


## Privacy: Anonymity and Pseudonymity

Slide 1

Principles of Computer Security, Fifth Edition

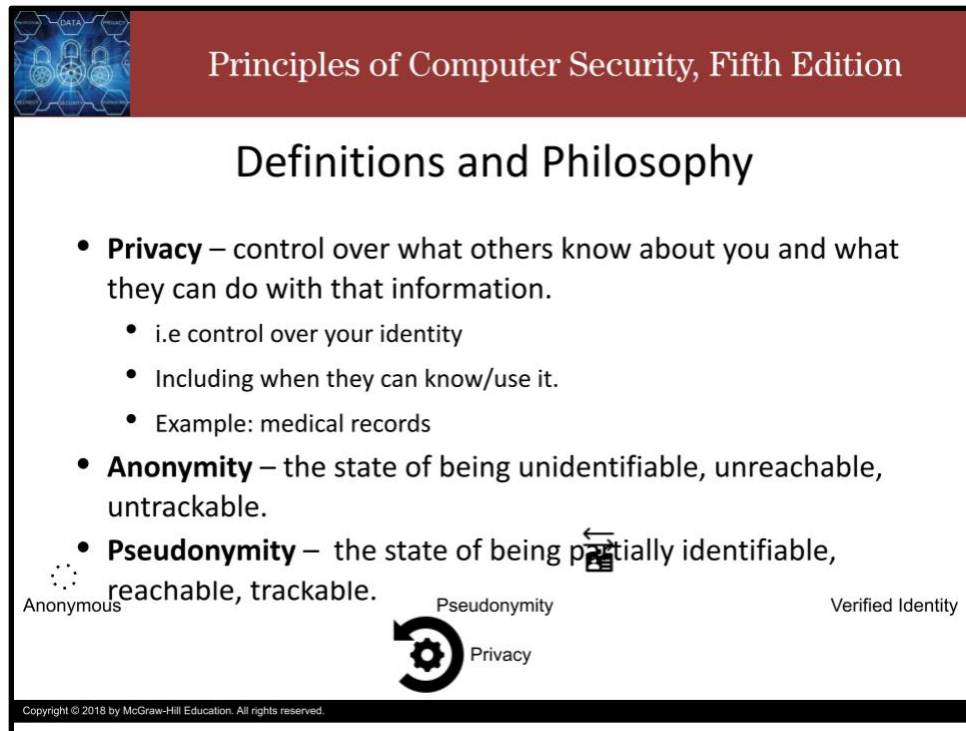
# Privacy



Anonymity and Pseudonymity

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


Howdy! In this video, we discuss anonymity and pseudonymity.



**Principles of Computer Security, Fifth Edition**

## Definitions and Philosophy

- **Privacy** – control over what others know about you and what they can do with that information.
  - i.e control over your identity
  - Including when they can know/use it.
  - Example: medical records
- **Anonymity** – the state of being unidentifiable, unreachable, untrackable.
- **Pseudonymity** – the state of being partially identifiable, reachable, trackable.



The diagram illustrates a spectrum of identity and privacy. On the left is 'Anonymous' (represented by a dotted circle), in the middle is 'Privacy' (represented by a gear icon), to its right is 'Pseudonymity' (represented by a gear icon with a red arrow pointing left), and on the far right is 'Verified Identity' (represented by a solid circle). A red arrow points from 'Pseudonymity' towards 'Privacy'.

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

**Privacy** can be defined as the power to control what others know about you and what they can do with that information. In other words, having privacy means having control over your identity. That control includes the ability to control when others have access to the information. For example, a medical doctor might have read and append-only access to your medical records only during your appointment.

**Anonymity** is more than just being nameless. The crux of anonymity is that a person is unidentifiable, unreachable, or untrackable. Anonymity means that your identity is unknown. Your actions cannot be attributed to you, neither can they even be attributed confidently to the same entity. The notion of “you” does not meaningfully exist for others.

**Pseudonymity** is like anonymity, except that your actions can be attributed to the same person, but that person cannot necessarily be identified as you. To me, identifiability is a spectrum, from anonymous on one end, where one’s identity is completely unknown and cannot be known, to the other end where one’s identity is known and verified. Privacy is a control that moves a person along the identifiability spectrum. But it’s not that more privacy means more anonymity. For me, as I see privacy as control, more privacy means more accuracy and precision of controlling one’s location on the identifiability spectrum. Also, one’s location on the spectrum may be different from the perspective of different others and different sets of information items. So... identity and privacy are complicated and complex. In the computer age, personal information forms the basis for many decisions, from credit cards purchases to travel. Although it is possible to live a life of near complete anonymity, the cost is one which most people are unwilling to pay. Most people live comfortably in various forms of pseudonymity.

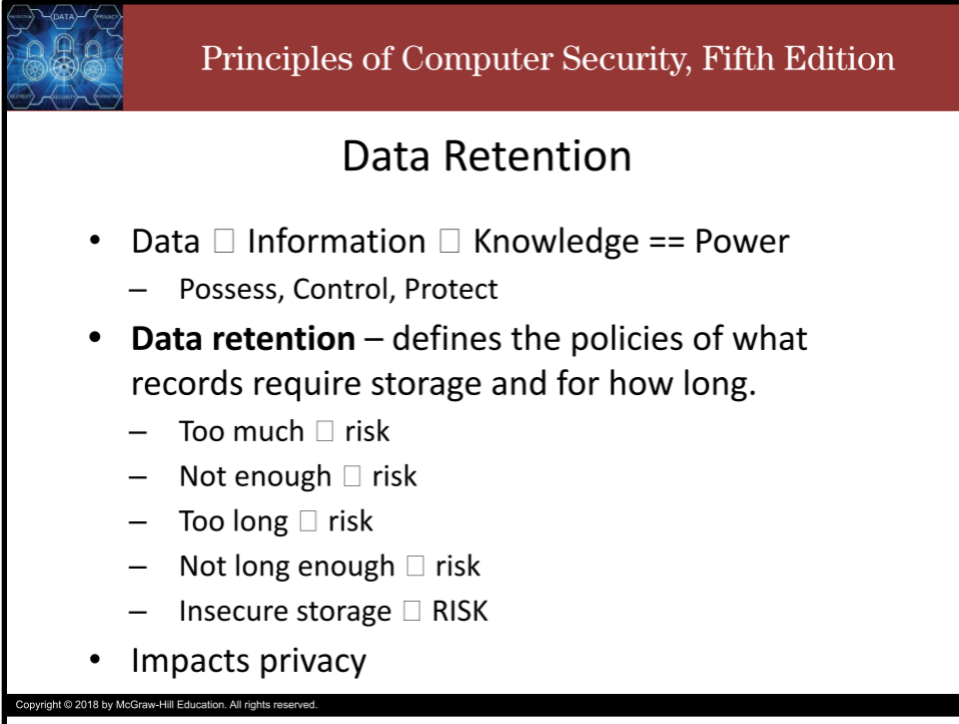
On the other end, can you ever really know someone? I wonder if it's even possible to for anyone, even one's own self to achieve a level of complete knowledge about one's identity and personal information. The issue of privacy, to me, is not one of where we should be on the spectrum, but how much knowledge and control we should have over all dimensions of our location on it.

Wallace, Kathleen A (1999). "Anonymity". *Ethics and Information Technology*. 1: 23–35.  
doi:10.1023/A:1010066509278.;

Nissenbaum, Helen (1999). "The Meaning of Anonymity in an Information Age". *The Information Society*. 15 (2): 141–44. doi:10.1080/019722499128592.;

Matthews, Steve (2010). "Anonymity and the Social Self". *American Philosophical Quarterly*. 47: 351–63.

### Slide 3



**Principles of Computer Security, Fifth Edition**

## Data Retention

- Data □ Information □ Knowledge == Power
  - Possess, Control, Protect
- **Data retention** – defines the policies of what records require storage and for how long.
  - Too much □ risk
  - Not enough □ risk
  - Too long □ risk
  - Not long enough □ risk
  - Insecure storage □ RISK
- Impacts privacy

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

Information is important in today's society. After all, knowledge is power. The reliance on information imbues information with value, creating the desire to possess and control it, which demands the ability to protect it, **Data retention** is the determination of what records require storage and for how long. It is actually a somewhat thin line to walk, as storing too much or too little data are risks. So, too, are maintaining data stores for longer than is required and not storing the information long enough.

Failure to maintain the data in a secure state is also a retention issue.

In some cases, destruction of data, specifically data subject to legal hold in a legal matter, can result in adverse court findings and sanctions.

This makes determining, labeling, and maintaining data associated with legal hold an added dimension for normal storage times.

Data retention impacts privacy. In order to have control over who knows what and when, we must be able to control who can store what and for how long. Without such control, we can never move left on the identifiability spectrum, towards anonymity, as once we share any information, we can never unshare it. If your momma ain't told you before, I'mma tell you now: anything you post on the Internet, or send to someone else digitally, lives forever. It never goes away. This great truth implies also that only data that you need later will become unavailable or lost. So, backup your data. Securely. Which includes meaningful privacy controls over who can access it and when.

Slide 4







**Principles**

- 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.

<https://xkcd.com/1269/>

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

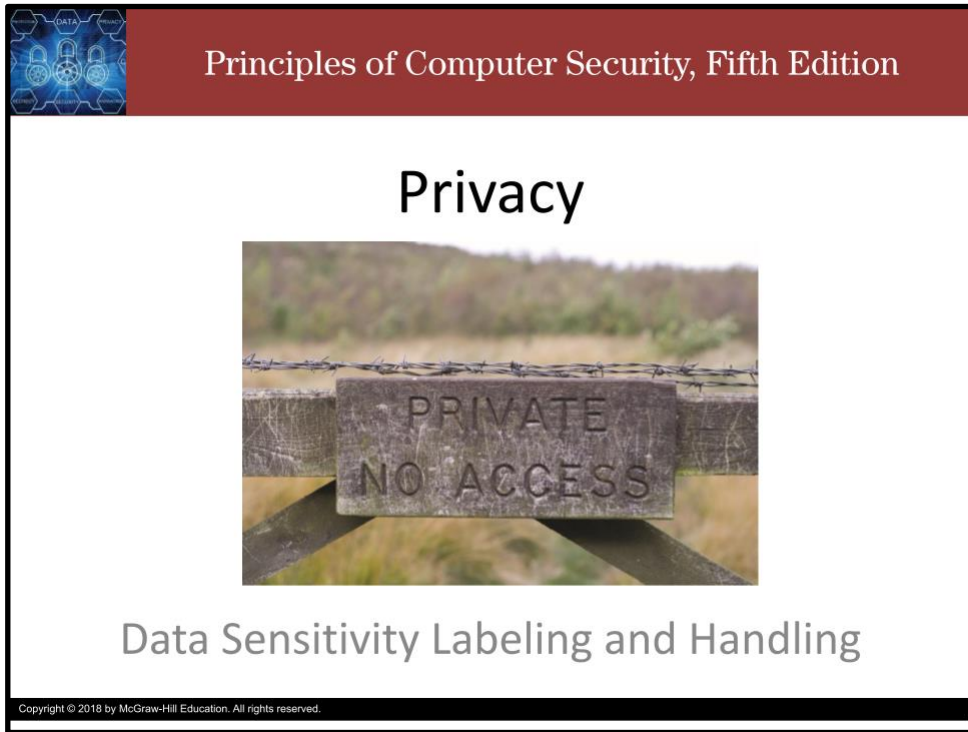
### OPINIONS ON INTERNET PRIVACY

<p><b>THE PHILOSOPHER:</b></p> <p>"PRIVACY" IS AN IMPRACTICAL WAY TO THINK ABOUT DATA IN A DIGITAL WORLD SO UNLIKE THE ONE IN WHICH OUR SOCIETY LIVES.</p> <p style="text-align: center; font-weight: bold; font-size: 1.2em;">SO BORED.</p> 	<p><b>THE CRYPTO NUT:</b></p> <p>MY DATA IS SAFE BEHIND SIX LAYERS OF SYMMETRIC AND PUBLIC-KEY ALGORITHMS.</p> <p style="text-align: center;">WHAT DATA IS IT?</p> <p>MOSTLY ME EMAILING WITH PEOPLE ABOUT CRYPTOGRAPHY.</p> 	<p><b>THE CONSPIRACIST:</b></p> <p>THESE LEAKS ARE JUST THE TIP OF THE ICEBERG. THERE'S A WAREHOUSE IN UTAH WHERE THE NSA HAS THE ENTIRE ICEBERG.</p> <p style="text-align: center;">I DON'T KNOW HOW THEY GOT IT THERE.</p> 
<p><b>THE NIHILIST:</b></p> <p>JOKES ON THEM, GATHERING ALL THIS DATA ON ME AS IF ANYTHING I DO MEANS ANYTHING.</p> 	<p><b>THE EXHIBITIONIST:</b></p> <p>MIMM? I SURE HOPE THE NSA ISN'T WATCHING ME BITE INTO THESE JUICY STRAWBERRIES!!</p> <p>OOFS I DRIPPED SOME ON MY SHIRT! BETTER TAKE IT OFF.</p> <p>GOOGLE, ARE YOU THERE? GOOGLE, THIS LOTION FEELS SOOOO GOOD.</p> <p style="text-align: center;">UM.</p> 	<p><b>THE SAGE:</b></p> <p>I DON'T KNOW OR CARE WHAT DATA ANYONE HAS ABOUT ME.</p> <p style="text-align: center;">DATA IS IMAGINARY. THIS BURRITO IS REAL.</p> 

Thank you and take care.


