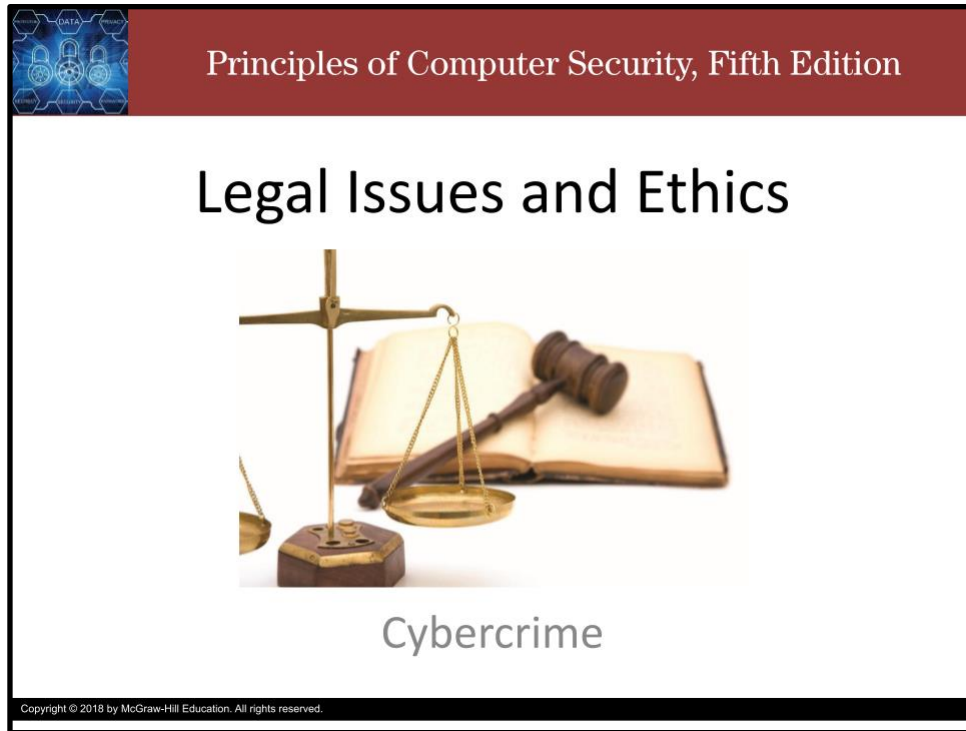


Legal Issues and Ethics: Cybercrime


Slide 1



The image shows a book cover with a dark red header. The header contains the text "Principles of Computer Security, Fifth Edition" in white. Below the header, the title "Legal Issues and Ethics" is written in large black font. Underneath the title is a photograph of a brass scale of justice, an open book, and a wooden gavel. At the bottom of the cover, the word "Cybercrime" is written in a grey font. A small copyright notice is visible at the very bottom of the cover.

Principles of Computer Security, Fifth Edition

Legal Issues and Ethics




Cybercrime

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Howdy! In this video, we begin a discussion of laws and standards related to cybercrime.

Slide 2



Principles of Computer Security, Fifth Edition

Cybercrime

- Three types of computer crimes commonly occur:
 - Computer-assisted crime
 - Computer-targeted crime
 - Computer-incidental crime
- Legal system slow to react; Law enforcement struggles to respond to new threats
- 80s and 90s: most cybercrime was destructive
- 00s and onward: all about the Benjamins \$\$\$\$\$

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

There are three forms of computer involvement in criminal activity: The computer as a tool of the crime, the computer as a victim of a crime, and the computer that is incidental to a crime.

The differentiating factor is in how the computer is specifically involved from the criminal's point of view.

Just as crime is not a new phenomenon, neither is the use of computers, and cybercrime has a history of several decades.

What is new is how computers are involved in criminal activities.

The days of simple teenage hacking have been replaced by organized crime such as controlled botnets and acts designed to attack specific targets.

The legal system has been slow to react, and law enforcement has been hampered by their own challenges in responding to the new threats posed by high-tech crime.

What comes to mind when most people think about cybercrime is a computer that is targeted and attacked by an intruder.

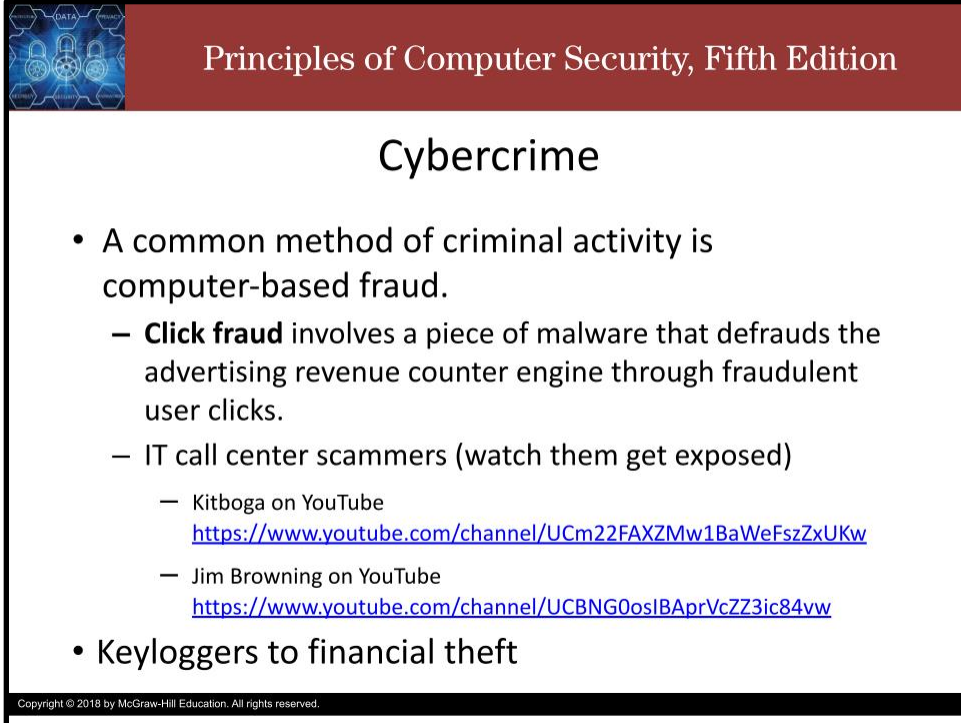
The criminal attempts to benefit from some form of unauthorized activity associated with a computer.

In the 1980s and '90s, cybercrime was mainly virus and worm attacks, each exacting some form of damage, yet the gain for the criminal was usually negligible. In the 21st century, with new forms of

malware, rootkits, and targeted attacks; criminals can now target individual users and their bank accounts.

In the current environment it is easy to predict where this form of attack will occur—where there is money, there is motive for crime.

