Laws which define computer crimes

Now let's move the discussion to laws which define computer crimes. We touched on this a little in a previous video but now we'll go into greater depth. Oh … and once again, there are a lot of laws related to cyber-crime and sooner or later you may have to memorize all of them, especially if you're planning on taking some of the various certification tests. But for now just try and get familiar with the main laws, but don't stress and try and memorize everything. Remember the tests for this class are open book, so you can always look up the specific laws if you need to.

Ok, now let's get to discussing the laws. Humans have long had problems with crimes like trespass, theft or assault. So some of the first laws developed addressed activities like harming someone, stealing or damaging property and made them illegal. Computers are a fairly new development in human history, and when they first came into use there were no laws that specifically addressed crimes that involved computers, either as the victim of an attack or theft, or as a tool in an attack.

Most of the early computer crimes involved someone damaging a computer. Some of the first recorded crimes happened in the late 1960's when computers were large and expensive so personal computers didn't exist. An employee would get angry and hit the company computer with a hammer or shoot it with a gun. Since there were no laws specifically protecting computers the existing laws against damaging property would be used. But it also brought up problems as these charges didn't take into account the damage to the information on the computers.

In the 1970's people started hacking into phone systems and computers through the phone system. While laws against trespass existed there was a question whether they could be applied or not as they don't specifically address computers, networks, or other forms of technology.

While it might seem to make common sense that breaking into a computer is a form of trespass our justice system has a characteristic or feature called the "rule of lenity" which means that if there is any doubt as to whether a law may be applied then it must be assumed that it doesn't apply. The rule of lenity requires the wording of any law describing a crime to be clear and unambiguous. This meant that entirely new laws needed to be written and approved to ensure they applied to computer crimes.

Over the years new laws have been passed and there are now several state and Federal laws that specifically address computer and technology crimes. For this class you should be aware of the main Federal law, the Computer Fraud and Abuse Act 18 (U.S. Code § 1030) (CFAA). This law was first enacted in 1984 and has been revised several times to clarify any issues brought up in court cases and accommodate changes in technology. The CFAA has several sections and criminalizes the following actions:

- Computer espionage
- Computer trespassing, and taking government, financial, or commerce info
- Computer trespassing in a government computer
- Committing fraud with computer
- Damaging a protected computer (including viruses, worms)
- Trafficking in passwords of a government or commerce computer
- Threatening to damage a protected computer. This includes threats to steal data, publicly disclose stolen data or not repair damage already caused (ransomware).

The CFAA was originally limited in scope to crimes involving a "federal interest computer" which includes any computer used by a government agency or contractor, as well as computers used by any financial institution. During one the revisions the scope was expanded to include any computer or device “which is used in or affecting interstate or foreign commerce or communication”, which means applies to almost any computer, networking device, cell phone, etc.

The one large category of offenses not covered by the CFAA are cyberstalking, cyber bullying and cyber harassment. In some cyber stalking and cyber harassment cases prosecutors have been able to obtain convictions using real world stalking and harassment laws but bullying cases, and cyber bullying in particular, have been harder to prosecute. It’s a serious issue with many cases of young people committing suicide after being bullied online. Most politicians have recognized the need for laws to address these crimes and some attempts have been made at developing legislation. While laws have been proposed they have been seen by most as too vague and far reaching and nothing has been passed at a Federal level, at least at the time of this writing, December 2016.

https://ilt.eff.org/index.php/Computer_Fraud_and_Abuse_Act_(CFAA)

https://www.law.cornell.edu/wex/statutory_construction

https://www.law.cornell.edu/uscode/text/42/13031

http://www.mekabay.com/overviews/history.pdf

http://groups.csail.mit.edu/mac/classes/6.805/articles/computer-crime/rasch-criminal-law.html

Laws which require data to be protected

Another set of laws you should be familiar with are those which require certain organizations and certain types of businesses to protect their digital data. These laws will be more of a concern to the Information Security and Assurance portion of cyber security than they are to pure forensics. But one of the requirements of these laws that a forensics investigation must be performed any time there’s a security incident. These laws include:

- HIPAA (Health Insurance Portability and Accountability Act of 1996) requires medical facilities to protect patient records.
- Gramm-Leach-Bliley Act (GLBA) requires financial institutions to protect customer data. It also requires financial institutions to send annual written notices that explain their information-sharing practices, which is why you get those weird letters from your bank and credit card companies.
- FERPA Family Educational Rights and Privacy Act (20 U.S.C. § 1232g) requires educational institutions to protect student data. Only parents can access this data until the student reaches the age of 18 at which time only the student should have access.
- Computer Security Act of 1987 requires federal agencies to protect their data

Note that there’s no law requiring you or any private citizen to protect your own computer, but maybe there should be. Maybe we need laws that fine people that don’t use basic security practices such as running free security software or changing the password on their home router; especially if their computer becomes a zombie and is used as part botnet for attacking other computers. In other words, you need to

do some minimal amount of work to keep your home computer and network secure or face a fine. We already have laws that set a precedent for this. I know that many cities, including the City of Kennewick, have laws that make it illegal to leave your running car unlocked. This is a controversial area, and you'll need to draw your own conclusions. But let me tell you that if you get a job in cyber security I bet you'll be surprised at how lax most people are about protecting their data and equipment.

Mandatory Reporting

The next law we'll talk about is the Child Abuse mandatory reporting law, which is part of the U.S. code (42 U.S. Code § 13031). You don't really need to know the details about this law, but you should have some idea of what you should do if you find evidence of child abuse on a computer.

This law requires people in certain occupations to report any suspicions of child abuse. These professions include anyone on the medical field, teachers, foster parents, agents of law enforcement, and film processors. They must file a report with the appropriate authorities if they see any evidence of physical or mental abuse, or evidence of exploitation such as pictures or video.

The occupations of forensics investigator or Information Technology worker are not listed, so if you're working on someone's computer or phone and see some suspicious pictures you are not legally required to make a report (unless you work at a hospital, school, etc.) However I'd like to suggest that everyone has a moral obligation to report child abuse, regardless of their occupation.

In 2008 the state of Texas passed a law that required all IT techs to obtain a Private Investigators license. Part of the reasoning behind the law is that as PIs, anyone working on a computer would know what to do if they found suspicious material; how to report it and how to preserve the evidence. Several computer repair shops filed a suit to rescind the law as obtaining a PI license is both time consuming and expensive, and the law has since been taken off the books. But hopefully you can see the point behind the law. And you might also want to think about what you're going to do if you find yourself in this situation. That is, what will you do if you're working on someone's computer and you find evidence of child porn or other crimes?

Ok, that's it for the main laws related to cyber security. Once again don't worry about memorizing a bunch of details about these laws, just try and remember the names of the main laws and what they cover. And also remember you can always look these up if you need to.