## Privacy: Data Sensitivity Labeling and Handling

Slide 1



Principles of Computer Security, Fifth Edition


# Privacy



Data Sensitivity Labeling and Handling

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

Howdy! In this video, we discuss data sensitivity labeling and handling.




Principles of Computer Security, Fifth Edition

## Data Sensitivity Labeling and Handling

- **Data sensitivity labeling** necessary for effective data classification programs
  - Lets people know how to handle the data
  - Training is important
- Protection of information is key to IT security.
- Organizations need to recognize that not all information is of equal importance or sensitivity.
  - Define classification levels that dictate handling
  - Factors: value, age, laws

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

Effective data classification programs include data sensitivity labeling, which enables personnel handling the data to know whether it is sensitive and to understand the level of protection required. Training to ensure that labeling occurs and that it is used and followed is important for users whose roles can be impacted by this material. Properly trained personnel act as security controls. Untrained or improperly trained personnel increase the risk of compromise. A key component of IT security is the protection of the information processed and stored on the computer systems and network. Organizations deal with many different types of information and they need to recognize that not all information is of equal importance or sensitivity. Information should be categorized by the level of protection required or the level of access permitted. Factors that affect this classification include value to the organization, age, and relevant laws and regulations.




Principles of Computer Security, Fifth Edition

## Data Sensitivity Labeling and Handling

- The most widely known system of classification of information is implemented by the U.S. government
  - Top Secret, Secret, Confidential, Unclassified.
- Businesses use categories such as Publicly Releasable, Proprietary, Company Confidential, and For Internal Use Only.
- Policy should describe: how to protect, who can access, who can disclose and how, how to destroy
  - All employees should be trained to apply the policy

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

The most widely known system of classification of information is that implemented by the U.S. government and military, which classifies information as top secret, secret, confidential, or unclassified. Businesses also need to keep data secure and often use categories such as Publicly Releasable, Proprietary, Company Confidential, and For Internal Use Only. Each policy for the classification of information should describe how it should be protected, who may have access to it, who has the authority to release it and how, and how it should be destroyed. All employees of the organization should be trained in the procedures for handling the information that they are authorized to access.



Principles of Computer Security, Fifth Edition

## Basic Labels

- **Confidential** – would cause harm if released
  - Define by policy
- **Private** – do not share
  - Need-to-know basis only
- **Proprietary** – shareable with 3<sup>rd</sup> party partner, but no further
  - Proprietary for me, private for you
- **Public** – no confidentiality protection necessary
  - Still requires integrity protection

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

**Confidential** data is data that is defined to represent a harm to the enterprise if it is released to unauthorized parties.

This data should be defined by policy, and that policy should include details on who has the authority to release the data.


**Private** data is data marked to alert people that it is not to be shared with other parties, typically because they have no need to see it.

**Proprietary** data may be shared with a third party that is not a competitor, but in marking the data, you alert the sharing party that the data is not to be shared further.

**Public** data is data that can be seen by the public and has no needed protections with respect to confidentiality.

It is important to protect the integrity of public data, lest one communicate incorrect data as being true.





## Principles of Computer Security, Fifth Edition

### Attribution

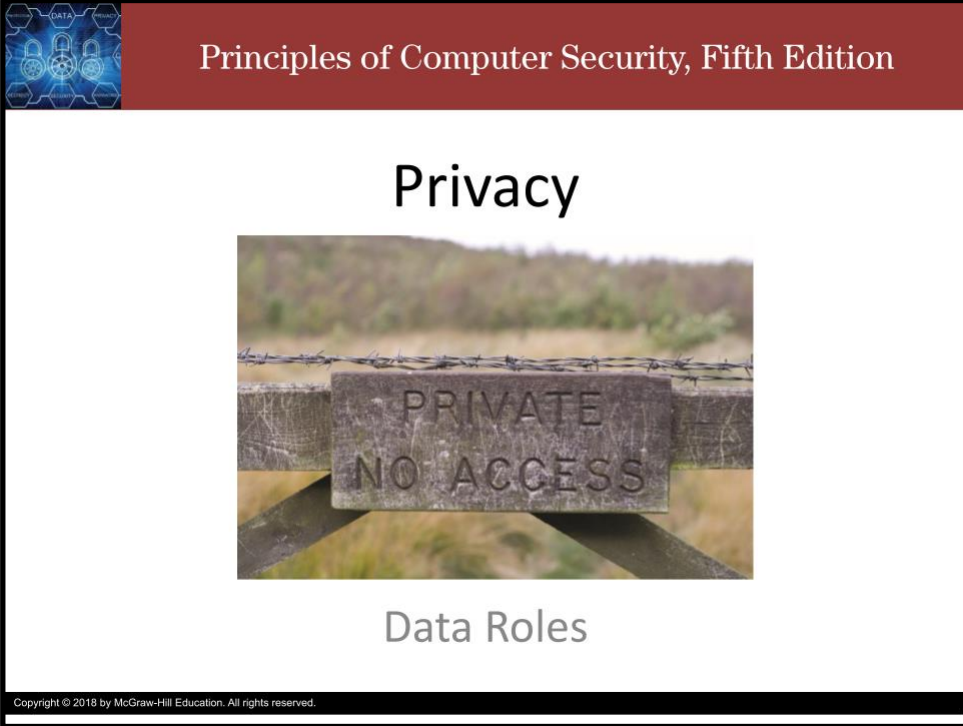
- The course slides are based on slides developed by the textbook authors, W. “Art” Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.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

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

Thank you and take care.


## Privacy: Data Roles

Slide 1



The slide features a dark red header with the text "Principles of Computer Security, Fifth Edition" in white. On the left side of the header is a small blue icon depicting a network of nodes and locks. The main content area is white and contains the word "Privacy" in a large, black, sans-serif font. Below this is a photograph of a concrete barrier with a sign that reads "PRIVATE NO ACCESS" in raised letters. The barrier is topped with a strand of barbed wire. Below the photograph, the words "Data Roles" are written in a smaller, grey, sans-serif font. At the bottom left of the slide, there is a small copyright notice: "Copyright © 2018 by McGraw-Hill Education. All rights reserved."

Howdy! In this video, we introduce personnel roles associated with the control and administration of data.



Principles of Computer Security, Fifth Edition


## Data Roles

- Data owner
  - Required for all data
  - Defines handling requirements
- Data custodian/steward
  - Responsible for day-to-day caretaking
  - Enforces policies set by data owner
- Privacy officer
  - C-level executive responsible for privacy
  - Likes data minimization
  - Important role for dealing with data on EU citizens

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

Multiple personnel are associated with the control and administration of data, **Data roles** include data owners, stewards, custodians, and users. Data requires a **data owner**. Data ownership roles for all data elements need to be defined in the business. Data ownership is a business function, where the requirements for security, privacy, retention, and other business functions must be established. Different data has different handling requirements, but those requirements must be defined. The data owner is responsible for defining those requirements, **Data custodians** or **stewards** are the parties responsible for the day-to-day caretaking of data. The data owner sets the relevant policies, and the steward or custodian ensure these policies are followed.

The **privacy officer** is the C-level executive who is responsible for privacy issues in the firm. One of the key initiatives run by privacy officers is the drive for data minimization. Privacy officer plays an important role if information on European customers is involved.



## Principles of Computer Security, Fifth Edition

### Attribution

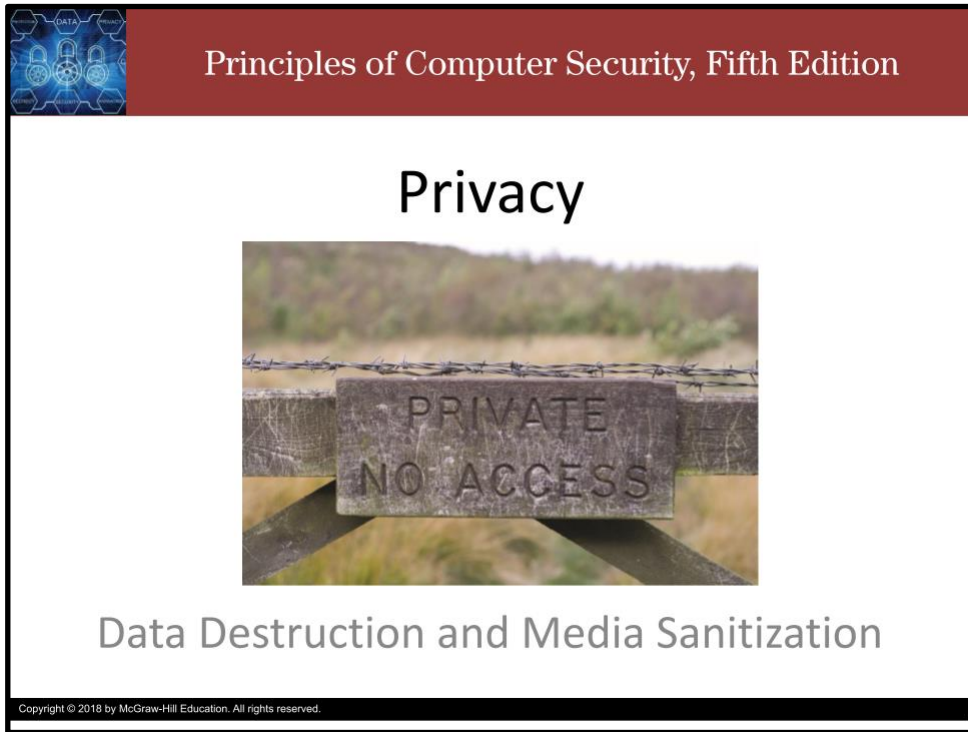
- The course slides are based on slides developed by the textbook authors, W. "Art" Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.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

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

Thank you and take care.


## Privacy: Data Destruction and Media Sanitization

Slide 1



Principles of Computer Security, Fifth Edition

# Privacy

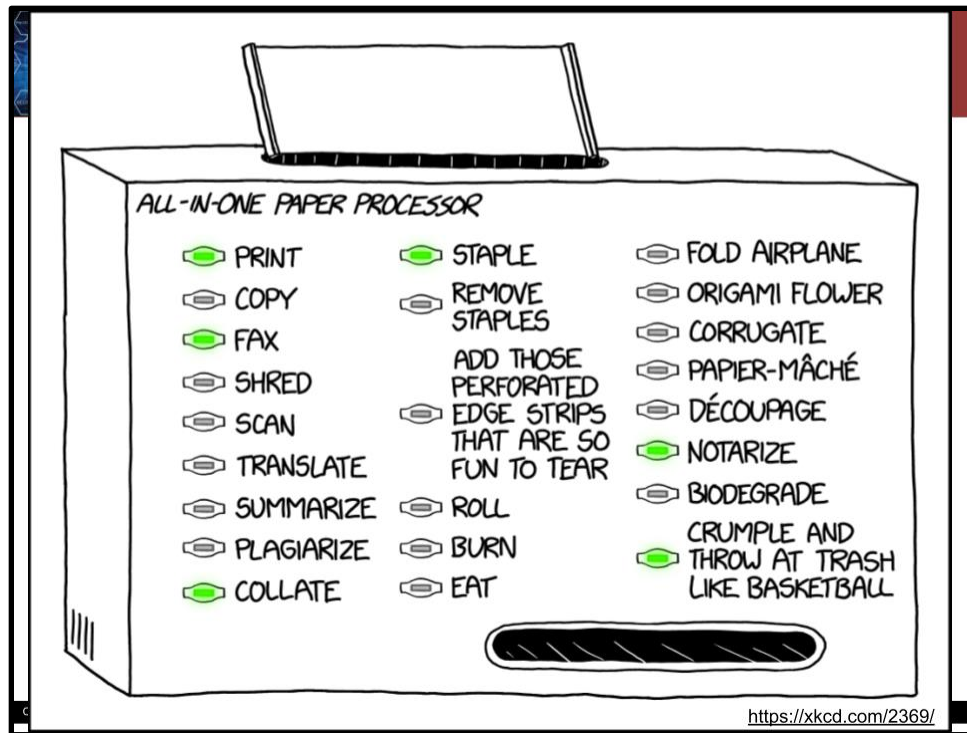


Data Destruction and Media Sanitization


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

Howdy! In this video, we discuss data destruction and media sanitization.