Slide 3



Principles of Computer Security, Fifth Edition

Cybercrime

- A common method of criminal activity is computer-based fraud.
 - **Click fraud** involves a piece of malware that defrauds the advertising revenue counter engine through fraudulent user clicks.
 - IT call center scammers (watch them get exposed)
 - Kitboga on YouTube
<https://www.youtube.com/channel/UCm22FAXZMw1BaWeFszZxUKw>
 - Jim Browning on YouTube
<https://www.youtube.com/channel/UCBNG0osIBAprVcZZ3ic84vw>
- Keyloggers to financial theft

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

A common method of criminal activity is computer-based fraud, such as click fraud and IT call center scammers.

eBay and Amazon are frequent targets of fraud. Whether the fraud occurs by fraudulent listing, fraudulent bidding, or outright stealing of merchandise, the results are the same: a crime is committed. As users move toward online banking and stock trading, so moves the criminal element.


Malware designed to install a keystroke logger and then watch for bank/brokerage logins is common on the Internet.

Once the attacker finds the targets, they can begin looting accounts.

Their risk of getting caught and prosecuted is exceedingly low.

If you walk into a bank in the United States and rob it, the odds are better than 95 percent that you will be doing time in federal prison after the FBI hunts you down and slaps the cuffs on your wrists.

But if you do it through a computer, the odds are even better for the opposite: less than 1 percent of these attackers are caught and prosecuted.



Principles of Computer Security, Fifth Edition

Cybercrime

- Low risk of getting caught
- Steal IP, PII (credit cards, drivers' licences, SSN, etc.)
 - What is your data worth on the dark web?
<https://www.privacyaffairs.com/dark-web-price-index-2021/>
- Physical isolation of criminal from crime
 - Investigation and prosecution more challenging.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The low risk of being caught is one of the reasons that criminals are turning to computer crime.


Today's cyber criminals use computers as tools to steal intellectual property or other valuable data and then subsequently market these materials through underground online forums.

Using the computer to physically isolate the criminal from the direct event of the crime has made the investigation and prosecution of these crimes much more challenging for authorities.

Principles of Computer Security, Fifth Edition

Cybercrime

- The last way computers are involved with criminal activities is through incidental involvement.
 - Al Capone: They can't collect legal taxes from illegal money.
Supreme Court in U.S. v. Sullivan:
- (3 forms of involvement) * (criminal use of computers) + (remote access) = 21st century cybercrime



Copyright © 2018 by McGraw-Hill Education. All rights reserved.


The last way computers are involved with criminal activities is through incidental involvement.

Back in 1931, the U.S. government used accounting records and tax laws to convict Al Capone, who was a notorious gangster, of tax evasion.

Computers are also used to traffic child pornography and engage in other illicit activities.

Because these activities existed before computers, the use of the computer is actually incidental to the crime itself.

With the three forms of computer involvement in criminal activities, multiplied by the myriad of ways a criminal can use a computer to steal or defraud, added to the indirect connection mediated by the computer and the Internet, computer crime of the 21st century is a complex problem indeed.



Principles of Computer Security, Fifth Edition


Common Internet Crime Schemes

- To find crime, just follow the money.
- In the United States, the FBI and the [National White Collar Crime Center \(NW3C\)](#) have joined forces in developing the [Internet Crime Complaint Center \(IC3\)](#), an online clearinghouse that communicates issues associated with cybercrime.
- One of the items provided to the online community is a list of common Internet crime schemes and explanations of each.
 - <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes>

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

In the United States, the FBI and the National White Collar Crime Center (NW3C) have joined forces in developing the Internet Crime Complaint Center (IC3), an online clearinghouse that communicates issues associated with cybercrime.

One of the items provided to the online community is a list of common Internet crime schemes and explanations of each along with advice on how to prevent these crimes through individual actions.



Principles of Computer Security, Fifth Edition

Sources of Laws

- 3 primary sources
 - Statutory – law passed by legislative body
 - Administrative – law made by administrative body (with power granted by legislative body)
 - Common/Case – law interpreted by judicial body; based on precedent
- All 3 involved in computer security

Copyright © 2018 by McGraw-Hill Education. All rights reserved.


In the United States, there are 3 primary sources of laws and regulations: statutory, administrative, and common or case law.

A statutory law is passed by a legislative branch of government, be it the U.S. Congress or a local city council.

The power of government-sponsored agencies, such as the EPA, FAA, FCC, and others, lies in the ability to enforce behaviors through administrative rule making, or administrative law.

Common law, or case law, is based on previous events or precedent. This source of law comes from the judicial branch of government: judges decide on the applicability of laws and regulations.

All three sources have an involvement in computer security.



Principles of Computer Security, Fifth Edition

Computer Trespass

- Unauthorized entry into a computer system via any means.
- New area of law with (inter)national consequences
 - Within country: national laws
 - Between countries: international law and treaties
 - Borders are immaterial
- Crime in many countries
 - US, Canada, EU members
 - Laws vary by country, but have similar provisions
 - Cross-national issues growing in prominence
 - Likely require international treaty in the future

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Computer trespass is the unauthorized entry into a computer system via any means, including remote network connections.


These crimes have introduced a new area of law that has both national and international consequences.

For crimes that are committed within a country's borders, national laws apply.

For cross-border crimes, international laws and international treaties are the norm.

Computer-based trespass can occur even if countries do not share a physical border.

Computer trespass is treated as a crime in many countries. National laws against computer trespass exist in many countries, including Canada, the United States, and the member states of the European Union. These laws vary by country, but they all have similar provisions defining the unauthorized entry into and use of computer resources for criminal activities. Whether called computer mischief as in Canada or computer trespass as in the United States, unauthorized entry and use of computer resources is treated as a crime with significant punishments. With the globalization of computer network infrastructure, issues that cross national boundaries have arisen and will continue to grow in prominence. Some of these issues are dealt with through the application of national laws upon request of another government. In the future, an international treaty may pave the way for closer cooperation.



Principles of Computer Security, Fifth Edition

Computer Trespass

- Unauthorized entry into a computer system via any means.
- New area of law with (inter)national consequences
 - Within country: national laws
 - Between countries: international law and treaties
 - Borders are immaterial
- Crime in many countries
 - US, Canada, EU members
 - Laws vary by country, but have similar provisions
 - Cross-national issues growing in prominence
 - Likely require international treaty in the future

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The Convention on Cybercrime of the Council of Europe, known as the Budapest Convention, is the only binding international instrument on the issue of cybercrime.

It serves as a guideline for any country developing comprehensive national legislation against Cybercrime and as a framework for international cooperation between State Parties to the treaty.

The Convention on Cybercrime is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security.

