HACKING FOR FUN, PROFIT … AND AN A TO BOOT!

Vicki Miller Luoma,
Minnesota State University
Mankato, Minnesota

Milton Luoma
Metropolitan State University
St. Paul, Minnesota

Abstract

After earning an A in their school Computer and Network Security class project, three MIT students decided to present details at a well-known hackers conference on how to "get free rides for life" on the Massachusetts Bay Transit Authority (MBTA) transit system. When the MBTA discovered that the MIT students had hacked into their system and were planning to present their results to many other hackers, the MBTA sued the students and MIT alleging a violation of the Computer Fraud and Abuse Act. The defendants claimed that they were providing a service to the MBTA and the public as white-hat hackers by exposing system vulnerabilities. While the case was ultimately settled out of court short of trial, important legal and business issues were raised that will likely arise again in the future under similar circumstances. This case will allow students to study and to decide legal issues including whether the acts complained of were a violation of the Computer Fraud and Abuse Act. Further, was there a legitimate the First Amendment issue of prior restraint of publication of the security vulnerability? This case gives students a rare opportunity to study a case that involves students like them and an opportunity to decide whether they went too far.

Keywords: Hacking; Cloud Computing; Prior Restraint of Speech, Free Speech, Computer Fraud and Abuse Act, Hacktivist

Case Problem

This legal and business case gives students the opportunity to study facts involving college students much like themselves who complete a class project. However, the choices these students make in completing this project, although obtaining them an A grade in the class, creates serious legal problems for them, their university, and their professor. Studying this case allows students to exam the criminal, civil, constitutional, and ethical aspects of a case they can relate to their own university experience.

The Case

"What is this thing?" Zach Anderson shouted as he waved the restraining order he was just served by some young person dressed in black and riding a motorcycle. "Are you crazy? I got an A on this project! What does this mean?" Zach continued to shout to no one in particular. He raced from his apartment to Professor Ronald Rivest's office to see if he could help. The last thing Zach Anderson thought he would get as a graduation present was a restraining order along with a summons and complaint. How could everything go so wrong just as he thought everything was going so right? Zach and two of his friends had just completed a very tough course in Network and Computer Security at Massachusetts Institute of Technology taught by the renowned Ronald Rivest and earned an A in the class. Even better, their research was accepted for presentation at the famous/infamous DEFCON 16 conference. Zach had been bragging for weeks about how prestigious this presentation was going to be for them. Dr. Rivest was not in his office, but one of the graduate assistants was in the office and tried to help the students.

"What does this mean? Does it really say I can't present our paper at the DEFCON conference? I have already bought my airplane ticket and booked a room. Can someone just give you a piece of paper and prevent you from talking? I just don't understand." Zach had barely gotten those words out of his mouth and suddenly his classmates Ryan and Chiesa appeared and were also waving papers. "We have already bought our airline tickets!" they yelled almost in unison.

"Does this mean we can't go to the DEFCON Conference?" The DEFCON Conference was started in 1992 by Dark Tangent and is the world's longest running and largest underground hacking conference. "I guess we need to see a lawyer," the graduate assistant said. (MBTA v Anderson, et al, 2008)

The Facts

These three MIT students, Anderson, Ryan, and Chiesa were enrolled in the Network and Computer security class at Massachusetts Institute Technology, which was taught by the renowned Professor Ronald Rivest. Rivest was one of two creators of the modern public key encryption. As part of the class, Zach Anderson, R.J. Ryan, and Alessandro Chiesa were in a team for the semester. For their final project the students were to present research on network or computer security. The professor did not require the students to obtain approval of their projects or actually monitor any of the research. Anderson, Ryan, and Chiesa presented their final project after conducting research on the security vulnerabilities in the Automated Fare Collection System used by the Massachusetts Bay Transit Authority. As a result of their research they prepared a paper and received an A in the class. The paper revealed a study the students had done to find vulnerabilities in the Charlie Card system used by MBTA. Once they discovered vulnerabilities they all took a few free rides. Then they decided to present their paper to others and submitted it to DEFCON 16, the largest computer hacker convention. On July 30, 2008 a vendor called the Massachusetts Bay Transit Authority (MBTA) to alert them to an advertisement promising "Free Subway Rides for Life" on the MBTA. (Luoma & Luoma, Is there a White-Hat Exception to the Computer Fraud and Abuse Act?, 2009) The MBTA found Internet advertising for an upcoming presentation at DEFCON 16 conference that read as follows:

> "Want free subway rides for life? In this talk we go over weakness in common subway fare collection systems. We focus on the Boston T subway, and show how we reverse engineered the data on mag-stripe card. We present several attacks to completely break the CharlieCard, a MIFARE Classic smartcard used in many subways around the world,

> and we discuss physical security problems. We will discuss practical brute force attacks using FPGAs and how to use software-radio to read RFID cards. We go over social engineering attacks we executed on employees, and we present novel new method of hacking Wi-Fi: WARCARTING. We will release several open source tools we wrote to perform these attacks. (Docket No. 20, Ex 6)

The MBTA had no idea that the students had conducted the study until the vendor called and told them about the presentation scheduled for the DEFCON 16. MBTA officials tried calling the students to find out what was going on, but the students failed to meet with them or provide their study. As a result, the MBTA obtained a restraining order to prevent the students from appearing at the DEFCON conference. MBTA argued that the MIT students had violated the Computer Fraud and Abuse Act (CFAA). The MIT students argued that preventing them from speaking was a violation of their constitutional right of Freedom of Speech as a prior restraint.

Cast of Characters

MIT Students

Zach Anderson, R.J. Ryan, and Alessandro Chiesa were three students in Professor Ronald Rivest's Network and Computer Security class at Massachusetts Institute Technology. The students were taught in a team-based format, and for their last project decided to research the vulnerabilities of the MBTA's Charlie Card system. (MBTA v Anderson, et al, 2008)

Ronald Rivest

Professor Ronald Rivest is a renowned researcher, cryptographer and professor at MIT. Professor Rivest, along with two others, invented asymmetric key encryption algorithms and the RSA encryption system. Encryption is a means of encoding information in a format that is unintelligible without the proper key. Asymmetric encryption uses one key to encode information, such as text, but uses a different key to decrypt, or un-encode the information. For example, someone can make one key public, which anyone can use to encrypt a message to the person, and the other key is used to decrypt the message and is kept private so no one else can decrypt the message. The public encryption key will not decrypt the message. (MBTA v Anderson, et al, 2008)

MBTA

The Massachusetts Bay Transit Authority is the nation's fifth largest transit system serving approximately five million citizens in 175 cities. The MBTA has 183 bus routes, three rapid transit lines, five streetcars, four trolley lines and 13 commuter rail routes. In an average week the MBTA provides 1.4 million passenger trips with average weekday revenue of $700,000. The MBTA had recently installed an Automated Fare Collection system in an effort to improve its services. This system was called the "Charlie System." (Complaint MBTA v. Anderson, et.al) Over 68% of riders use the CharlieCard pass and 90% use monthly magnetic stripe cards. The Charlie Cards account for approximately $500,000 of revenue per weekday. (MBTA v Anderson, et al, 2008)

Dark Tangent (Jeff Moss)

Dark Tangent is a security consultant and founder of the Black Hat and DEFCON hacker conferences. He warns all participants at his conferences to beware there are undercover FBI agents in the audiences. In 2009 Jeff Moss became part of the Obama administration when he was appointed to the Homeland Security Advisory Council. The Black Hat conferences have approximately 4,000 attendees and the DEFCON is the premier hacking conference. (MBTA v Anderson, et al, 2008)

Electronic Frontier Foundation

The Electronic Frontier Foundation was founded by Perry Barlow and Mitch Kapor in 1990 to advocate for Internet civil liberties. It is an international organization that provides funds for legal defense and an organization that can provide a voice for emerging issues in cyber space. Both Barlow and Kapor felt that they had been harassed by the government over their online activities. (Godwin, 2003)

Issues

- **Criminal Law:** Is there a White Hat Exception (or Gray Hat Exception) to the Computer Fraud and Abuse Act? Should there be?
- **Constitutional:** Is the students' presentation at the DEFCON Conference protected speech under the First Amendment? Did the restraining order violate the students' constitutional rights? What is prior restraint of speech? When is it appropriate to grant a restraining order to prevent future speech? Which court ruled correctly in this case, the first judge or the second judge? Why?
- **Ethics:** Were the students' actions ethical? Is it ethical if your actions cause harm even if that wasn't your intent? These students have ended up security consultants is that ethical?
- **Tort:** Was the professor's supervision of the students negligent? Were the students' actions and the damages to the MBTA foreseeable? Did the professor or MIT have any vicarious liability for the students' actions?
- **Intellectual Property:** Did the students' action violate either copyright or trade secrets law?
- **Business Issues:** How big of a problem is hacking for business? Should companies welcome White Hat Hacker into their business for security reasons? What realistic measures should universities take to prevent hackers?