Slide 2



When data is no longer being used, whether it be on old printouts, old systems being discarded, or broken equipment, it is important to destroy the data before losing physical control over the media it is on. It is critical for every organization to have a strong disposal and destruction policy and related procedures.




Principles of Computer Security, Fifth Edition

## Data Destruction and Media Sanitization

- Burning
  - A gold-standard methods of data destruction.
  - Once the storage media is rendered into a form that can be destroyed by fire, the chemical processes of fire are irreversible and render the data lost forever.
- Shredding
  - Physical destruction by tearing an item into many small pieces, which can then be mixed, making reassembly difficult if not impossible.
  - Important papers should be shredded.

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

Burning is a gold-standard method of data destruction. Once the storage media is rendered into a form that can be destroyed by fire, the chemical processes of fire are irreversible and render the data lost forever. Shredding is the physical destruction by tearing an item into many small pieces, which can then be mixed, making reassembly difficult if not impossible. Important papers should be shredded, at a minimum, if not burned or pulped.



Principles of Computer Security, Fifth Edition

## Data Destruction and Media Sanitization (3 of 5)


- [Pulping](#)
  - Process by which paper fibers are suspended in a liquid and recombined into new paper.
- [Pulverizing](#)
  - Process of destruction using excessive physical force to break an item into unusable pieces.

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

Pulping is a process by which paper fibers are suspended in a liquid and recombined into new paper. Anything printed on the paper is dissolved in the process and, like burning, the process is irreversible.

Pulverizing is a process of destruction using excessive physical force to break an item into unusable pieces.





Principles of Computer Security, Fifth Edition

## Data Destruction and Media Sanitization

- [Degaussing](#)
  - (for magnetic HDDs) Realigns the magnetic particles, removing the organized structure that represented the data.
- [Wiping](#)
  - Overwriting the storage media with garbage data
  - More times  more security
  - Solid-state drives require special utilities to ensure that all the sectors are wiped.

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


Degaussing is a method of destroying data on magnetic storage media. Degaussing realigns the magnetic particles, removing the organized structure that represented the data.

Wiping data is the process of rewriting the storage media with a series of patterns of 1's and 0's.

This is not done once, but is done multiple times to ensure that every trace of the original data has been eliminated.

There are data-wiping protocols for various security levels of data, with just a few passes, up to many tens of passes to destroy every last trace of old data.

For solid-state drives, a special utility is required to ensure that all the sectors are wiped. Additionally, wiping a solid state drive wears out the drive much more quickly than normal use.



Principles of Computer Security, Fifth Edition

## Attribution

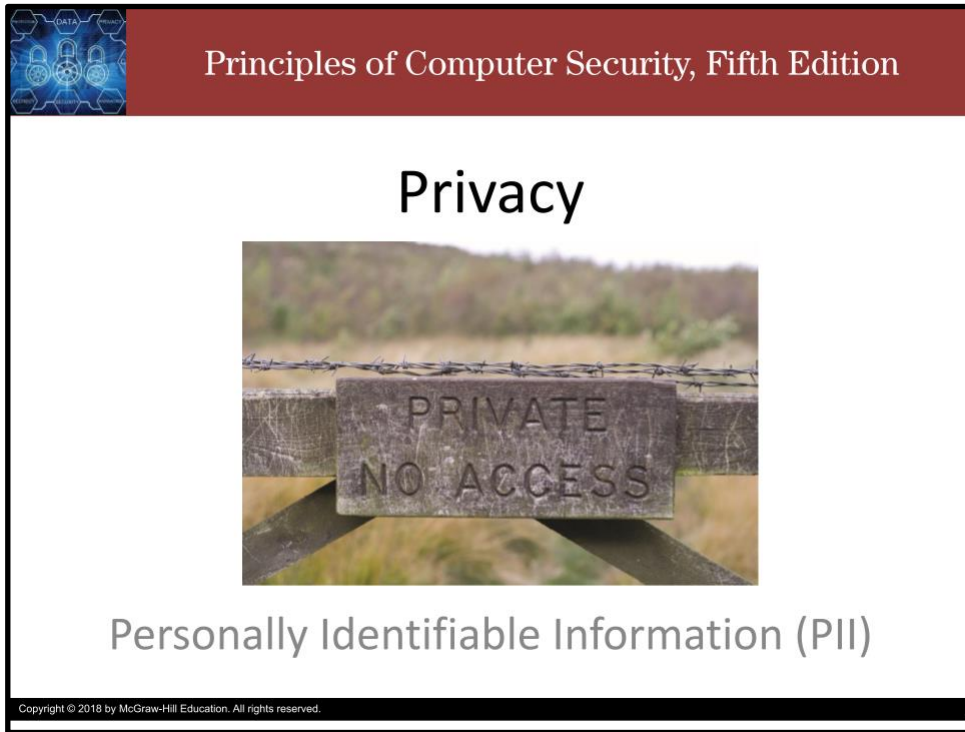
- The course slides are based on slides developed by the textbook authors, W. “Art” Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.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

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

Thank you and take care


## Privacy: Personally Identifiable Information (PII)

Slide 1



Principles of Computer Security, Fifth Edition


# Privacy



Personally Identifiable Information (PII)

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

Howdy! In this video, we discuss personally identifiable information.




## Principles of Computer Security, Fifth Edition

### Personally Identifiable Information (PII)

- A set of elements that can lead to the specific identity of a person
- Can be used to identify a specific individual
  - Even if an entire set is not disclosed.
- An essential element of many online transactions
  - Can be misused if disclosed to unauthorized parties.
- Should be protected at all times
  - by all parties that possess it.
- Used to identify which data elements require a specific level of protection.
  - Businesses must protect PII from cradle to grave

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

Personally identifiable information (PII) is anything, from a single element of data to a set of data, that can lead to the specific identity of a person. By definition, PII can be used to identify a specific individual, even if an entire set is not disclosed. PII is an essential element of many online transactions, but it can also be misused if disclosed to unauthorized parties. Therefore, PII should be protected at all times, by all parties that possess it. The concept of PII is used to identify which data elements require a specific level of protection. The U.S. Federal Trade Commission has repeatedly ruled that if a firm collects PII, it is responsible for it through the entire lifecycle, from initial collection through use, retirement, and destruction. Only after the PII is destroyed in all forms and locations is the company's liability for its compromise abated.



Principles of Computer Security, Fifth Edition


## Sensitive PII

- Requires special handling
  - Collection, storage, destruction
- Examples: credit, bank account, SSN, DL, etc.
- Compromise  direct financial damage
- If disclosure could cause harm,
  - Then treat as sensitive PII

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

Some PII is so sensitive to disclosure and resulting misuse that it requires special handling to ensure protection. Data elements such as credit card data, bank account numbers, and government identifiers (social security number, driver's license number, and so on) require extra levels of protection to prevent harm from misuse. Should these elements be lost or compromised, direct, personal financial damage may occur to the person identified by the data.

These elements need special attention when planning data stores and executing business processes associated with PII data, including collection, storage, and destruction. If the accidental disclosure of user data could cause the user harm, such as discrimination (political, racial, health related, or lifestyle), then the best course of action is to treat the information as sensitive PII.



Principles of Computer Security, Fifth Edition


## Notice, Choice, and Consent

- **Notice** – Informing the customer that PII will be collected and used and/or stored.
- **Choice** – The opportunity for the end user to consent to the data collection or to opt out.
- **Consent** – Positive affirmation by a customer that they read the notice, understands their choices, and agrees to release their PII for the purposes explained to them.

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

Three words can govern good citizenry when collecting PII: Notice, Choice, and Consent. Notice means informing the customer, in a clear and comprehensible way, what PII will be collected and how it will be used and stored.

Choice means then end user has the opportunity to consent to the data collection or to opt out, and that that choice will be respected. Consent is a positive affirmation by a customer that they read the notice, understands their choices, and agrees to release their PII for the purposes explained to them. Yes means yes, everything else means no (including not making a choice since, if you choose not to decide, you still have made a choice).



## Principles of Computer Security, Fifth Edition

### Attribution

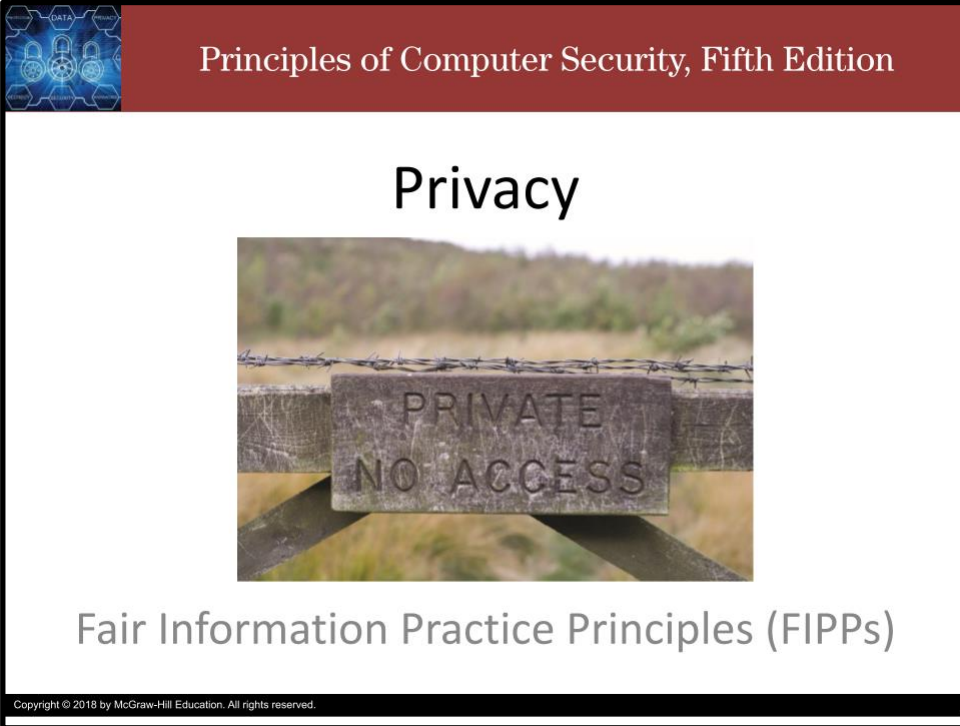
- The course slides are based on slides developed by the textbook authors, W. "Art" Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.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

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

Thank you and take care


## Privacy: Fair Information Practice Principles

Slide 1



Principles of Computer Security, Fifth Edition

# Privacy




Fair Information Practice Principles (FIPPs)

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

Howdy! In this video, we introduce the Fair Information Practice Principles.





Principles of Computer Security, Fifth Edition

## Fair Information Practice Principles (FIPPs)

- FTC uses FIPPs, laid out in [OMB Circular A-130](#)
- **Access and Amendment**
- **Accountability**
- **Authority**
- **Minimization**
- **Quality and Integrity**
- **Individual Participation**
- **Purpose Specification and Use Limitation**
- **Security**
- **Transparency**

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

In the United States, the Federal Trade Commission has a significant role in addressing privacy concerns. The core principles the FTC uses are referred to as the **Fair Information Practice Principles (FIPPs)**. The FIPPs and their components are detailed in OMB Circular A-130.

**Access and Amendment** – Agencies should provide individuals with appropriate access to their own PII and appropriate opportunity to correct or amend their own PII.

**Accountability** – Agencies should be accountable for complying with these principles and applicable privacy requirements.

**Authority** – Agencies should only see or touch PII if they have the authority to do so.

**Minimization** – Agencies should only see or touch PII that is directly relevant and necessary to accomplish a legally authorized purpose and should only maintain such PII for as long as necessary to accomplish said purpose.

**Quality and Integrity** – Agencies should see and touch PII with whatever quality and integrity is reasonably necessary to ensure fairness to the individual.


**Individual Participation** – Agencies should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for seeing or touching PII.

**Purpose Specification and Use Limitation** – Agencies should provide notice of the specific purpose for which PII is collected and should only see or touch it for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected.

**Security** – Agencies should establish administrative, technical, and physical safeguards to protect PII commensurate with the risk of harm caused by its unauthorized access, use, modification, loss, destruction, or disclosure.