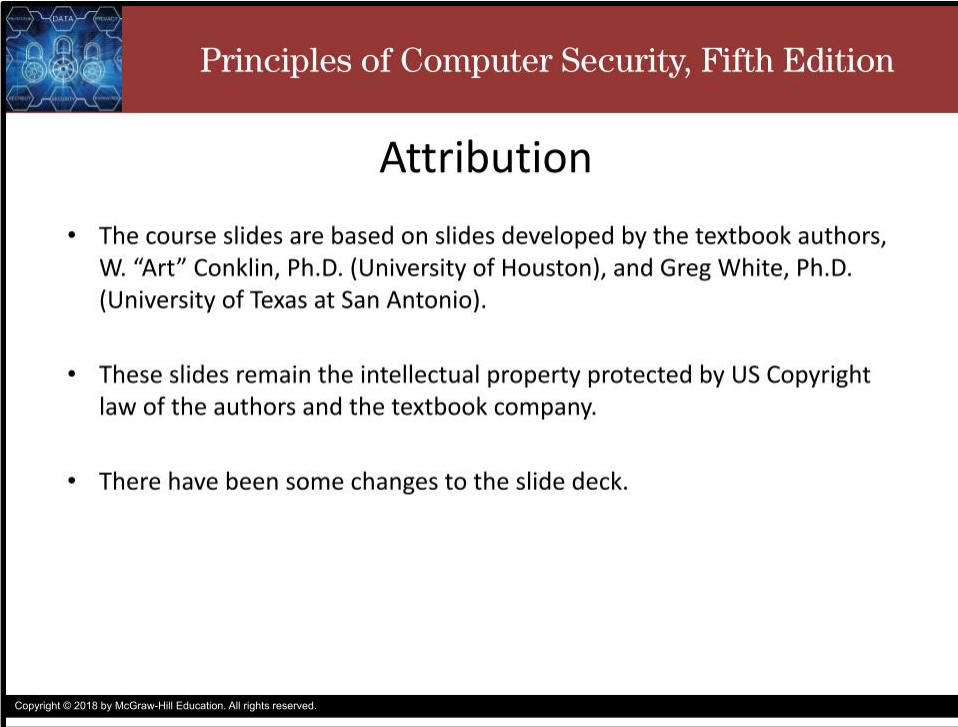
It also contains a series of powers and procedures such as the search of computer networks and interception. It has been supplemented by an additional protocol making any publication of racist and xenophobic propaganda via computer networks a criminal offense.

The convention is the product of four years of work by the Council of Europe, but also by the United States, Canada, Japan, and other non-CoE countries. The convention has been ratified and came into force in July 2004, and by September 2006, 15 member nations had also ratified it. The United States ratified it in the summer of 2006, with it entering into force in the United States in January 2007.

One of the main objectives of the Convention, set out in the preamble, is “to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international cooperation.” This has become an important issue with the globalization of network communication. The ability to create a virus anywhere in the world and escape prosecution because of the lack of local laws has become a global concern.

One of the challenges of enacting elements such as this convention is the varying legal and constitutional structures from country to country. Simple statements such as a ban on child pornography, although clearly desirable, can run into complicating issues, such as constitutional protections of free speech in the United States. Because of such issues, this well-intended joint agreement will have variations across the political boundaries of the world.

Slide 10



The slide features a dark red header with the text "Principles of Computer Security, Fifth Edition" in white. To the left of the header is a small graphic with a blue background and white icons representing data, security, and connectivity. The main content area is white with a black border. The title "Attribution" is centered in a large, bold, black font. Below the title is a bulleted list of three items. At the bottom of the slide, there is a small black bar containing the copyright notice.

Principles of Computer Security, Fifth Edition

Attribution

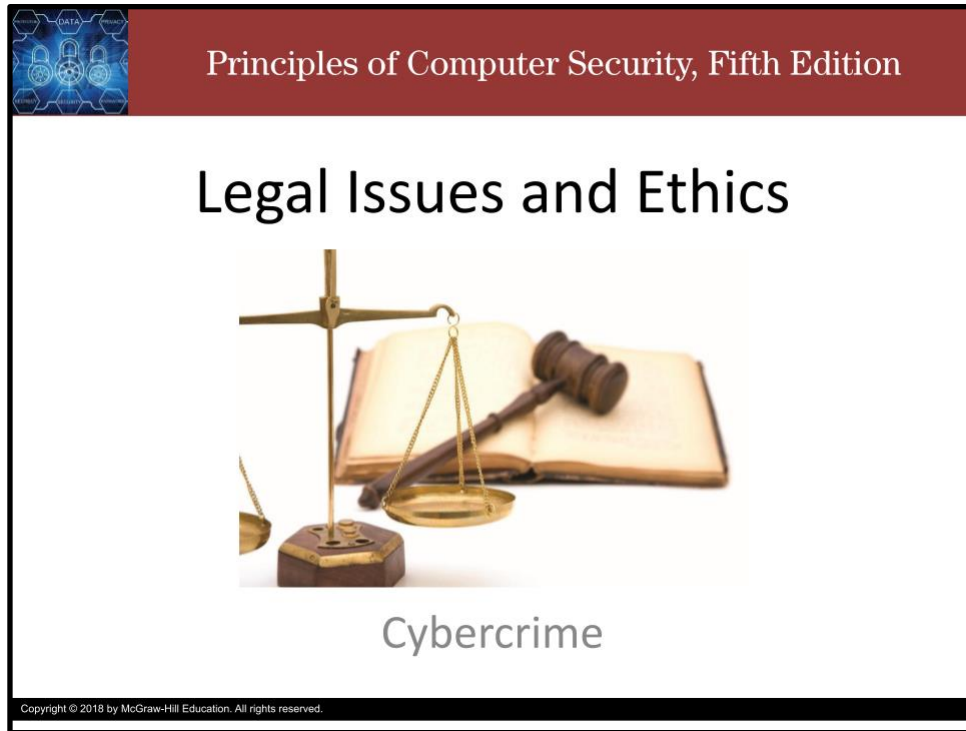
- The course slides are based on slides developed by the textbook authors, W. "Art" Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you and take care.

Legal Issues and Ethics: Significant U.S Laws

Slide 1



The image shows the cover of a book titled "Principles of Computer Security, Fifth Edition". The cover has a dark red header with the title in white. Below the header, the text "Legal Issues and Ethics" is prominently displayed in a large, black, sans-serif font. Underneath this, there is a photograph of a brass scale of justice, an open book, and a wooden gavel. At the bottom of the cover, the word "Cybercrime" is written in a smaller, grey font. A small copyright notice is visible at the very bottom of the cover.


Principles of Computer Security, Fifth Edition

Legal Issues and Ethics

Cybercrime

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Howdy! In this video, we continue our discussions of laws and standards related to cybercrime with a focus on significant laws in the united states.



Principles of Computer Security, Fifth Edition

Significant U.S. Laws

- The United States is a has been leader in the development and use of computer technology
- US has a long history with computers and cybercrime.
- Also legal leadership
 - Once an item is identified and handled by the legal system in one jurisdiction, subsequent adoption in other jurisdictions is typically quicker.


Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The United States is a leader in the development and use of computer technology and therefore has a long history associated with computers and cybercrime.

Because legal systems tend to be reactive and move slowly, this leadership position has translated into a leadership position from a legal perspective as well.

One supposed advantage of this legal leadership position is that once an item is identified and handled by the legal system in one jurisdiction, subsequent adoption in other jurisdictions is typically quicker.

Slide 3



Principles of Computer Security, Fifth Edition

Electronic Communications Privacy Act (ECPA)

- 1986.
- Addresses privacy issues of electronic communications
 - Email, cellular, workplace, etc.
- Section 1: modify federal wiretap statutes
- Section 2 (Stored Communications Act): criminal sanctions for unauthorized access
- Section 3: pen registers, tap and trace.
- Prohibited monitoring of employee communications without consent
- Protection under 4th amendment – reasonable expectation of

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

PRIVACY

The ECPA of 1986 addresses a myriad of legal privacy issues that resulted from the increasing use of computers and other technology specific to telecommunications.

Sections of this law address e-mail, cellular communications, workplace privacy, and a host of other issues related to communicating electronically.


Section I was designed to modify federal wiretap statutes to include electronic communications.

Section II, known as the Stored Communications Act (SCA), was designed to establish criminal sanctions for unauthorized access to stored electronic records and communications.

Section III covers pen registers and tap and trace issues. Tap and trace information is related to who is communicating with whom and when. Pen register data is the conversation information.

A major provision of ECPA was the prohibition against an employer's monitoring an employee's computer usage, including e-mail, unless consent is obtained (for example, clicking Yes on a warning banner is considered consent).

Other legal provisions protect electronic communications from wiretap and outside eavesdropping, as users are assumed to have a reasonable expectation of privacy and afforded protection under the Fourth Amendment to the Constitution.



Principles of Computer Security, Fifth Edition

Warning Banners

- Establish expected level of privacy
 - None.
- Notification of real-time monitoring
 - Security, business/profit, performance
- Consent to monitoring (as condition of access)
 - Even if you expected privacy, your consent waives it away
- Warning that sys/net admin will comply with all (lawful) orders
 - Your ISP, employer, etc. will not protect you

Copyright © 2018 by McGraw-Hill Education. All rights reserved.


A common practice with respect to computer access today is the use of a warning banner. These banners are typically displayed whenever a network connection occurs and serve four main purposes.

First, from a legal standpoint, they establish the level of expected privacy (usually none on a business system).

Second, they serve notice to end users of the intent to conduct real-time monitoring from a business standpoint. Real-time monitoring can be conducted for security reasons, business reasons, or technical network performance reasons.

Third, they obtain the user's consent to monitoring. The key is that the banner tells users that their connection to the network signals their consent to monitoring. Consent can also be obtained to look at files and records. In the case of government systems, consent is needed to prevent direct application of the Fourth Amendment.

And the last reason is that the warning banner can establish the system or network administrator's common authority to consent to a law enforcement search.



Principles of Computer Security, Fifth Edition

Computer Fraud and Abuse Act (CFAA)

- The **CFAA** of 1986, amended in 1994, 1996, in 2001 by the USA Patriot Act, and in 2008 by the Identity Theft Enforcement and Restitution Act.
 - Serves as the current foundation for criminalizing unauthorized access to computer systems.
- CFAA makes it a crime to knowingly access a “protected computer” or to use a computer in a crime that is interstate in nature.
 - Protected computer: used by financial institution or US Gov’t or used in interstate commerce


Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The CFAA of 1986, amended in 1994, 1996, in 2001 by the USA Patriot Act, and in 2008 by the Identity Theft Enforcement and Restitution Act.

The CFAA serves as the current foundation for criminalizing unauthorized access to computer systems.

CFAA makes it a crime to knowingly access a computer that is either considered a government computer or used in interstate commerce, or to use a computer in a crime that is interstate in nature.

Slide 6



Principles of Computer Security, Fifth Edition

CFFA

- Financial thresholds for defining a criminal act
 - Easily met.
- Crime to knowingly transmit a program, code, or command that results in damage.
- Crime to traffic in passwords or similar access information.
- Wide-sweeping act
 - Challenge of proving a case still exists.


Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The act sets financial thresholds for defining a criminal act, which were lowered by the Patriot Act, but in light of today's investigation costs, these are easily met.

The act also makes it a crime to knowingly transmit a program, code, or command that results in damage.

Trafficking in passwords or similar access information is also criminalized.

This is a wide-sweeping act, but the challenge of proving a case still exists.



Principles of Computer Security, Fifth Edition


USA Patriot Act

- 2001, passed in response to the September 11 terrorist attacks.
- Substantially changed the levels of checks and balances in laws related to privacy in the U.S.
- Extends the tap and trace provisions of existing wiretap statutes to the Internet and mandates certain technological modifications at ISPs to facilitate electronic wiretaps on the Internet and for ISPs to cooperate with the government to aid monitoring.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The USA Patriot Act of 2001, passed in response to the September 11 terrorist attacks substantially changed the levels of checks and balances in laws related to privacy in the United States.

This law extends the tap and trace provisions of existing wiretap statutes to the Internet and mandates certain technological modifications at ISPs to facilitate electronic wiretaps on the Internet and for ISPs to cooperate with the government to aid monitoring.



Principles of Computer Security, Fifth Edition

USA Patriot Act

- Permitted the Justice Department to proceed with its rollout of the Carnivore program, an eavesdropping program for the Internet.
- The name Carnivore has been retired, but the ability of the government to eavesdrop on and monitor communications remains.
- Permits federal law enforcement personnel to investigate computer trespass (intrusions) and enacts civil penalties for trespassers.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.


The act also permits the Justice Department to proceed with its rollout of the Carnivore program, an eavesdropping program for the Internet.

There was much controversy over the use of Carnivore, but the Patriot Act mandates that ISPs cooperate and facilitate monitoring.

The FBI renamed Carnivore DCS1000 and allegedly stopped using the system in 2001 in favor of commercially available software.

Similar projects include ECHELON, Room 641A and Total Information Awareness.

The Patriot Act also permits federal law enforcement personnel to investigate computer trespass and enacts civil penalties for trespassers.



Principles of Computer Security, Fifth Edition

Gramm-Leach-Bliley Act (GLBA)


- 1999.
- Major piece of legislation
- Affects the financial industry
 - includes significant privacy provisions for individuals.
- Key privacy tenet enacted in GLBA
 - establishment of an opt-out method for individuals to maintain some control over the use of the information provided in a business transaction with a member of the financial community.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The Gramm-Leach-Bliley Act was signed into law in 1999.

GLBA is a major piece of legislation affecting the financial industry that includes significant privacy provisions for individuals.

