act protecting computer fraud.

Unlawfully gaining access to a computer you do not own without the owner's permission.

Works Cited

(2008). *2008 IC3 Annual Report.* Federal Bureau of Investigation.

Cox, N. (2006). *Technology and Legal Systems.* Burlington, VT: Ashgate Publishing Company.

Department of Justice. (2007). *Prosecuting Computer Crimes Manual*. Retrieved September 4, 2009, from http://www.cybercrime.gov/ccmanual/index.html

Doyle, C. (2008). *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Act and Related Federal Criminal Laws.* Retrieved September 16, 2009, from https://www.hsdl.org/?abstract&doc=264109&coll=documents&url=https%3A%2F%2Fwww.hsdl.org%2Fhomesec%2Fdocs%2Fcrs%2Fnps39-032708-02.pdf

Dunn, W. N. (1994). *Public Policy Analysis: An Introduction.* Englewood Cliffs, NJ: Prentice Hall.

Grabosky, P., & Broadhurst, R. (2005). *Cyber-Crime:The Challenge in Asia.* Hong Kong: Hong Kong University Press.

Grabosky, P., Smith, R. G., & Dempsey, G. (2001). *Electronic Theft: Unlawful Acquisition in Cyberspace.* Cambridge: Cambridge University Press.

Harada, K. (2003). *Japanese Information Security Status: Environment and Policies.* Tokyo: IT Security Center, Information-Technology Promotion Agency.

Klotz, R. J. (2004). *The Politics of Internet Communication.* Lanham: Rowman & Littlefield Publishers, Inc.

Nwokoma, A. (2008). *Process Evaluation of the Computer Fraud and Abuse Act of 1986.* Grambling, LA: Grambling State University.

Podgor, E. S. (2002). *Computer Crimes and the U.S.A. Patriot Act.* Retrieved September 14, 2009, from Criminal Justice Magazine: http://www.abanet.org/crimjust/cjmag/17-2/crimes.html

Saka, A. (2003). *Japan's Unauthorized Computer Access Law: Japan's Key Legislation Against Cyber-Crime.* Tokyo: National Police Agency of Japan.

Skibell, R. (2003). *Cybercrimes & Misdemeanors: A Re-evaluation of the Computer Fraud and Abuse Act.* New York: Columbia School of Law.

不正アクセス行為の禁止等に関する法律. (2000). Retrieved September 4, 2009, from 警察庁サイバー犯罪対策: http://www.npa.go.jp/cyber/legislation/hou/houann.htm

国家公安委員会. (２００９). *不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況.* 東京: 国家公安委員会.

警察庁. (2009). *平成２１年上期のサイバー犯罪の検挙状況等について.* 東京: 警察庁.