**Transparency** – Agencies should be transparent about information policies and practices with respect to PII.

## Slide 3



### Principles of Computer Security, Fifth Edition

## Attribution

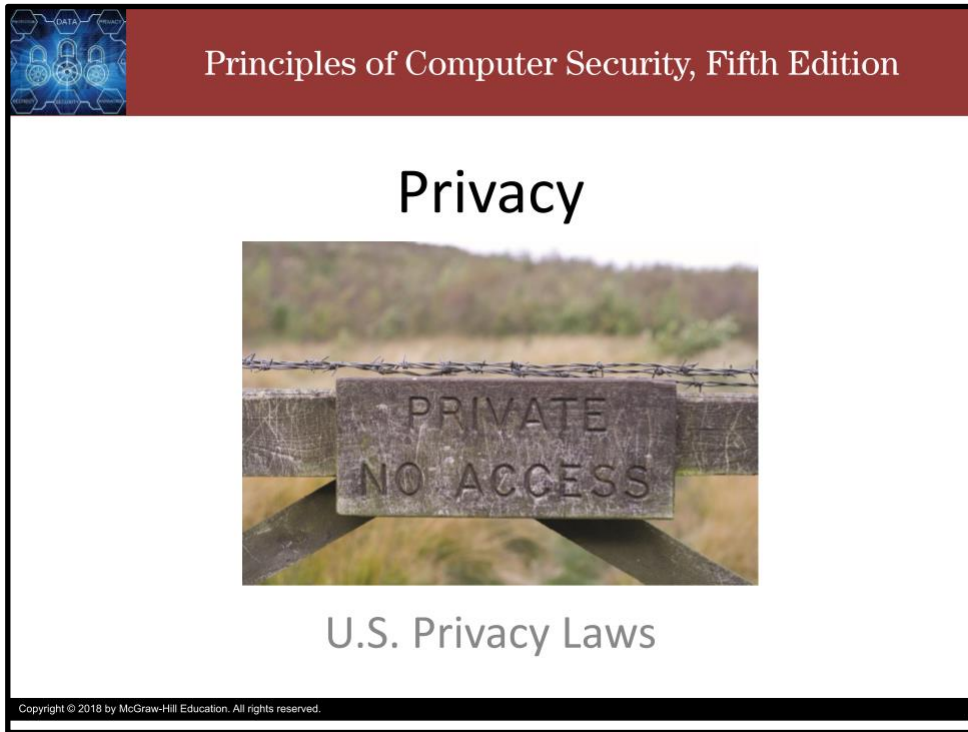
- The course slides are based on slides developed by the textbook authors, W. “Art” Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.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

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

Thank you and take care


## Privacy: U.S. Privacy Laws

Slide 1



Principles of Computer Security, Fifth Edition


# Privacy



U.S. Privacy Laws

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

Howdy! In this video, we discuss some privacy laws in the U.S.




Principles of Computer Security, Fifth Edition

## U.S. Privacy Laws

- Identity privacy and the establishment of identity theft crimes are governed by the Identity Theft and Assumption Deterrence Act of 1998.
  - It is a violation of federal law to knowingly use another's identity.
- The collection of information necessary to do this is also governed by the Gramm-Leach-Bliley Act (GLBA).
  - It is illegal for someone to gather identity information on another person under false pretenses.

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

Identity privacy and the establishment of identity theft crimes are governed by the Identity Theft and Assumption Deterrence Act of 1998, under which it is a violation of federal law to knowingly use another's identity. The collection of information necessary to do this is also governed by the Gramm-Leach-Bliley Act (GLBA) which make is it illegal for someone to gather identity information on another person under false pretenses.




## Principles of Computer Security, Fifth Edition

### U.S. Privacy Laws

- Identity Theft and Assumption Deterrence Act
- Privacy Act of 1974
- Freedom of Information Act (FOIA)
- Family Education Records and Privacy Act (FERPA)
- U.S. Computer Fraud and Abuse Act (CFAA)
- U.S. Children's Online Privacy Protection Act (COPPA)
- Video Privacy Protection Act (VPPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- California Senate Bill 1386 (SB 1386)
- U.S. Banking Rules and Regulations

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

There are many laws in the US that deal with privacy. The ones mentioned in this video are some of the most notable.




Principles of Computer Security, Fifth Edition

## Privacy Act of 1974

- The **Privacy Act of 1974** was an omnibus act designed to affect the entire federal information landscape.
  - This act has many provisions that apply across the entire federal government, with only minor exceptions for national security (classified information), law enforcement, and investigative provisions.

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

The **Privacy Act of 1974** was an omnibus act designed to affect the entire federal information landscape. This act has many provisions that apply across the entire federal government, with only minor exceptions for national security, law enforcement, and investigative provisions.




Principles of Computer Security, Fifth Edition

## Freedom of Information Act (FOIA)

- The **Freedom of Information Act (FOIA)** of 1996 is one of the most widely used privacy acts in the United States.
  - FOIA was designed to enable public access to U.S. government records.
    - “Public” includes the press.
  - FOIA carries a presumption of disclosure.
    - The burden is on the government, not the requesting party, to substantiate why information cannot be released.

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

The Freedom of Information Act (FOIA, “foya”) of 1996 is one of the most widely used privacy acts in the United States. FOIA was designed to enable public access to U.S. government records, where “Public” includes the press. FOIA carries a presumption of disclosure, which means the burden is on the government, not the requesting party, to substantiate why information cannot be released.



Principles of Computer Security, Fifth Edition

## FOIA

- Agencies of the U.S. government are required to disclose those records, unless they can be lawfully withheld from disclosure under one of nine specific exemptions in FOIA.
- Record availability under FOIA is less of an issue than is the backlog of requests.
- Agencies are allowed to charge for research time and duplication costs.

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

Upon receiving a written request, agencies of the U.S. government are required to disclose those records, unless they can be lawfully withheld from disclosure under one of nine specific exemptions in FOIA, which includes things like national security, confidential business information, unwarranted violations of privacy, and geological and geophysical information concerning wells.

The right of access is ultimately enforceable through the federal court system.

Record availability under FOIA is less of an issue than is the backlog of requests.

To defray some of the costs associated with record requests, and to prevent numerous trivial requests, agencies are allowed to charge for research time and duplication costs.

These costs vary by agency, but are typically nominal, in the range of \$8.00 to \$45.00 per hour for search/review fees and \$.10 to \$.35 per page for duplication.

Agencies are not allowed to demand a requester to make an advance payment unless the agency estimates that the fee is likely to exceed \$250 or the requester previously failed to pay proper fees.

For many uses, the first 100 pages are free, and under some circumstances the fees can be waived.

-----

The nine specific exemptions, listed in Section 552 of U.S. Code Title 5, fall within the following general categories:

1. National security and foreign policy information
2. Internal personnel rules and practices of an agency
3. Information specifically exempted by statute
4. Confidential business information



5. Inter- or intra-agency communication that is subject to deliberative process, litigation, and other privileges
6. Information that, if disclosed, would constitute a clearly unwarranted invasion of personal privacy
7. Law enforcement records that implicate one of a set of enumerated concerns
8. Agency information from financial institutions
9. Geological and geophysical information concerning wells

## Slide 7

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 of a blue padlock surrounded by icons representing data, security, and technology. The main content area is white with a black border. The title "Family Education Records and Privacy Act (FERPA)" is centered in a large, bold, black font. Below the title is a bulleted list of three points. 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

### Family Education Records and Privacy Act (FERPA)

- Student records have significant protections under the FERPA of 1974.
  - FERPA places significant restrictions on information sharing.
  - FERPA operates on an opt-in basis, as the student must approve the disclosure of information prior to the actual disclosure.
  - When a student turns 18 years old or enters a postsecondary institution at any age, these rights under FERPA transfer from the student's parents to the student.

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

Student records have significant protections under the Family Education Records and Privacy Act of 1974 (FERPA), which was designed to protect privacy of student information and which places significant restrictions on information sharing.

FERPA operates on an opt-in basis, as the student must approve the disclosure of information prior to the actual disclosure.

The law allows students to have access to their education records, an opportunity to seek to have the records amended, and some control over the disclosure of information from the records to third parties. For example, if the parent of a student who is 18 or older inquires about the student's schedule, grades, or other academic issues, the student has to give permission before the school can communicate with the parent, even if the parent is paying for the education.

At the K–12 school level, students are typically too young to have legal standing associated with exercising their rights, so FERPA recognizes the parents as part of the protected party. FERPA provides parents with the right to inspect and review their children's education records, the right to seek to amend information in the records they believe to be inaccurate, misleading, or an invasion of privacy,

and the right to consent to the disclosure of PII from their children's education records. When a student turns 18 years old or enters a postsecondary institution at any age, these rights under FERPA transfer from the student's parents to the student.

## Slide 8

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 blue graphic with the word "DATA" and various icons. The main content area is white with a black border. It contains the title "U.S. Computer Fraud and Abuse Act (CFAA)" and a bulleted list of three points. At the bottom left, there is a small copyright notice: "Copyright © 2018 by McGraw-Hill Education. All rights reserved."


Principles of Computer Security, Fifth Edition

### U.S. Computer Fraud and Abuse Act (CFAA)

- A major objective of CFAA is to prevent unauthorized parties access to information to which they should not have access.
- Fraudulent access, or even exceeding one's authorized access, is defined as a crime and can be punished.
- This act can be used protect privacy related to computer records through its enforcement of violations of authorized access.

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

The U.S. Computer Fraud and Abuse Act has several specific objectives, but one of the main ones is to prevent unauthorized parties access to information they should not have access to. Fraudulent access, or even exceeding one's authorized access, is defined as a crime and can be punished. This act can be used protect privacy related to computer records through its enforcement of violations of authorized access.




Principles of Computer Security, Fifth Edition

## U.S. Children's Online Privacy Protection Act (COPPA)

- Children lack the mental capacity to make responsible decisions concerning the release of PII.
- Before information can be collected and used from children (ages 13 and under), parental permission needs to be obtained.
- COPPA requires that sites obtain parental permission, post a privacy policy detailing specifics concerning information collected from children, and describe how the children's information will be used.

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

Most people, but especially children, lack the mental capacity to make responsible decisions concerning the release of PII. The U.S. Children's Online Privacy Protection Act of 1998 (COPPA) specifically addresses this privacy issue with respect to children accessing and potentially releasing information on the Internet. Any web site that collects information from children aged 13 and under is covered by this law. Before information can be collected and used from children aged 13 and under, parental permission needs to be obtained. COPPA requires that sites obtain parental permission, post a privacy policy detailing specifics concerning information collected from children, and describe how the children's information will be used.



Principles of Computer Security, Fifth Edition

## Video Privacy Protection Act (VPPA)


- Considered by many privacy advocates to be the strongest U.S. privacy law.
- Provides civil remedies against unauthorized disclosure of personal information concerning video tape rentals and, by extension, DVDs and games as well.
  - Protections by default
- Exemptions exist; Does not supersede state laws
  - Some states go harder/further

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

The VPPA of 1998 is considered by many privacy advocates to be the strongest U.S. privacy law. It provides civil remedies against unauthorized disclosure of personal information concerning video tape rentals and, by extension, DVDs and games as well. The statute provides the protections by default, thus requiring a video rental company to obtain the renter's consent to opt out of the protections if the company wants to disclose personal information about rentals.

Exemptions exist for issues associated with the normal course of business for the video rental company as well as for responding to warrants, subpoenas, and other legal requests. This law does not supersede state laws, of which there are several.

Many states have enacted laws providing both wider and greater protections than the federal VPPA statute. For example, Connecticut and Maryland laws brand video rental records as confidential, and therefore not subject to sale, while California, Delaware, Iowa, Louisiana, New York, and Rhode Island have adopted state statutes providing protection of privacy with respect to video rental records. Michigan's video privacy law specifically protects records of book purchases, rentals, and borrowing as well as video rentals.



Principles of Computer Security, Fifth Edition


## Health Insurance Portability & Accountability Act (HIPAA)

- Medical and health information also has privacy implications
- Includes significant restrictions on data transfers, security standards, electronic signature provisions
- Mandate compliance
  - Technical solutions left to industry
- PHI and NPP
- Covered entities: medical, billing, and insurance
  - HITECH Act: also health information exchanges and other “business associates” engaged in the collection and use of PHI

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

Medical and health information also has privacy implications, which is why the U.S. Congress enacted the **HIPAA** of 1996. From a privacy perspective, significant restrictions of data transfers to ensure privacy are included in HIPAA, including security standards and electronic signature provisions. HIPAA security standards mandate safeguards for physical storage, maintenance, transmission, and access to individuals' health information and that organizations that use electronic signatures have to meet standards ensuring information integrity, signer authentication, and nonrepudiation. These standards leave to industry the task of specifying the technical solutions and mandate compliance only to significant levels of protection. HIPAA's language is built upon the concepts of Protected Health Information (PHI) and **Notice of Privacy Practices (NPP)**. HIPAA describes “covered entities” including medical facilities, billing facilities, and insurance (third party payer) facilities.