The key privacy tenets enacted in GLBA include the establishment of an opt-out method for individuals to maintain some control over the use of the information provided in a business transaction with a member of the financial community.



Principles of Computer Security, Fifth Edition

GLBA


- Enacted through a series of rules governed by state law, federal law, securities law, and federal rules.
 - Cover a wide range of financial institutions
- GLBA ended sharing to external third-party firms.
 - Some internal information sharing is required under the Fair Credit Reporting Act (FCRA) between affiliated companies

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

GLBA is enacted through a series of rules governed by state law, federal law, securities law, and federal rules.

These rules cover a wider range of financial institutions, from banks and thrifts, to insurance companies, to securities dealers.

Some internal information sharing is required under the Fair Credit Reporting Act (FCRA) between affiliated companies, but GLBA ended sharing to external third-party firms.



Principles of Computer Security, Fifth Edition


Sarbanes-Oxley Act (SOX)

- 2002.
- Overhauled the financial accounting standards for publicly traded firms in the United States.
- **Section 404** controls specify that all processes associated with the financial reporting of a firm must be controlled and audited on a regular basis.
 - Auditors in IT
 - Control-based framework to detect/prevent fraud
 - Detect insider activity/attacks
 - Compliance is expensive

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The Sarbanes-Oxley Act was passed into law in 2002. SOX overhauled the financial accounting standards for publicly traded firms in the United States. With respect to information security, one of the most prominent changes was the provision of Section 404 controls, which specify that all processes associated with the financial reporting of a firm must be controlled and audited on a regular basis. Since the majority of firms use computerized systems, this places internal auditors into the IT shops, verifying that the systems have adequate controls to ensure the integrity and accuracy of financial reporting.

These controls have resulted in controversy over the cost of maintaining them versus the risk of not using them. Section 404 requires firms to establish a control-based framework designed to detect or prevent fraud that would result in misstatement of financials. In simple terms, these controls should detect insider activity that would defraud the firm. This has significant impacts on the internal security controls, because a system administrator with root-level access could perform many if not all tasks associated with fraud and would have the ability to alter logs and cover their tracks. Likewise, certain levels of power users of financial accounting programs would also have significant capability to alter records.



Principles of Computer Security, Fifth Edition

Attribution

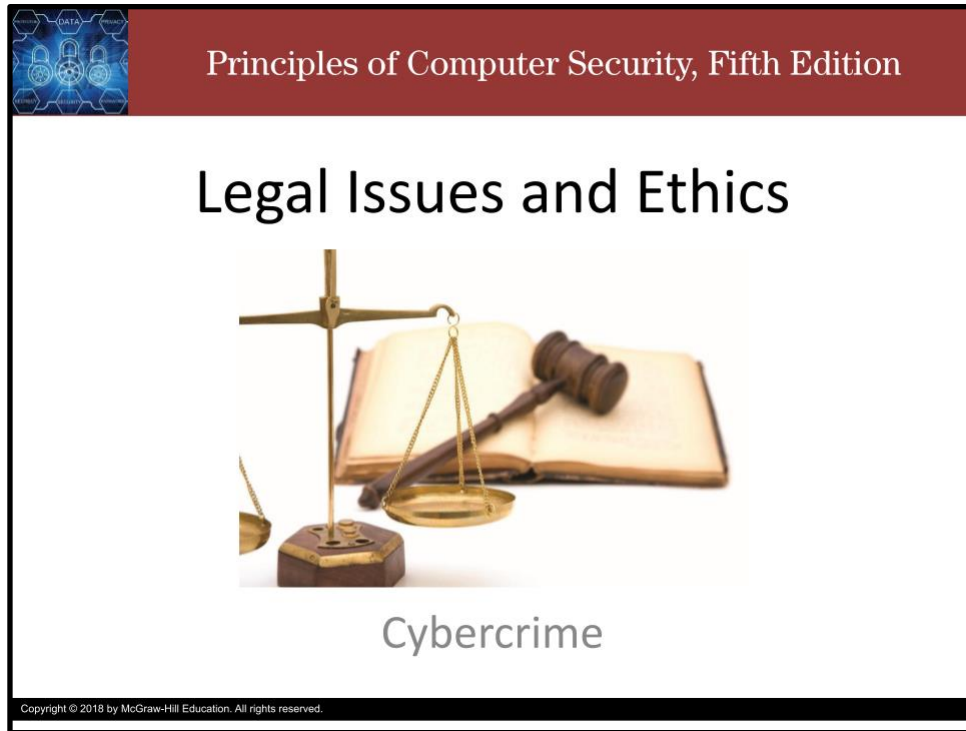
- The course slides are based on slides developed by the textbook authors, W. “Art” Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you and take care.

Legal Issues and Ethics: Cybercrime pt. 3


Slide 1



The image shows a book cover with a dark red header. The header contains the text "Principles of Computer Security, Fifth Edition" in white. Below the header, the title "Legal Issues and Ethics" is written in large black font. Underneath the title is a photograph of a brass scale of justice, an open book, and a wooden gavel. At the bottom of the cover, the word "Cybercrime" is written in a smaller black font. A small copyright notice is visible at the very bottom of the cover.

Principles of Computer Security, Fifth Edition


Legal Issues and Ethics



Cybercrime

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Howdy! In this video, we conclude our discussions of laws and standards related to cybercrime.



Principles of Computer Security, Fifth Edition

Payment Card Industry Data Security Standard (PCI DSS)

- **PCI DSS** is a set of contractual rules governing how credit card data is to be protected.
 - Current version is 3.2.1: released in May 2018
 - Voluntary, private sector initiative: proscriptive in its security guidance
 - Steep price for noncompliance

Copyright © 2018 by McGraw-Hill Education. All rights reserved.


The payment card industry, including the powerhouses of MasterCard and Visa, through its PCI Security Standards Council designed a private-sector initiative to protect payment card information between banks and merchants.

The Payment Card Industry Data Security Standard (PCI DSS) is a set of contractual rules governing how credit card data is to be protected.

The current version is 3.2.1, which was released in May 2018.

This is a voluntary, private sector initiative that is proscriptive in its security guidance.

Merchants and vendors can choose not to adopt these measures, but the standard has a steep price for noncompliance; the transaction fee for noncompliant vendors can be significantly higher, fines up to \$500,000 can be levied, and in extreme cases the ability to process credit cards can be revoked.