Web Source: http://www.eff.org/cases/mbta-v-anderson (Electronic Frontier Foundation, 2008) This site contains all the court papers and newspaper articles about the case including the Hearing Transcript, Exhibits, Motions and Memorandum.

Ethics

Students can be challenged to look at this problem through several different ethical lenses.

Discussion Questions

- What is the difference between a White Hat and Black Hat hacker?
- What about a Gray Hat hacker? If they intended to commit an illegal act but used that illegal act for good, is that ethical?
- Do you believe the purpose of the students' actions, or the end results of their actions, or the potential value of their actions should be the most important aspects in deciding whether their actions were ethical?
- Do you find any ethical violations by any parties – the professor, the students, the MBTA, or the DEFCON conference?
- Many of these hackers (hopefully former hackers) get high paying jobs at companies or with the government. Do you think it is ethical for companies and the government to hire hackers for security purposes and for these hackers to end up rich?

Free Speech/Prior Restraint

Discussion Questions

- The three MIT students argued that they had First Amendment rights to present their speech at the DEFCON Conference even though they obtained their information illegally. What do you think?
- What does "free speech" mean? How far does the Constitution protect you? What does prior restraint mean? The two judges in this case disagree about prior restraint (the restraining order preventing the MIT students from presenting at the DEFCON Conference.)
- The first judge granted the restraining order citing the damage this speech could do to the MBTA until it was able to fix the security breach. When the second judge refused to grant a temporary injunction pending trial, he said, "How much damage can some university students cause?" Which judge do you agree with? How can two judges disagree?
- The students' attorney stated "It's protected speech and vital to the free flow of information about computer security vulnerabilities. Silencing researchers does not improve security -- the vulnerability was there before the students discovered it and would remain in place regardless of whether the students publicly discussed it or not." Do you agree with this attorney?
- When is prior restraint constitutional and appropriate?

Business Issues

Discussion Questions

- Is Hacking an important issue for business?
- Are White Hat Hackers good for companies because they force the company to exam their security systems and exam their software for security weaknesses
- In reality hacking has not been a large problem for companies' bottom line so companies should continue to take a liaise-faire attitude towards security.
- Does the use of Cloud Computing increase hacking problems for companies?

- Why don't Companies pursue hackers under section G of the Computer Fraud and Abuse Act for Civil Damages?

Research Sources for Free Speech Argument

First Amendment to the Constitution

- Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances**.** (AmeUS)

New York Times Co. v. United States, 403 U.S. 713 (1971)

- This case is also known as the Pentagon Papers case in which the Nixon administration sought to enjoin the New York Times and the Washington Post newspapers from publishing excerpts from a top-secret United States Department of Defense history of the United States' involvement in the Vietnam War. (New York Times Co. v. United States, 1971)

Nebraska Press Assn. v. Stuart, 427 U.S. 539 (1979)

- In this case, the United States Supreme Court overturned the lower court's "gag order" in a trial citing the desire to obtain a fair trial. The Supreme Court found that alternative methods could have been used. (Nebraska Press Assn. v. Stuart, 1979)

Bantam Books v. Sullivan, 372 U.S. 58, 70 (1963)

- In this case the court found the following: "Any system of prior restraints of expression comes to this Court bearing a heavy presumption against its constitutional validity." (Bantam Books v. Sullivan, 1963)

Near v. Minnesota ex rel. Olson, 283 U.S. 697, 713 -14 (1931)

- The fact that the liberty of the press may be abused by miscreant purveyors of scandal does not make any the less necessary the immunity of the press from previous restraint in dealing with official misconduct. Subsequent punishment for such abuses as may exist is the appropriate remedy, consistent with constitutional privilege.' (Near v. Minnesota ex rel. Olson, 1931)

Research Sources for Criminal and Civil Arguments

Criminal Law; Computer Fraud and Abuse Act

- The Massachusetts Bay Transit Authority (MBTA) sued the students and MIT in United States District Court in Massachusetts, claiming that the students violated the Computer

Fraud and Abuse Act (CFAA) by delivering information to conference attendees that could be used to defraud the MBTA of transit fares.