In 2009, as part of the American Recovery and Reinvestment Act of 2009, the Health Information Technology for Economic and Clinical Health Act (HITECH Act) was passed into law. Although the primary purpose of the HITECH Act was to provide stimulus money for the adoption of electronic medical records (EMR) systems at all levels of the healthcare system, it also contained new security and privacy provisions to add teeth to those already in HIPAA. HIPAA protections were confined to the direct medical profession, and did not cover entities such as health information exchanges and other “business associates” engaged in the collection and use of PHI. Under HITECH, business associates will be required to implement the same security safeguards and restrictions on uses and disclosures, to protect individually identifiable health information, as covered entities under HIPAA. It also subjects business associates to the same potential civil and criminal liability for breaches as covered entities. HITECH also specifies that U.S. Department of Health & Human Services (HHS) is now required to conduct periodic audits of covered entities and business associates.




Principles of Computer Security, Fifth Edition

## Gramm-Leach-Bliley Act (GLBA)

- Introduced US Consumer to privacy notices
  - Disclose what, how, and with whom information is collected and shared
  - Required annually and must allow opt-out
    - You get them from your bank(s) and credit card companies
- Made it illegal to gather identity information on another person under false pretenses.

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

In the financial arena, GLBA introduced the U.S. consumer to privacy notices by requiring firms to disclose what they collect, how they protect the information, and with whom they will share it. Annual notices are required as well as the option for consumers to opt out of the data sharing, which is the primary concept behind U.S. privacy laws in the financial arena. Most U.S. consumers have witnessed the results of GLBA, every year receiving privacy notices from their banks and credit card companies. These notices are one of the visible effects of GLBA on changing the role of privacy associated with financial information.




Principles of Computer Security, Fifth Edition

## California Senate Bill 1386 (SB 1386)

- SB 1386 is a landmark law concerning information disclosures.
- It mandates that Californians be notified whenever PII is lost or disclosed.
  - Since the passage of SB 1386, numerous other states have modeled legislation on this bill.
  - The current list of U.S. states and territories that require disclosure notices is up to 49, with only Alabama, New Mexico, and South Dakota without bills.

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

SB 1386 is a landmark law concerning information disclosures which mandates that Californians be notified whenever PII is lost or disclosed. Since the passage of SB 1386 in 2002, numerous other states have modeled legislation on this bill. The current list of U.S. states and territories that require disclosure notices is up to 49, with only Alabama, New Mexico, and South Dakota without such bills. Each of these disclosure notice laws is different, making the case for a unifying federal statute compelling, but it is probably low on the priority lists of most politicians.



Principles of Computer Security, Fifth Edition

## U.S. Banking Rules and Regulations


- It was industry practice to write additional information on a check to assist a firm in later tracking down the drafting party.
  - E.g. address, work phone number, a credit card number, and so on.
  - Co-location of information about an individual used for **identity theft**.
  - Banking and financial regulations were issued to prohibit this form of information collection.
- Another example: limit printed CC #s to last 4 digits

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

At one time, it was standard practice to write additional information on a check to assist a firm in later tracking down the drafting party. This information included items such as address, work phone number, a credit card number, and so on. This led to the co-location of information about an individual, and this information was used at times to perpetrate the crime of **identity theft**. To combat this and prevent the gathering of this type of information, a series of banking and financial regulations were issued to prohibit this form of information collection.

Other regulations addressed items such as credit card numbers being printed on receipts, mandating only the last four digits be exposed.






Principles of Computer Security, Fifth Edition

## Payment Card Industry Data Security Standard (PCI DSS)

- This standard provides guidance on what elements of a credit card transaction need protection and the level of expected protection.
- PCI DSS is not a law.
  - It is a contractual regulation, enforced through a series of fines and fees associated with performing business in this space.
- PCI DSS was a reaction to two phenomena, data disclosures and identity theft.

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

The Payment Card Industry Data Security Standard provides guidance on what elements of a credit card transaction need protection and the level of expected protection. PCI DSS is not a law. It is a contractual regulation, enforced through a series of fines and fees associated with performing business in this space. PCI DSS was a reaction to the prevalence of data disclosures and identity thefts.




Principles of Computer Security, Fifth Edition

## Fair Credit Reporting Act (FCRA)

- This act requires that the agencies provide consumers notice of their rights and responsibilities.
- The agencies are required to perform timely investigations on inaccuracies reported by consumers.
- The act also has technical issues associated with data integrity, data destruction, data retention, and consumer and third-party access to data.

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

The Fair Credit Reporting Act (FCRA) requires that the agencies provide consumers notice of their rights and responsibilities. The agencies are required to perform timely investigations on inaccuracies reported by consumers. The agencies are also required to notify the other CRAs when consumers close accounts. The act also has technical issues associated with data integrity, data destruction, data retention, and consumer and third-party access to data.



Principles of Computer Security, Fifth Edition


## Fair and Accurate Credit Transactions Act (FACTA)

- The FACTA of 2003 was passed to enact stronger protections for consumer information from identity theft, errors, and omissions.
- FACTA amended portions of FCRA to:
  - Improve the accuracy of customer records in consumer reporting agencies
  - Improve timely resolution of consumer complaints concerning inaccuracies
  - Make businesses take reasonable steps to protect information that can lead to identity theft

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

The details of FCRA proved to be insufficient with respect to several aspects of identity theft, and in 2003, the Fair and Accurate Credit Transactions Act was passed, modifying and expanding on the privacy and security provisions of FCRA.

FACTA improved the accuracy of customer records in consumer reporting agencies and timely resolution of consumer complaints concerning inaccuracies, as well as made businesses take reasonable steps to protect information which could lead to identity theft if disclosed.



Principles of Computer Security, Fifth Edition


## FACTA

- FACTA includes other “**disposal rules**” associated with consumer information.
- FACTA mandates that information that is no longer needed must be properly disposed of, either by burning, pulverizing, or shredding.
- Any electronic information must be irreversibly destroyed or erased.
- Should third-party firms be used for disposal, the rules still pertain to the original contracting party.
  - Third parties should be selected with care and monitored for compliance.

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

FACTA also includes “**disposal rules**” associated with consumer information, mandating that information that is no longer needed must be properly disposed of, either by burning, pulverizing, or shredding.

Any electronic information must be irreversibly destroyed or erased. Should third-party firms be used for disposal, the rules hold the original contracting party responsible. Thus, third parties should be selected with care and monitored for compliance.



## 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.

## Privacy: International Privacy Laws

Slide 1



Principles of Computer Security, Fifth Edition

# Privacy



International Privacy Laws

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

Howdy! In this video, we discuss some international privacy laws.



## Principles of Computer Security, Fifth Edition


### International Privacy Laws

- Privacy is a universal but diverse concern
- Legal protections follow socio-cultural norms
  - US: opt-in; EU: opt-opt
  - Canada closer to Europe than US
- Organization for Economic Co-operation and Development (OECD)
  - Founded in 1961 to stimulate economic progress and world trade
  - Members committed to democracy and the market economy
  - Platform to compare policy experiences, seek answers to common problems, identify good practices and coordinate domestic and international policies of its members
    - Including **privacy**

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

Privacy is not a U.S.-centric phenomenon, but it does have strong cultural biases. Legal protections for privacy tend to follow the socio-cultural norms by geography. There are different policies in European nations than in the United States. In the United States, the primary path to privacy is via opt-out, whereas in Europe and other countries, it is via opt-in. In the U.S., a consumer must notify a firm that they wish to block the sharing of personal information. Otherwise, the firm has permission by default. In the EU, sharing is blocked unless the customer specifically opts in to allow it.

Even in countries with common borders, distinct differences exist, such as the United States and Canada; Canadian laws and customs have strong roots to their UK history, and in many cases follow European ideals as opposed to U.S. ones. One of the primary sources of intellectual and political thought on privacy has been the Organization for Economic Co-operation and Development (OECD). This multinational entity has for decades conducted multilateral discussions and policy formation on a wide range of topics, including privacy.



Principles of Computer Security, Fifth Edition

## OECD Fair Information Practices


- Foundational element for many worldwide privacy practices.
- 1980s
- Set of principles and practices
  - set out how to approach information handling, storage, management, and flows while maintaining fairness, **privacy**, and security.
- OECD Privacy Guidelines
  - <https://www.oecd.org/digital/ieconomy/privacy-guidelines.htm>

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

Members of the OECD recognized that information was a critical resource in a rapidly evolving global technology environment, and that proper handling of this resource was critical for long-term sustainability of growth. So, they developed Guidelines which would help to harmonize national privacy legislation.

The OECD Fair Information Practices are a foundational element for many worldwide privacy practices. From the 1980s, this is a set of principles and practices that set out how an information-based society may approach information handling, storage, management, and flows with a view toward maintaining fairness, privacy, and security.





Principles of Computer Security, Fifth Edition

## European Laws

- Data Protection statutes all personal data
  - Administered by state and national data protection agencies in each country.
- Different from privacy laws in the US (patchwork)
- Privacy is a fundamental human right
- Data Protection Directive
  - allows the EC to block transfers of personal data to any country outside the EU that has been determined to lack adequate data protection policies.

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


The EU has developed a comprehensive concept of privacy, which is administered via a set of statutes known as data protection. These privacy statutes cover all personal data, whether collected and used by government or by private firms. These laws are administered by state and national data protection agencies in each country. With the advent of the EU, this common comprehensiveness stands in distinct contrast to the patchwork of laws in the United States.

Privacy laws in Europe are built around the concept that privacy is a fundamental human right that demands protection through government administration. When the EU was formed, many laws were harmonized across the original 15 member nations, and data privacy was among those standardized.

One important aspect of this harmonization is the Data Protection Directive, adopted by EU members. A provision within this directive allows the European Commission to block transfers of personal data to any country outside the EU that has been determined to lack adequate data protection policies.

The impetus for the EU directive is to establish the regulatory framework to enable the movement of personal data from one country to another, while at the same time ensuring that privacy protection is “adequate” in the country to which the data is sent.

If the recipient country has not established a minimum standard of data protection, it is expected that the transfer of data will be prohibited.



Principles of Computer Security, Fifth Edition

## US Data Protection Considered Harmful

- Pre-2000: EU considers US privacy law too weak
- 2000: U.S.-EU Safe Harbor Framework patches the problem
- 2013: Snowden
- 2015: Safe Harbor not good enough
- 2016: EU-U.S. Privacy Shield Framework replaces Safe Harbor and patches the problems
- 2020: Privacy Shield not good enough
- ????: patch TBD...
  - In the meantime, use SCCs – treat EU data subjects protection as if the data was within the EU (and all those protections)

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

U.S. organizations that voluntarily joined an arrangement known as Safe Harbor and abided by the privacy principles set out therein would be considered adequate in terms of data protection. A business joining the Safe Harbor Consortium made commitments to abide by specific guidelines concerning privacy and also agreed to be governed by certain self-enforced regulatory mechanisms, backed ultimately by FTC action.

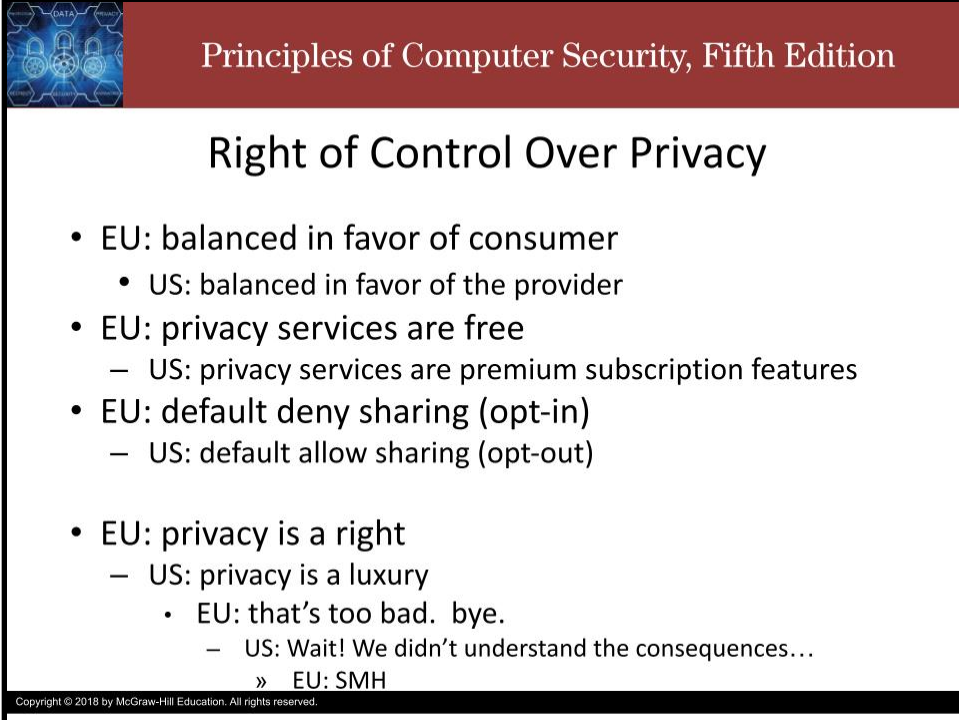
The Safe Harbor principles were quite similar to the FTC's Fair Information Practice Principles. But, their protections and enforcement were ultimately inadequate. On October 6, 2015, the European Court of Justice issued a judgment declaring invalid the European Commission's July 26, 2000 decision on the legal adequacy of the U.S.-EU Safe Harbor Framework. On July 12, 2016, the European Commission issued an adequacy decision on the EU-U.S. Privacy Shield Framework. This new Framework, which replaces the Safe Harbor program, provides a legal mechanism for companies to transfer personal data from the EU to the United States. The FTC will enforce the Privacy Shield Framework and continues to expect companies to comply with their ongoing obligations with respect to data previously transferred under the Safe Harbor Framework. In the end, it turned out the Privacy Shield was also inadequate.