Principles of Computer Security, Fifth Edition

PCI DSS Requirements

1. Build and Maintain a Secure Network and Systems
 1. Install and maintain a firewall to protect cardholder data.
 2. Change vendor-supplied defaults for system passwords and other security parameters.
2. Protect Cardholder Data
 1. Protect stored cardholder data.
 2. Encrypt transmission of cardholder data over open, public networks.
3. Maintain a Vulnerability Management Program
 1. Protect all systems against malware and perform regular updates of anti-virus software.
 2. Develop and maintaining secure systems and applications.
4. Implement Strong Access Control Measures
 1. Restrict access to cardholder data to only authorized personnel.
 2. Identify and authenticate access to system components.
 3. Restrict physical access to cardholder data.
5. Regularly Monitor and Test Networks
 1. Track and monitor all access to cardholder data and network resources.
 2. Test security systems and processes regularly.
6. Maintain an Information Security Policy
 1. Maintain an information security policy for all personnel.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The PCI Data Security Standard specifies twelve requirements for compliance, organized into six logically related groups called "control objectives". The six groups are: build and Maintain a Secure Network and Systems, Protect Cardholder Data, Maintain a Vulnerability Management Program, Implement Strong, Access Control Measures, Regularly Monitor and Test Networks, Maintain an Information Security Policy.

The twelve requirements for building and maintaining a secure network and systems can be summarized as follows:

Install and maintain a firewall to protect cardholder data.

Change vendor-supplied defaults for system passwords and other security parameters.

Protect stored cardholder data.

Encrypt transmission of cardholder data over open, public networks.

Protect all systems against malware and perform regular updates of anti-virus software.

Develop and maintaining secure systems and applications.

Restrict access to cardholder data to only authorized personnel.


Identify and authenticate access to system components.

Restrict physical access to cardholder data.

Track and monitor all access to cardholder data and network resources.

Test security systems and processes regularly.

And Maintain an information security policy for all personnel.




Principles of Computer Security, Fifth Edition

PCI DSS Data Retention Guidelines

		Data Element	Storage Permitted	Render Stored Data Unreadable
Account Data	Cardholder Data	Primary Account Number	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Data	Yes	No
	Sensitive Authentication Data	Full Track Data	No	Cannot Store
		CAV2/CVC2/CVV2/CID	No	Cannot Store
		PIN/PIN Block	No	Cannot Store

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

PCI DSS has two defined types of information: cardholder data and sensitive authentication data. Cardholder data, such as the account number, name on the card, and the expiration date can be stored. The account number, if stored, must be stored in an unreadable format. Sensitive authentication data like the full magnetic track data and the cvv2 code cannot be stored.



Principles of Computer Security, Fifth Edition

Import/Export Encryption Restrictions

- Encryption tech is gov't controlled
 - Outright banned ,..., no regulation
 - Because... reasons (“it’s a weapon”, “this mail is my mail”)
 - Majority of laws are about encryption
 - Until recently: mainly used by the military
 - Now: Internet, eCommerce, and financial institutions are heaviest users
 - $\frac{d}{dt} \textit{Practice} > \frac{d}{dt} \textit{Law}$

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Encryption technology has been controlled by governments for a variety of reasons.

The level of control varies from outright banning to little or no regulation.

The reasons behind the control vary as well, and control over import and export is a vital method of maintaining a level of control over encryption technology in general.


The majority of the laws and restrictions are centered on the use of cryptography, which was until recently used mainly for military purposes.

The advent of commercial transactions and network communications over public networks such as the Internet has expanded the use of cryptographic methods to include securing of network communications.

As is the case in most rapidly changing technologies, the practice moves faster than law.

Many countries still have laws that are outmoded in terms of e-commerce and the Internet.

Slide 6



Principles of Computer Security, Fifth Edition

Import/Export Encryption Restrictions: US Law

- U.S. export controls on commercial encryption products are administered by the Bureau of Industry and Security (BIS).
 - Violation of encryption export regulations is a serious matter and is not an issue to take lightly.
 - Until recently, encryption protection was accorded the same level of attention as the export of weapons for war.
 - Remember: PGP and Phil Zimmerman.


Copyright © 2018 by McGraw-Hill Education. All rights reserved.

In the US, export controls on commercial encryption products are administered by the Bureau of Industry and Security (BIS) in the U.S. Department of Commerce.

Violation of encryption export regulations is a serious matter and is not an issue to take lightly.

Until recently, encryption protection was accorded the same level of attention as the export of weapons for war.

With the rise of the Internet, widespread personal computing, and the need for secure connections for e-commerce, this position has relaxed somewhat.



Principles of Computer Security, Fifth Edition

U.S. encryption export control policy

- 3 principles
 - Review of encryption products prior to sale,
 - Streamlined post-export reporting,
 - License review of certain exports of strong encryption to foreign government end users
- Lighter restriction for “mass-market” products
 - Available to the public by OTC, mail-order, electronic, or telephone call transactions
 - Crypto functionality cannot be changed by user
 - Designed for installation by user without further support
 - Details are accessible and provided on request for verification of

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The U.S. encryption export control policy continues to rest on three principles: review of encryption products prior to sale, streamlined post-export reporting, and license review of certain exports of strong encryption to foreign government end users.

The current set of U.S. rules requires notification to the BIS for export in all cases, but the restrictions are significantly lessened for mass-market products, as defined by all of the following:

They are generally available to the public by being sold, without restriction, from stock at retail selling points by any of these means of transaction:

Over-the-counter, Mail-order, Electronic, or Telephone call

The cryptographic functionality cannot easily be changed by the user.

They are designed for installation by the user without further substantial support by the supplier.

When necessary, details of the items are accessible and will be provided, upon request, to the appropriate authority in the exporter’s country in order to ascertain compliance with export regulations.

This is a very technical area, with significant rules and significant penalties for infractions.

The best rule is that whenever you are faced with a situation involving the export of encryption-containing software, first consult an expert and get the appropriate permission or a statement that permission is not required.

This is one case where it is better to be safe than sorry.



Principles of Computer Security, Fifth Edition

Import/Export Encryption Restrictions: Non-U.S. Laws

- Wassenaar Arrangement – international arrangement on export controls for conventional arms and dual-use goods and technologies.
- Some countries have more restrictive policies
 - Some countries may go more repressive
 - Others are being lobbied for less restrictive rules
- UK has a key disclosure law
 - As do many others
 - US has 5th amendment □ “LOLno.”

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Export control rules for encryption technologies fall under the Wassenaar Arrangement, an international arrangement on export controls for conventional arms and dual-use goods and technologies. “Dual-use” refers to technology that can be used for both peaceful and military aims. The Wassenaar Arrangement was established to contribute to regional and international security and stability by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilizing accumulations. Participating states, of which the United States is one of 42, will seek, through their own national policies and laws, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities that undermine these goals, and are not diverted to support such capabilities. Many nations have more restrictive policies than those agreed upon as part of the Wassenaar Arrangement. Australia, New Zealand, United States, France, and Russia go further than is required under Wassenaar and restrict general-purpose cryptographic software as dual-use goods through national laws. The Wassenaar Arrangement has had a significant impact on cryptography export controls, and there seems little doubt that some of the nations represented will seek to use the next round to move toward a more repressive cryptography export control regime based on their own national laws. There are ongoing campaigns to attempt to influence other members of the agreement toward less restrictive rules or, in some cases, no rules.