- What about hackers claiming to be Gray Hats? Some computer security researchers argue that even though they have illegally hacked into a company's system, once they have discovered the security flaw they would like to report the problem to the company. Or sometimes they may have intended to do something illegal but have found a different security flaw and would like to report the flaw to the company, but under current laws they can't because it would reveal their illegal activity.

- These hackers would like an exception to criminal charges if they report the security flaw; what do you think? Do you think this argument should apply to the MIT Students? Did the MIT students intend to find a security problem or was the discovery inadvertent? Did they make an effort to report the flaw? Should there be such a thing as Gray Hat Exceptions to the Computer Fraud and Abuse Act? Even if the Computer Fraud and Abuse Act had provisions that required criminal "intent" would that excuse the MIT students' actions?

- The MIT students claim they did nothing illegal because their access "was *not* obtained through any kind of unauthorized access to computers. It was research that they performed by applying existing commonly used research technique to the magnetic stripe, to examine the data that are stored on those cards." (MBTA v Anderson, et al. Answer) Do you agree with the students? Why or why not?

  - What is unauthorized access to a computer?
  - Does authorization mean someone gave you permission?
  - What if the party had permission but used the computer in ways that wasn't considered by the person or company who gave permission?
  - The MBTA argues the students' actions violate the Computer Fraud and Abuse Act (CFAA) by enabling others to defraud the MBTA of transit fares. Do you agree?
  - What is the CFAA definition to illegal access to computers? What does case law state?

Research Sources

- Computer Fraud and Abuse Act 1030
- Shurgard Storage Centers, Inc. V Safeguard Self Storage, Inc, 119 F. Supp 2d 1121 (W.D. Washington, 2000)
- EF Cultural Travel BV v Explorica Inc 274 F.3d 577 (1st Cir. 2001)
- Luoma, M and Luoma, V.Luoma, M. &. (2010). The Computer Fraud and Abuse Act and the Law of Unintended Consequences. Digital Forensic Journal.
- In Meats by Linz, Inc. v. Dear, 2011 WL 1515028 (N.D. Tex. Apr. 20, 2011)

Teaching Notes

This case could be compared and contrasted to another case in which criminal action was brought under the Computer Fraud and Abuse Act.On May 15, 2008, Lori Drew was indicted in federal court in California for her alleged role in a hoax on MySpace directed at Megan Meier, a 13-year-old neighbor of Drew's who committed suicide in October 2006 after a "boy" she met on MySpace abruptly turned on her and ended their relationship. The boy was allegedly Lori Drew, who pretended to be 16-year-old "Josh Evans" to gain the trust of Megan, who had been fighting with Drew's daughter. The grand jury charged Drew with conspiracy and three counts of accessing protected computers without authorization in violation of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030. The indictment charges that read:

> [o]n or about the following dates, defendant DREW, using a computer in O'Fallon, Missouri, intentionally accessed and caused to be accessed a computer used in interstate commerce, namely, the MySpace servers located in Los Angeles County, California, within the Central District of California, without authorization and in excess of authorized access, and, by means of interstate commerce obtained and caused to be obtained information from that computer to further tortious acts, namely intentional infliction of emotional distress on [Meier].

The prosecutor brought action against Lori Drew under the CFAA criminal provisions because she violated the terms of service of MySpace which prohibited creating fake profiles, and she did so in furtherance of committing the tort of intentional infliction of emotional distress. The CFAA § 1020(a)(2)(C) makes it a criminal misdemeanor to “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer if the conduct involved an interstate or foreign communication.” The CFAA § 1030(c)(2)(B)(2) make it a felony if one “intentionally accesses a computer without authorization . . . , and thereby obtains . . . information from any protected computer” and “the offense was committed in furtherance of any . . . tortious act [in this case intentional infliction of emotional distress] in violation of the . . . laws . . . of any State.” (U.S. v. Lori Drew, 2009)

Civil/Negligence and Vicarious Liability

- The students completed this study as part of school project. Did the professor have a duty to supervise their research?
- Once the project was turned into the professor did the professor have a responsibility to inform the MBTA of the vulnerabilities in their system?
- After this incident, the professor included in his syllabus an ethics code and required the students to get permission from him prior to conducting research. Does that fact prove the professor responsibility?
- In this case is reasonable to expect the professor or the university to have control over these students?
- Normally vicarious liability involves a master/servant relationship, can than apply also to Faculty/student.