On July 16, 2020, the European Court of Justice issued a judgment declaring invalid the European Commission's Decision 2016/1250/EC of July 12, 2016 on the adequacy of the EU-U.S. Privacy Shield Framework. The FTC continues to expect companies to comply with their ongoing obligations with respect to transfers made under the Privacy Shield Framework and also encourages companies to continue to follow robust privacy principles, such as those underlying the Privacy Shield Framework, and to review their privacy policies to ensure they describe their privacy practices accurately, including with regard to international data transfers.

The CJEU held that transfers to non-EU countries must afford EU data subjects a level of protection essentially equivalent to that guaranteed within the EU. The court found that the European Commission's standard contractual clauses ("SCCs") meet this standard, even though they do not bind the authorities of the non-EU country. However, the CJEU invalidated the EU-U.S. Privacy Shield on the ground that the United States failed to ensure equivalent protections. In particular, the court considered that certain U.S. government surveillance programs fail to limit themselves to what is strictly necessary or grant EU data subjects actionable rights.

Following the CJEU's judgment, the Privacy Shield is no longer a basis for EU-U.S. transfers. The CJEU's judgment is effective immediately, and there is no grace period. The European Commission has announced that it is already speaking with U.S. authorities "to develop a strengthened and durable transfer mechanism," but there is no telling how long this might take.

## Slide 6



Principles of Computer Security, Fifth Edition

### Right of Control Over Privacy

- EU: balanced in favor of consumer
  - US: balanced in favor of the provider
- EU: privacy services are free
  - US: privacy services are premium subscription features
- EU: default deny sharing (opt-in)
  - US: default allow sharing (opt-out)
- EU: privacy is a right
  - US: privacy is a luxury
    - EU: that's too bad. bye.
    - US: Wait! We didn't understand the consequences...
    - » EU: SMH

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


Another major difference between U.S. and European regulation lies in where the right of control is exercised. In European directives, the right of control over privacy is balanced in such a way as to favor consumers. Rather than having to pay to opt out, as with unlisted phone numbers in the United States, consumers have such services for free.

Rather than having to opt out at all, the default privacy setting is deemed to be the highest level of data privacy, and users have to opt in to share information. This default setting is a cornerstone of the European Union's Directive on Protection of Personal Data and is enforced through national laws in all member nations.

Principles of Computer Security, Fifth Edition

## General Data Protection Regulation (GDPR)

- 2 factors led to a rewrite of EU data protection regulations
  1. 2013: Snowden reveals US's dirty secrets
  2. 2015: CJEU invalidates Safe Harbor
- 2018: GDPR: ----- 
  - Data Protection Officer
  - Improved consent requirements
  - New individual rights: information, access, rectification, restrict processing, objection, erasure, data portability




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

Two factors led to what can only be seen as a complete rewrite of EU data protection regulations. In light of the Snowden revelations, the EU began a new round of examining data protection when shared with the U.S. and others. Then the European Court of Justice's invalidated the Safe Harbor provisions. This led the way to the passage of the General Data Protection Regulation (GDPR), which went into effect in May of 2018.

The GDPR ushers in a brand-new world with respect to data protection and privacy. Anyone wishing to do trade with the EU must abide by GDPR, or else. Or else the EU won't trade with you. It brings many changes, one being the appointment of a Data Protection Officer (DPO), which reports to the highest level of management and must operate with significant independence.

The GDPR also specifies requirements regarding consent, and they are significantly more robust than previous regulations. And it provides protections for new individual rights, which may force firms to adopt new policies to address these requirements.




Principles of Computer Security, Fifth Edition

## Canadian Law

- Centralized form of privacy legislation that applies to every organization that collects, uses, or discloses personal information
- **Personal Information Protection and Electronic Data Act (PIPEDA)**
  - Requires that personal information be collected and used only for appropriate purposes
  - Individuals must be notified as to why the information is requested and how it will be used.
  - Safeguards associated with storage, use, reuse, and retention.
- National- and provincial-level privacy commissioners
  - act as advocates on behalf of individuals and use legal actions to

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

Like many European countries, Canada has a centralized form of privacy legislation that applies to every organization that collects, uses, or discloses personal information, including information about employees. These regulations stem from the Personal Information Protection and Electronic Data Act (PIPEDA) which requires that personal information be collected and used only for appropriate purposes. Individuals must be notified as to why the information is requested and how it will be used. PIPEDA has safeguards associated with storage, use, reuse, and retention. To ensure leadership in the field of privacy issues, Canada has a national level privacy commissioner and each province has a province-level privacy commissioner. These commissioners act as advocates on behalf of individuals and have used legal actions to enforce the privacy provisions associated with PIPEDA to protect personal information.



Principles of Computer Security, Fifth Edition

## Laws in Asia


- Japan's Personal Information Protection Law
- Hong Kong office of the Privacy Commissioner for Personal Data, Personal Data (Privacy) Ordinance
- China has had a long reputation of poor privacy practices.

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

Provisions of Japan's Personal Information Protection Law require the government entity to specify the purpose for which information is being collected, the safeguards applied, and when permitted, discontinue use of the information upon request

Hong Kong has a statutory body entrusted with the task of protecting personal data privacy of individuals and to ensure compliances

China has had a long reputation of poor privacy practices. China's constitution has provisions for privacy protections for the citizens. Even so, issues have come in the area of enforcement and penalties, and privacy items that have been far from uniform in their judicial history.



## 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.

# Privacy: Privacy-Enhancing Technologies

Slide 1



The slide features a dark red header with the text "Principles of Computer Security, Fifth Edition" in white. On the left side of the header is a small blue icon depicting a network of nodes and locks. The main content area is white and contains the word "Privacy" in a large, black, sans-serif font. Below this is a photograph of a concrete barrier with a sign that reads "PRIVATE NO ACCESS" in raised letters. The background of the photo shows a field and trees. At the bottom of the slide, the text "Privacy-Enhancing Technologies" is written in a smaller, grey font. A small copyright notice is visible at the very bottom left of the slide frame.

Principles of Computer Security, Fifth Edition

## Privacy



Privacy-Enhancing Technologies

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

Howdy! In this video, we discuss privacy-enhancing technologies.



## Slide 2

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 of a blue circuit board with various components. The main content area is white with a black border. It contains a title "Privacy-Enhancing Technologies (PET)" and a bulleted list of three main points. The first point is "There is no privacy without information security," which has two sub-points: "Don't Forget: There is no security without physical security" and "CIA are still important." The second point is "Technology offers the means to protect privacy," with a sub-point "Part of the problem and solution." The third point is "An application or tool that assists in such protection is called a **privacy-enhancing technology (PET)**." 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

### Privacy-Enhancing Technologies (PET)

- There is no privacy without information security.
  - Don't Forget: There is no security without physical security
  - CIA are still important
- Technology offers the means to protect privacy.
  - Part of the problem and solution
- An application or tool that assists in such protection is called a **privacy-enhancing technology (PET)**.

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

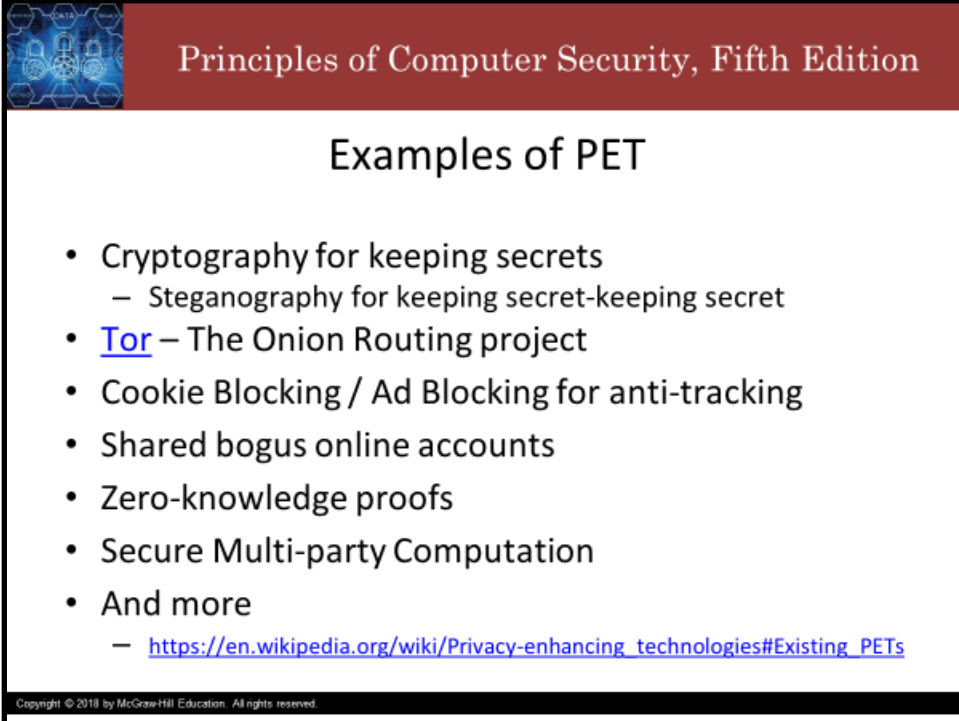
One principal connection between information security and privacy is that without information security, you cannot have privacy.

Since privacy is the ability to control information about oneself, the security goals of confidentiality, integrity, and availability are also critical elements of privacy.

Just as technology has enabled many privacy-impacting issues, technology also offers the means in many cases to protect privacy.

An application or tool that assists in such protection is called a **privacy-enhancing technology (PET)**.

## Slide 3



The slide features a dark red header with the text "Principles of Computer Security, Fifth Edition" in white. Below the header, the title "Examples of PET" is centered in black. A list of examples follows, including Cryptography, Tor, Cookie Blocking, Shared bogus online accounts, Zero-knowledge proofs, and Secure Multi-party Computation. A URL is provided at the bottom of the list. A small copyright notice is visible in the bottom left corner of the slide frame.

Principles of Computer Security, Fifth Edition

### Examples of PET

- Cryptography for keeping secrets
  - Steganography for keeping secret-keeping secret
- [Tor](#) – The Onion Routing project
- Cookie Blocking / Ad Blocking for anti-tracking
- Shared bogus online accounts
- Zero-knowledge proofs
- Secure Multi-party Computation
- And more
  - [https://en.wikipedia.org/wiki/Privacy-enhancing\\_technologies#Existing\\_PETs](https://en.wikipedia.org/wiki/Privacy-enhancing_technologies#Existing_PETs)

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

Encryption is at the top of the list of PETs for protecting privacy and anonymity. Encryption is very useful for keeping secrets. Steganography is up there, too, though it is not as popular yet. Steganography is good for keeping the secret that secrets are being kept, which is to say, hiding the usage of cryptography.

Tor uses onion routing. The goal of onion routing was to have a way to use the Internet with as much privacy as possible, and the idea was to route traffic through multiple servers and encrypt it each step of the way. Tor enables secure and anonymous browsing of the web.


There are browser plugins that are designed to prevent the transfer of cookies between browsers and web servers, which can be used to track users across the web. Ad blockers also have a cookie blocking feature by virtue of preventing the advertisements from loading.

Shared bogus online accounts are used by multiple unrelated people. Somebody creates an account on some web service with bogus personal information and then publishes the user-ID and password on the Internet so that anybody can use the account. The users are sure that there is no personal data about themselves in the account profile and the activities of the account are not attributable to any single person.

Zero-knowledge proof is a method by which one party (the prover) can prove to another party (the verifier) that they know a value  $x$  without conveying any information apart from the fact that they know the value  $x$ .

Secure multi-party computation is a method for parties to jointly compute a function over their inputs while keeping those inputs private.

## Slide 4



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.