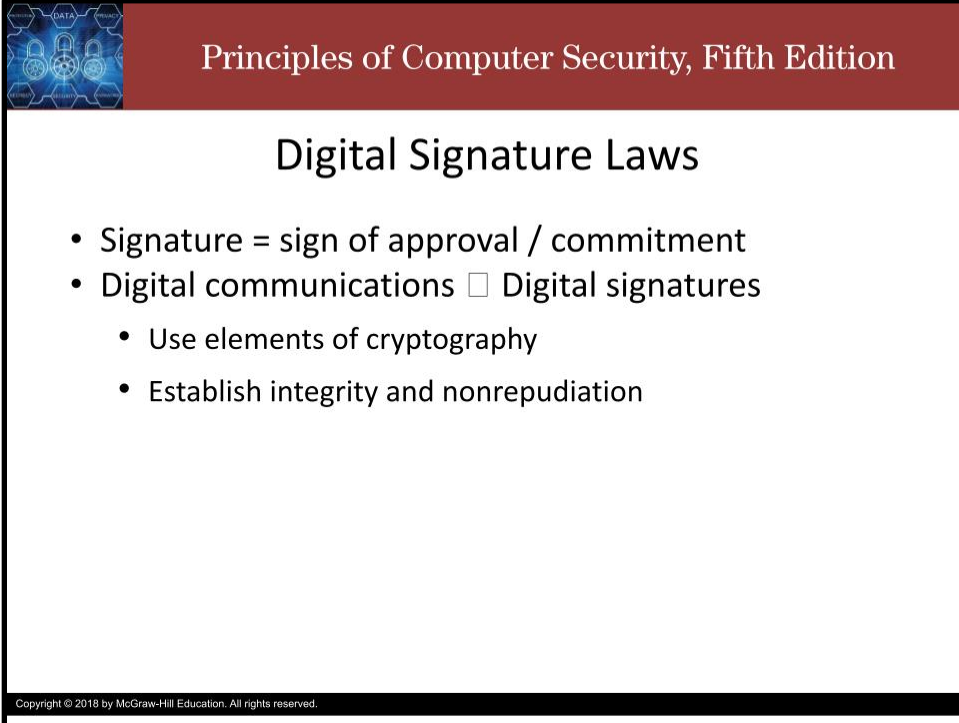
These lobbying efforts are based on e-commerce and privacy arguments., such as “key escrow will kill both eCommerce and privacy”.

In 2007, the United Kingdom passed a new law mandating that when requested by UK authorities, either police or military, encryption keys must be provided to permit decryption of information.

Failure to deliver either the keys or decrypted data can result in an automatic prison sentence of two to five years, which is often less than the penalty for possession of whatever might be encrypted so refusing to comply is the rational choice and thus the law is as ineffective as it is dangerous.

In the US, the 5th amendment protections mean that you do not have to decrypt anything or give anyone your decryption keys or password for any reason. If someone, especially an employer or government agency asks us for our password or decryption key, we ask them politely, yet firmly, to leave.

Slide 9




Principles of Computer Security, Fifth Edition

Digital Signature Laws

- Signature = sign of approval / commitment
- Digital communications □ Digital signatures
 - Use elements of cryptography
 - Establish integrity and nonrepudiation

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Whether a ring and wax seal, a stamp, or a scrawl indicating a name, signatures have been used to affix a sign of one’s approval for centuries. As communications have moved into the digital realm, signatures need to evolve with the new medium, and hence digital signatures were invented. Using elements of cryptography to establish integrity and nonrepudiation, digital signature schemes can actually offer more functionality than their predecessors in the paper-based world.



Principles of Computer Security, Fifth Edition

US Digital Signature Laws

- Electronic Signatures in Global and National Commerce Act (“E-Sign”), 2000.
 - See also: Uniform Electronic Transactions Act (UETA).
- Many states have adopted digital signature laws.
- Consumers assume a duty of care when they adopt the use of digital signatures for their transactions, not unlike the care required for PINs on debit cards.


Copyright © 2018 by McGraw-Hill Education. All rights reserved.

On October 1, 2000, the Electronic Signatures in Global and National Commerce Act (commonly called the E-Sign law) went into effect in the United States. This law implements a simple principle: a signature, contract, or other record may not be denied legal effect, validity, or enforceability solely because it is in electronic form. Another source of law on digital signatures is the Uniform Electronic Transactions Act (UETA), which was developed by the National Conference of Commissioners on Uniform State Laws (NCCUSL) and has been adopted in all but four states—Georgia, Illinois, New York, and Washington—which have adopted a non-uniform version of UETA. The precise relationship between the federal E-Sign law and UETA has yet to be resolved and will most likely be worked out through litigation in the courts over complex technical issues. Many states have adopted digital signature laws, the first being Utah in 1995. The Utah law, which has been used as a model by several other states, confirms the legal status of digital signatures as valid signatures, provides for use of state-licensed certification authorities, endorses the use of public key encryption technology, and authorizes online databases called repositories, where public keys would be available. The Utah act specifies a negligence standard regarding private encryption keys and places no limit on liability.

Thus, if a criminal uses a consumer’s private key to commit fraud, the consumer is financially responsible for that fraud, unless the consumer can prove that he or she used reasonable care in safeguarding the private key. Consumers assume a duty of care when they adopt the use of digital signatures for their transactions, not unlike the care required for PINs on debit cards. From a practical standpoint, the existence of the E-Sign law and UETA has enabled e-commerce transactions to proceed, and the resolution of the technical details via court actions will probably have little effect on consumers beyond

the need to exercise reasonable care over their signature keys. For the most part, software will handle these issues for the typical user.

Slide 11



The slide features a dark red header with the text "Principles of Computer Security, Fifth Edition" in white. To the left of the header is a small graphic with the word "DATA" and several padlock icons. The main content area is white with a black border. The title "UN Digital Signature Laws" is centered in black. Below the title is a bulleted list of four items. At the bottom left of the slide, there is a small copyright notice: "Copyright © 2018 by McGraw-Hill Education. All rights reserved."

Principles of Computer Security, Fifth Edition

UN Digital Signature Laws

- UN has a mandate to harmonize international trade.
- United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce, 1996
 - More work needed
- UNCITRAL Model Law on Electronic Signatures, 2001.
- Basis for many national and international efforts.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The United Nations has a mandate to further harmonize international trade. With this in mind, the UN General Assembly adopted in 1996 the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce. To implement specific technical aspects of this model law, more work on electronic signatures was needed. The General Assembly then adopted in 2001 the UNCITRAL Model Law on Electronic Signatures. These model laws have become the basis for many national and international efforts in this area.