Research Sources

- Gebser v. Lago Vista Independent School District 524 U.S. 274 (1998).
- Merrett v. Babb EWCA Civ 214 [2001]

Teaching Notes

The general rule in tort law is that a person who authorizes a tort will personally be liable for damage or harm as a result. However, vicarious liability defines the circumstances in which a person is liable for the torts of another without express authorization or ratification. The purpose of vicarious liability is to hold the proper party responsible when harm is committed. In this case the professor made the assignment but did not monitor the topic or the methods used by the students. (Gebser v Lago Vista Independent School District, 1998) (Merrett v. Babb EWCA, 2001)

Hacking was a problem almost the moment computers were invented. By 1984 it had reached epidemic proportions and so Congress passed the first Computer Fraud and Abuse Act (CFAA). The original purpose of this act was to protect government computers and records at financial institutions. The original act as been amended numerous times and now covers all computers and has both criminal and civil provisions.

Copyright, Trade Secret Violations

Discussion Questions

- Can the discovery of a security flaw be a violation of a trade secret?
- What is reverse engineering? Can that be a patent infringement?
- Is this an abuse of the Computer Fraud and Abuse Act?
- Are vulnerabilities within a program, or software or hardware system, protected trade secret information?
- If the courts find reverse engineering as violation of trade secrets or patent infringement, will that stifle researchers from finding vulnerabilities in computer systems?
- There is an anti-circumvention provision of the DMCA, 17 U.S.C. 1201, what does that mean?

Research Sources

- DMCA, 17 U.S.C. 1201
- 35 U.S.C. § 1201(a)(1)(A)

Teaching Notes

The anti-circumvention provisions of the DMCA, 17 U.S.C. 1201, prohibit circumvention of “technological protection measures” that effectively control access to copyrighted works. The law also prohibits trafficking in tools that are primarily designed for circumvention, have only limited commercially significant purpose other than circumvention or are marketed for circumvention.

Under 35 U.S. C. § 1201(a)(1)(A) product reverse engineering is illegal if the action effectively controls access to a work protected by copyright law. In Universal City Studios v.

Remierdes 55 U.S.P.Q.2d 1873 (S.D.N.Y. 2000) an online hacker magazine posted software called DeCSS which stripped the encryption for DVDs (Digital Video Disks.) The motion picture industry brought suit arguing that this program would allow users to circumvent copyrighted work. The court found in favor of the motion picture industry even though the defendants had argued they had used legitimate reverse engineering procedures.

In another interesting case, IOActive, a security firm created a hand-held device that read and cloned the prox cards used for access to a building used by many schools and companies. They planned to demonstrate and explain their findings at the Black Hat Conference in Washington, D.C. HID Global, the company who produced the cards, threatened a lawsuit on patent infringement. IOActive decided not to present its findings at the conference for fear of a lawsuit. An ACLU attorney read the findings at the conference daring HID to bring a lawsuit.

In yet another case, one of the most common civil action using the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, et seq. is a trade secret case. Steve Dear was the general manger of the Meats by Linz, Inc (MBL) and had signed an employment agreement in which included an non-disclosure agreement. Dear took a job with a competitor of Meats but before turning in his resignation he accessed MBL's password-protected confidential and proprietary information to which only he, and others on a "need to know" basis, had access and downloaded confidential information. (Meats by Linz, Inc. v. Dear, 2011) He then emailed this information to his new employer. MBL sued alleging violation of the Computer Fraud and Abuse Act for improperly and illegally accessing its confidential and proprietary information on its computer system "without authorization" or by "exceeding authorization". Dear argued he had authority to be on the computer. (Meats by Linz, Inc. v. Dear, 2011)

Is this computer misuse? Is it different from what the MIT students did? Should Dear be charged criminally under the act? What about the MIT students? How can one act cover both kinds of actions? Is hacking worse than giving away trade secrets?