# Privacy: Privacy Policies


Slide 1



The slide features a dark red header with the text "Principles of Computer Security, Fifth Edition" in white. On the left side of the header is a small blue icon depicting a network of nodes and locks. The main content area is white and contains the word "Privacy" in a large, black, sans-serif font. Below this is a photograph of a concrete barrier with a wooden sign that reads "PRIVATE NO ACCESS" in capital letters. The background of the photo shows a field with a line of trees in the distance. Below the photograph, the words "Privacy Policies" are written in a smaller, grey, sans-serif font. At the bottom left of the slide, there is a small copyright notice: "Copyright © 2018 by McGraw-Hill Education. All rights reserved."

Howdy! In this video, we discuss privacy policies.

## Slide 2



Principles of Computer Security, Fifth Edition

### Privacy Policies

- One of the direct outcomes of the legal statutes associated with privacy has been the development of a need for corporate privacy policies associated with data collection.
- Policies and procedures are the best way to ensure uniform compliance across an organization.
- The development of a **privacy policy** is an essential foundational element of a company's privacy stance.

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

One of the direct outcomes of the legal statutes associated with privacy has been the development of a need for corporate privacy policies associated with data collection.

Policies and procedures are the best way to ensure uniform compliance across an organization.

The development of a **privacy policy** is an essential foundational element of a company's privacy stance.

## Slide 3



Principles of Computer Security, Fifth Edition

### Privacy Compliance Steps

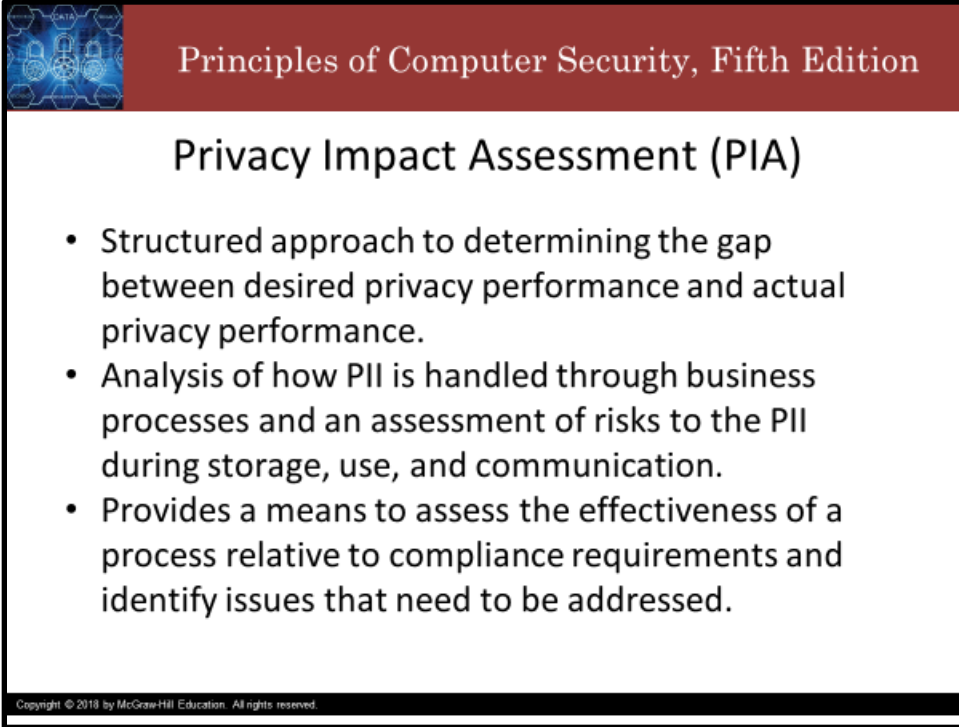
1. Identify the role in the organization that will be responsible for compliance and oversight.
2. Document all applicable laws and regulations, industry standards, and contract requirements.
3. Identify any industry best practices.
4. Perform a privacy impact assessment (PIA) and a risk assessment.
5. Map the identified risks to compliance requirements.
6. Create a unified risk mitigation plan.

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

To ensure that an organization complies with the numerous privacy requirements and regulations, a structured approach to privacy planning and policies is recommended.

1. Identify the role in the organization that will be responsible for compliance and oversight.
2. Document all applicable laws and regulations, industry standards, and contract requirements.
3. Identify any industry best practices.
4. Perform a privacy impact assessment (PIA) and a risk assessment.
5. Map the identified risks to compliance requirements.
6. Create a unified risk mitigation plan.

## Slide 4



The slide features a dark red header with the text "Principles of Computer Security, Fifth Edition" in white. Below the header, the title "Privacy Impact Assessment (PIA)" is centered in a large, bold, black font. The main content consists of three bullet points, each starting with a black dot. At the bottom left of the slide, there is a small, light-colored icon depicting a network of nodes and connections. A thin black line runs along the bottom edge of the slide content area.

Principles of Computer Security, Fifth Edition

### Privacy Impact Assessment (PIA)

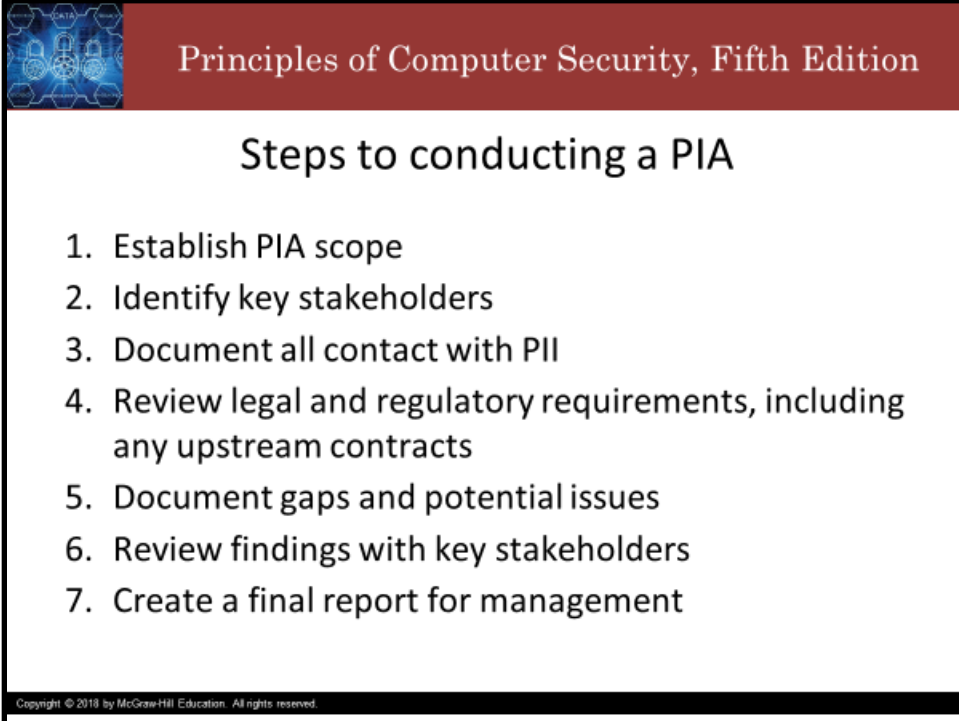
- Structured approach to determining the gap between desired privacy performance and actual privacy performance.
- Analysis of how PII is handled through business processes and an assessment of risks to the PII during storage, use, and communication.
- Provides a means to assess the effectiveness of a process relative to compliance requirements and identify issues that need to be addressed.

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

A **privacy impact assessment (PIA)** is a structured approach to determining the gap between desired privacy performance and actual privacy performance.

A PIA is an analysis of how PII is handled through business processes and an assessment of risks to the PII during storage, use, and communication and provides a means to assess the effectiveness of a process relative to compliance requirements and identify issues that need to be addressed.

## Slide 5



Principles of Computer Security, Fifth Edition

### Steps to conducting a PIA

1. Establish PIA scope
2. Identify key stakeholders
3. Document all contact with PII
4. Review legal and regulatory requirements, including any upstream contracts
5. Document gaps and potential issues
6. Review findings with key stakeholders
7. Create a final report for management


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

The following steps comprise a high-level methodology and approach for conducting a PIA:

- 1. Establish PIA scope.** Determine the departments involved and the appropriate representatives. Determine which applications and business processes need to be assessed. Determine applicable laws and regulations associated with the business and privacy concerns.
- 2. Identify key stakeholders.** Identify all business units that use PII. Examine staff functions such as HR, Legal, IT, Purchasing, and Quality Control.
- 3. Document all contact with PII:**
  - PII collection, access, use, sharing, disposal
  - Processes and procedures, policies, safeguards, data-flow diagrams, and any other risk assessment data
  - Web site policies, contracts, HR, and administrative for other PII
- 4. Review legal and regulatory requirements, including any upstream contracts.** The sources are many, but some commonly overlooked issues are agreements with suppliers and customers over information sharing rights.
- 5. Document gaps and potential issues between requirements and practices.** All gaps and issues should be mapped against where the issue was discovered and the basis (requirement or regulation) that the gap maps to.
- 6. Review findings with key stakeholders to determine accuracy and clarify any issues.** Before the final report is written, any issues or possible miscommunications should be clarified with the appropriate stakeholders to ensure a fair and accurate report.
- 7. Create the final report for management.**



## Slide 6

	<h1>Principles of Computer Sec</h1>	<h3>PRIVACY POLICY</h3> <p>WE'VE UPDATED OUR PRIVACY POLICY. THIS IS PURELY OUT OF THE GOODNESS OF OUR HEARTS, AND HAS NOTHING TO DO WITH ANY HYPOCRITICAL LINKS ON ANY PARTICULAR CONTINENTS. PLEASE READ EVERY PART OF THIS POLICY CAREFULLY, AND DON'T JUST SKIP AHEAD LOOKING FOR SEX SCENES.</p> <p>THIS POLICY GOVERNS YOUR INTERACTIONS WITH THIS WEBSITE, HEREIN REFERRED TO AS "THE SERVICE," "THE WEBSITE," "THE INTERNET," OR "FACEBOOK," AND WITH ALL OTHER WEBSITES AND ORGANIZATIONS OF ANY KIND. THE ENFORCEMENT IN THIS POLICY OF CERTAIN RIGHTS, SHALL NOT BE CONSTRUED TO DENY OR DISPARAGE OTHERS RETAINED BY THE USERS. BY USING THIS SERVICE, YOU OPT IN TO QUARANTERING TREES IN YOUR HOME.</p>
<h2>Attribution</h2> <ul style="list-style-type: none"><li>• 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).</li><li>• These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.</li><li>• There have been some changes to the slide deck.</li></ul> <p><a href="https://xkcd.com/1998/">https://xkcd.com/1998/</a></p>		<h3>YOUR PERSONAL INFORMATION</h3> <p>PLEASE DON'T SEND US YOUR PERSONAL INFORMATION. WE DO NOT WANT YOUR PERSONAL INFORMATION. WE HAVE A HARD ENOUGH TIME KEEPING TRACK OF OUR OWN PERSONAL INFORMATION, LET ALONE YOURS.</p> <p>IF YOU TELL US YOUR NAME OR ANY IDENTIFYING INFORMATION, WE WILL FORGET IT IMMEDIATELY. THE NEXT TIME WE SEE YOU, WE'LL STRUGGLE TO REMEMBER WHO YOU ARE, AND TRY DESPERATELY TO GET THROUGH THE CONVERSATION SO WE CAN GO ONLINE AND HOPEFULLY FIGURE IT OUT.</p> <h3>TRACKING PIXELS, COOKIES, AND BEACONS</h3> <p>THIS WEBSITE PLACES PIXELS ON YOUR SCREEN IN ORDER TO FORM TEXT AND IMAGES, SOME OF WHICH MAY REMAIN IN YOUR MEMORY AFTER YOU CLOSE THE PAGE. WE USE COOKIES TO ENHANCE YOUR PERFORMANCE. OUR WEBSITE MAY USE LOCAL STORAGE ON YOUR DEVICE IF WE RUN LOW ON SPACE. ON OUR END, WE MAY USE BEACONS TO CALL HOMES FOR AD.</p> <h3>3RD PARTY EXTENSIONS</h3> <p>THIS SERVICE MAY UTILIZE 3RD PARTY EXTENSIONS IN ORDER TO PLAY THE SONG <i>OWN YOUR FEEL IT</i> FROM THEIR DEBUT ALBUM <i>ALONE</i>.</p> <h3>PERMISSION</h3> <p>FOR USERS WHO ARE CITIZENS OF THE EUROPEAN UNION, WE WILL NOW BE REQUESTING PERMISSION BEFORE INITIATING ORGAN HARVESTING.</p> <h3>SCOPE AND LIMITATIONS</h3> <p>THIS POLICY SUPERSEDES ANY APPLICABLE FEDERAL, STATE, AND LOCAL LAWS, REGULATIONS AND ORDINANCES, INTERNATIONAL TREATIES, AND LEGAL AGREEMENTS THAT WOULD OTHERWISE APPLY. IF ANY PROVISION OF THIS POLICY IS FOUND BY A COURT TO BE UNENFORCEABLE, IT NEVERTHELESS REMAINS IN FORCE.</p> <p>THIS ORGANIZATION IS NOT LIABLE AND THIS AGREEMENT SHALL NOT BE CONSTRUED. THESE STATEMENTS HAVE NOT BEEN EVALUATED BY THE FDA. THIS WEBSITE IS INTENDED TO TREAT, CURE, AND PREVENT ANY DISEASE. IF YOU KNOW ANYONE IN EUROPE, PLEASE TELL THEM WE'RE COOL.</p>
<p>Copyright © 2018 by McGraw-Hill Education. All rights reserved.</p>		

Thank you and take care.