Principles of Computer Security, Fifth Edition

Canadian Digital Signature Laws

- Early leader, 1998.
- Adopted a national model bill for electronic signatures to promote e-commerce.
 - Uniform Electronic Commerce Act (UECA)
 - Allows the use of electronic signatures in communications with the government.
- Individual Canadian provinces have passed similar legislation defining digital signature provisions for e-commerce and government use.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Canada was an early leader in the use of digital signatures. Singapore, Canada, and the U.S. state of Pennsylvania were the first governments to have digitally signed an interstate contract. This contract, digitally signed in 1998, concerned the establishment of a Global Learning Consortium between the three governments. Canada went on to adopt a national model bill for electronic signatures to promote e-commerce.

This bill, the Uniform Electronic Commerce Act (UECA), allows the use of electronic signatures in communications with the government. The law contains general provisions for the equivalence between traditional and electronic signatures and is modeled after the UNCITRAL Model Law on E-Commerce. The UECA is similar to Bill C-54, Personal Information Protection and Electronic Documents Act, in authorizing governments to use electronic technology to deliver services and communicate with citizens.

Individual Canadian provinces have passed similar legislation defining digital signature provisions for e-commerce and government use. These laws are modeled after the UNCITRAL Model Law on E-Commerce to enable widespread use of e-commerce transactions. These laws have also modified the methods of interactions between the citizens and the government, enabling electronic communication in addition to previous forms.



Principles of Computer Security, Fifth Edition


European Digital Signature Laws

- Ensuring Security and Trust in Electronic Communication—Towards a European Framework for Digital Signatures and Encryption.
 - Common framework at the EU level is urgently needed
 - To stimulate
 - the free circulation of digital signature related products and services within the Internal market
 - the development of new economic activities linked to electronic commerce
 - To facilitate the use of digital signatures across national borders
- Electronic Commerce Directive, 2000.
 - Led to uniform digital signature laws across the EU.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The European Commission adopted a Communication on Digital Signatures and Encryption: “Ensuring Security and Trust in Electronic Communication—Towards a European Framework for Digital Signatures and Encryption.” This communication states that a common framework at the EU level is urgently needed to stimulate “the free circulation of digital signature related products and services within the Internal market” and “the development of new economic activities linked to electronic commerce” as well as “to facilitate the use of digital signatures across national borders.” Community legislation should address common legal requirements for certificate authorities, legal recognition of digital signatures, and international cooperation. This communication was debated, and a common position was presented to the member nations for incorporation into national laws.

On May 4, 2000, the European Parliament and Council approved the common position adopted by the council. In June 2000, the final version, the Electronic Commerce Directive (2000/31/EC), was adopted. The directive has been implemented by member states. To implement the articles contained in the directive, member states had to remove barriers, such as legal form requirements, to electronic contracting, leading to uniform digital signature laws across the EU.



Principles of Computer Security, Fifth Edition


Digital Rights Management

- **Digital Millennium Copyright Act (DMCA)**
 - Primary statute enacted in the United States to bring copyright legal concerns up to date with the digital world.
 - The majority of this law was well crafted, but one section has drawn considerable comment and criticism.
 - A section that makes it illegal to develop, produce, and trade any device or mechanism designed to circumvent technological controls used in copy protection
 - Cryptography. DMCA tried to kill cryptography research.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The ability to make flawless copies of digital media has led to another “new” legal issue. For years, the music and video industry has relied on technology to protect its rights with respect to intellectual property. It has been illegal for decades to copy information, such as music and videos, protected by copyright. Even with the law, people have for years made copies of music and videos to share, violating the law. Until the advent of digital copies, this did not represent a significant economic impact in the eyes of the industry, as the copies were of lesser quality and people would pay for original quality in sufficient numbers to keep the economics of the industry healthy. As such, legal action against piracy was typically limited to large-scale duplication and sale efforts, commonly performed overseas and subsequently shipped to the United States as counterfeit items.

The primary statute enacted in the United States to bring copyright legal concerns up to date with the digital world is the Digital Millennium Copyright Act (DMCA). The DMCA states its purpose as follows: “To amend title 17, United States Code, to implement the World Intellectual Property Organization Copyright Treaty and Performances and Phonograms Treaty, and for other purposes.” The majority of this law was well crafted, but one section has drawn considerable comment and criticism. A section of the law makes it illegal to develop, produce, and trade any device or mechanism designed to circumvent technological controls used in copy protection. This is obviously a ridiculous requirement as it has the ability to limit research on cryptography and the strengths and weaknesses of specific methods. The RIAA, paragons of virtue that they are, sued a Princeton research team for trying to publish a paper detailing weaknesses in DMCA copy-protection mechanisms that were discovered during an industry-sponsored challenge to break the methods. Unfortunately, the RIAA dropped the case before case law could be made to prevent future bullying from the industry.



Principles of Computer Security, Fifth Edition

Digital Rights Management

- DMCA takedown notices.
 - Carriers are granted protection from content violation,
 - provided they remove the content when requested with a takedown order.
 - Scanners and automated systems issue takedown notices
 - sometimes go awry.
 - Fair use is not well-delineated
 - system sides with the takedown requestor by default.
- DMCA's (and DRM in general) effect on software/IT is unclear

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Another controversial issue associated with DMCA is the issue of takedown notices.

Carriers, like YouTube, are granted protection from content violation, provided they remove the content when requested with a takedown order.

Certain organizations use scanners and automated systems to issue takedown notices with the effect of stealing content from the legitimate creator (which is, ironically, something DMCA is supposed to protect against).

Apparently, this happens to NASA's YouTube channel often. News organizations use NASA's content, then issue automated takedown notices to NASA for alleged copyright infringement on the content they borrowed (and now are effectively trying to steal) from NASA.


The issue of fair use is one that is not delineated by bright-line regulations, making the system one that sides with the takedown requestor unless the content poster takes them to court.

I am sure that, if you are a regular user of YouTube, you are well-familiar with the absolute dumpster fire that is YouTube's handling of these kinds of automated copyright strikes. If one didn't know better, the drama-worthiness of the stories is almost enough to make you think they do it on purpose for content.

Exemptions are scattered throughout the DMCA, although many were created during various deliberations on the act and do not make sense when the act is viewed in whole. The effect of these exemptions upon people in the software and technology industry is not clear, and until restrained by case law, the DMCA gives large firms with deep legal pockets a potent weapon to use against parties who disclose flaws in encryption technologies used in various products. Actions have already been

initiated against individuals and organizations who have reported security holes in products. This will be an active area of legal contention, as the real issues behind digital rights management have yet to be truly resolved.


Slide 16



Principles of Computer Security, Fifth Edition

Attribution

- The course slides are based on slides developed by the textbook authors, W. "Art" Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.



[NEFFEX OP](#)

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you and take care.