In an earlier case much like the MBL case, Shurgard Storage case Shurgard sued Safeguard when one of Shurgard's employees, Eric Leland, accepted a position at Safeguard. Leland used the computer at Shurgard to send Safeguard confidential business plans, expansion plans and other trade secrets. Shurgard sued Safeguard under the Computer Fraud and Abuse Act claiming that Leland, encouraged by Safeguard, misused Shurgard's computer and violated the CFAA. Safeguard argued that Leland had Shurgard's permission to use the computer while he was still an employee of Shurgard. The court found as soon as Leland was working against the interest of his employer, the employee was without authorization and thus in violation of the Computer Fraud and Abuse Act. (Shurgard Storage Centers, In v Safeguard Self Storage, Inc, 2000)

In E.F. Cultural Travel BV v. Explorica, Inc., former employees of E.F. Cultural started their own travel company. The former employees used a scraper program to collect non-confidential data about E.F. Cultural on its website. The court found that the employees violated the CFAA even though the information was freely available to anyone accessing the website. The court found that only an employee would understand the value of the information obtained.

The courts have also found in this case that the $5,000 damages requirement could be the cost of hiring an expert to determine that the former employees had used the scraper program. (EF Cultural Travel BV v Explorica Inc, 2001)

Business Issues

Discussion Questions

- Why is Business Hacking Increasing?
- Hackers include hacktivist groups like Anonymous, corporate and state-sponsored cyber espionage and organized crime and rogue hackers. What is the difference in these Hackers if any?
- Does the motives of the Hackers matter?
- Which type of hackers cause the most damage to businesses?
- Why has the 2011 been called the year of the Hacker?

Research Sources

Computer Fraud and Abuse Act Section G

Teaching Notes

The Computer Fraud and Abuse Act is a criminal statute passed to provide punishment for Hackers and other computer criminals but it also has a section G that allows anyone to bring a Civil Action under this statute. Businesses would have the authority to after individuals or organizations who have hacked into their companies. Instead companies have mainly used this authority to go after former employees for trade secret violations.

- (g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses [5] (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware. (35US)

Many Hackers argue that they are doing a service to the Business by hacking and showing their vulnerabilities. (Majuca, 2010)

Suggested Teaching Methodology

- Problem Based Learning - Give each team the original ill-structured problem and require the teams to come up with the issues, make a decision and argue their stances.

- Team work – Give each team a different issue to resolve and present to the rest of the class.
- Debate – Give the different teams different sides to argue. For example one team could argue it is a prior restraint of Free Speech and the other side could argue it side after doing research.

Bibliography

35 (U.S.C. 1201).

1030 (Computer Fraud and Abuse Act).

Amendment 1 (U.S. Constitution).

Bantam Books v. Sullivan, 372 (U.S. 1963).

Bantam Books v. Sullivan, 372 U.S. 58 (U.S. 1963).

DMCA, 17 (U.S.C. 1201).

EF Cultural Travel BV v Explorica Inc, 274 (F 3rd 577 2001).

Electronic Frontier Foundation. (2008, August 19). *Defending Your Rights in the Digital World*. Retrieved July 8, 2010, from MBTA v Anderson: http://www.eff.org/cases/mbta-v-anderson

Gebser v Lago Vista Independent School District, 524 (U.S. 274 1998).

Godwin, M. (2003). *Cyber Rights: Defending Free Speech in the Digital Age.* Boston: Cambridge MIT Press.

Luoma, M., & Luoma, V. (2009). Is there a White-Hat Exception to the Computer Fraud and Abuse Act? *South Africa Cyberlaw and ICT Conference* (pp. 95-103). Pretoria: ICT Conference.

Luoma, M., & Luoma, V. (2010). The Computer Fraud and Abuse Act and the Law of Unintended Consequences. *Digital Forensic* , 40-52.

Majuca, R. a. (2010). ARTICLE: DATA DEVOLUTION: CORPORATE INFORMATION SEC. *Chicago-Kent Law Review* (p. 713). Chicago: Chicago Kent Law Review.

MBTA v Anderson, et al, Civ No. 08-11364-GAO (D. Mass August 19, 2008).

Meats by Linz, Inc. v. Dear, WL 1515028 (N.D. Texas Aprl 20, 2011).

Merrett v. Babb EWCA, 214 (District 2001).

Near v. Minnesota ex rel. Olson, 283 U.S. 697 (U.S. 1931).

Nebraska Press Assn. v. Stuart, 427 U.S. 539 (U.S. 1979).

New York Times Co. v. United States, 403 (U.S. 1971).

Shurgard Storage Centers, In v Safeguard Self Storage, Inc, 119 F. Supp 2d 1121 (W.D. Washington 2000).

U.S. v. Lori Drew, 259 F.R.D. 449 (C.D.Cal. 2009).