# Privacy: Web Privacy Issues

Slide 1



Principles of Computer Security, Fifth Edition

## Privacy




Web Privacy Issues

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

Howdy! In this video, we briefly discuss web privacy issues.

## Slide 2



Principles of Computer Security, Fifth Edition

### Web Privacy Issues

- The Internet acts as a large information-sharing domain.
  - Serves as a conduit for the transference of information among many parties
- The Web offers much in the form of communication between machines, people, and systems.
  - This exchange of information can be associated with privacy based on the content of the information and the reason for the exchange.

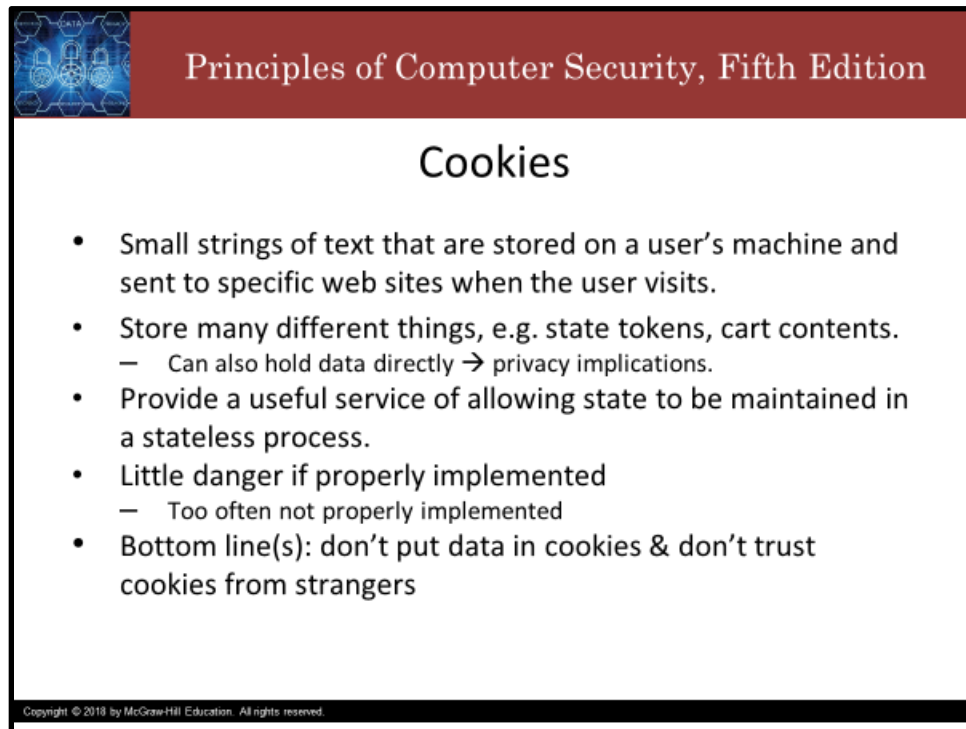
Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The Internet is a large information-sharing domain and serves as a conduit for the transference of information among many parties.

Some of that transfer is intended, and some not so much. Some is with consent, and some without.

The exchange of information on the Internet entails privacy considerations based on the content of the information and the reason for the exchange.

## Slide 3



Principles of Computer Security, Fifth Edition

### Cookies

- Small strings of text that are stored on a user's machine and sent to specific web sites when the user visits.
- Store many different things, e.g. state tokens, cart contents.
  - Can also hold data directly → privacy implications.
- Provide a useful service of allowing state to be maintained in a stateless process.
- Little danger if properly implemented
  - Too often not properly implemented
- Bottom line(s): don't put data in cookies & don't trust cookies from strangers

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

Cookies are small bits of text that are stored on a user's machine and sent to specific websites when the user visits.

Cookies can store many different things, from tokens that provide a reference to a database server behind the webserver to assist in maintaining state through an application to the contents of a shopping cart.

Cookies can also hold data directly, in which case there are possible privacy implications.

When a cookie holds a token number that is meaningless to outsiders but meaningful to a back-end server, then the loss of the cookie represents no loss at all.

When the cookie text contains meaningful information, then the loss can result in privacy issues.

For instance, when a cookie contains a long number that has no meaning except to the database server, then the number has no PII.

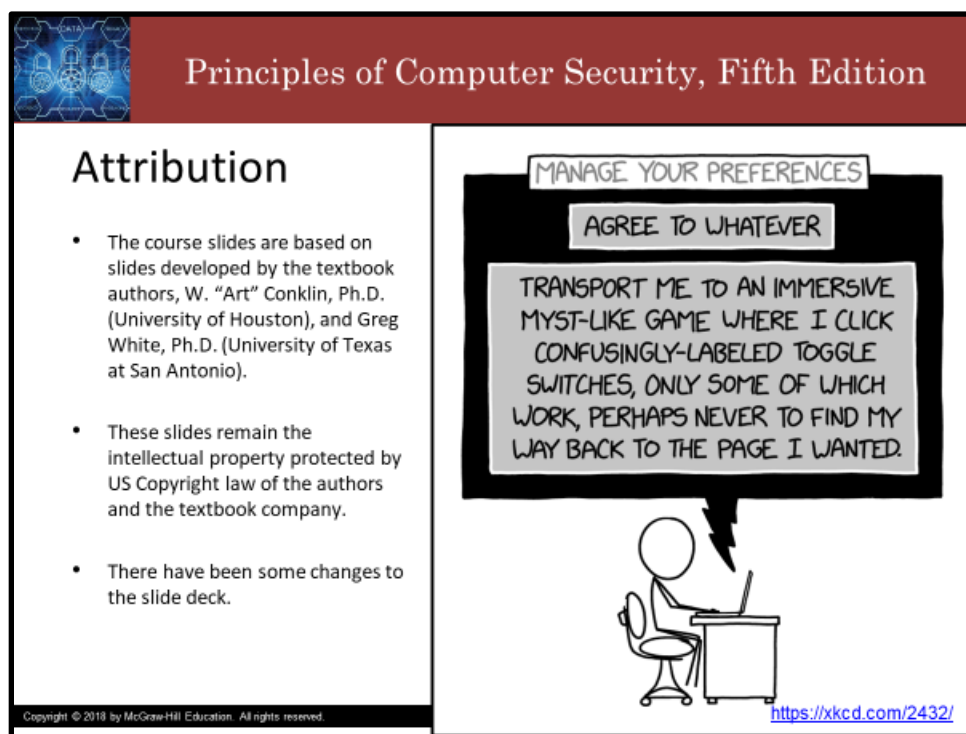
But if the cookie contains text, such as a ship-to address for an order, this can represent PII and can result in a privacy violation.

It is common to encode the data in cookies, but encoding – such as Base64 -- is not encryption and can be decoded by anyone, thus providing no security.

Cookies provide a useful service of allowing states to be maintained in a stateless process like web serving. But because of the potential for PII leakage, many users have sworn off cookies. This leads to issues on numerous websites, for when properly implemented, they pose no privacy danger and can greatly enhance website usefulness.

The bottom line for cookies is fairly easy—done correctly, they do not represent a security or privacy issue. Done incorrectly, they can be a disaster. A simple rule solves most problems with cookies: never store data directly on a cookie; instead, store a reference to another web application that permits the correct actions to occur based on the key value.

## Slide 4



The slide features a red header with the text "Principles of Computer Security, Fifth Edition" and a small graphic of a globe with circuit patterns. The main content is divided into two sections. The left section, titled "Attribution", contains three bullet points. The right section contains a cartoon of a person at a computer with a large speech bubble containing text about user preferences. A URL is provided at the bottom right of the cartoon.

**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.

**MANAGE YOUR PREFERENCES**  
**AGREE TO WHATEVER**

TRANSPORT ME TO AN IMMERSIVE MYST-LIKE GAME WHERE I CLICK CONFUSINGLY-LABELED TOGGLE SWITCHES, ONLY SOME OF WHICH WORK, PERHAPS NEVER TO FIND MY WAY BACK TO THE PAGE I WANTED.

<https://xkcd.com/2432/>

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

Thank you and take care.

# Privacy: Privacy in Practice

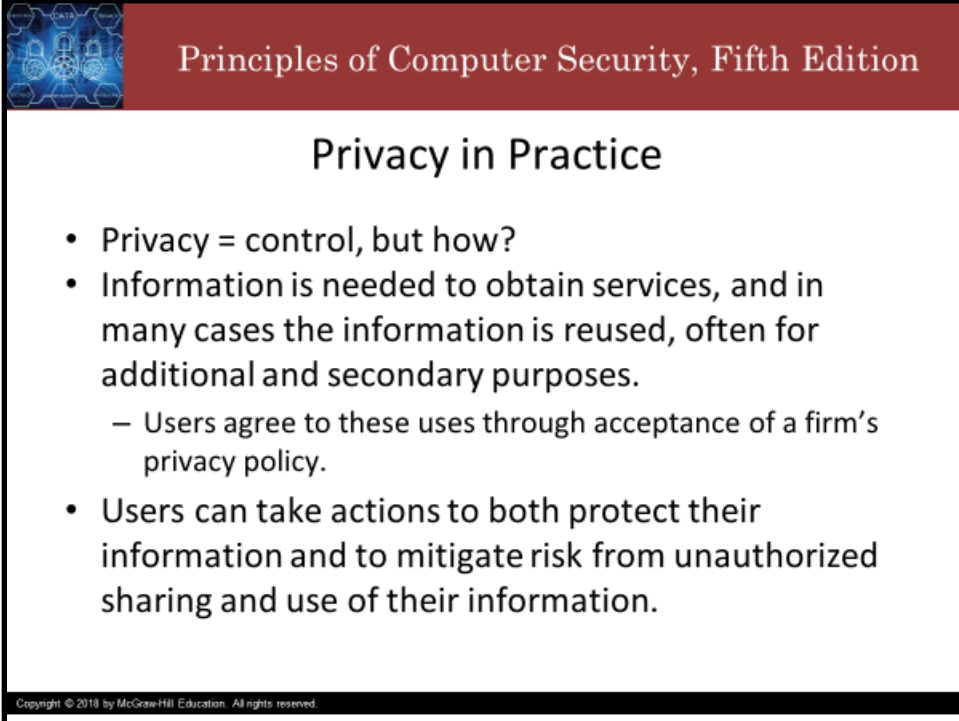
Slide 1



The slide features a dark red header with the text "Principles of Computer Security, Fifth Edition" in white. On the left side of the header is a small blue icon depicting a network of nodes and locks. The main content area is white and contains the word "Privacy" in a large, black, sans-serif font. Below this is a photograph of a concrete barrier with a sign that reads "PRIVATE NO ACCESS" in raised letters. The background of the photo shows a field and a line of trees. Below the photo, the text "Privacy in Practice" is written in a smaller, grey, sans-serif font. At the bottom left of the slide, there is a small copyright notice: "Copyright © 2018 by McGraw-Hill Education. All rights reserved."

Howdy! In this video, we briefly discuss privacy in practice.

## Slide 2



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 of a network with nodes and connections. The main content area is white with a black border. The title "Privacy in Practice" is centered in black. Below the title is a bulleted list of three points. The first point is "Privacy = control, but how?". The second point is "Information is needed to obtain services, and in many cases the information is reused, often for additional and secondary purposes." with a sub-bullet: "– Users agree to these uses through acceptance of a firm's privacy policy." The third point is "Users can take actions to both protect their information and to mitigate risk from unauthorized sharing and use of their information." 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

### Privacy in Practice

- Privacy = control, but how?
- Information is needed to obtain services, and in many cases the information is reused, often for additional and secondary purposes.
  - Users agree to these uses through acceptance of a firm's privacy policy.
- Users can take actions to both protect their information and to mitigate risk from unauthorized sharing and use of their information.

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

With privacy being defined as the power to control what others know about you and what they can do with that information, there remains the question of what you can do to exercise that control.

Information is needed to obtain services, and in many cases, the information is reused, often for additional and secondary purposes.

Users agree to these uses through acceptance of a firm's privacy policy.

Shared information still requires control, and in this case, the control function has shifted to the party that obtained the information.

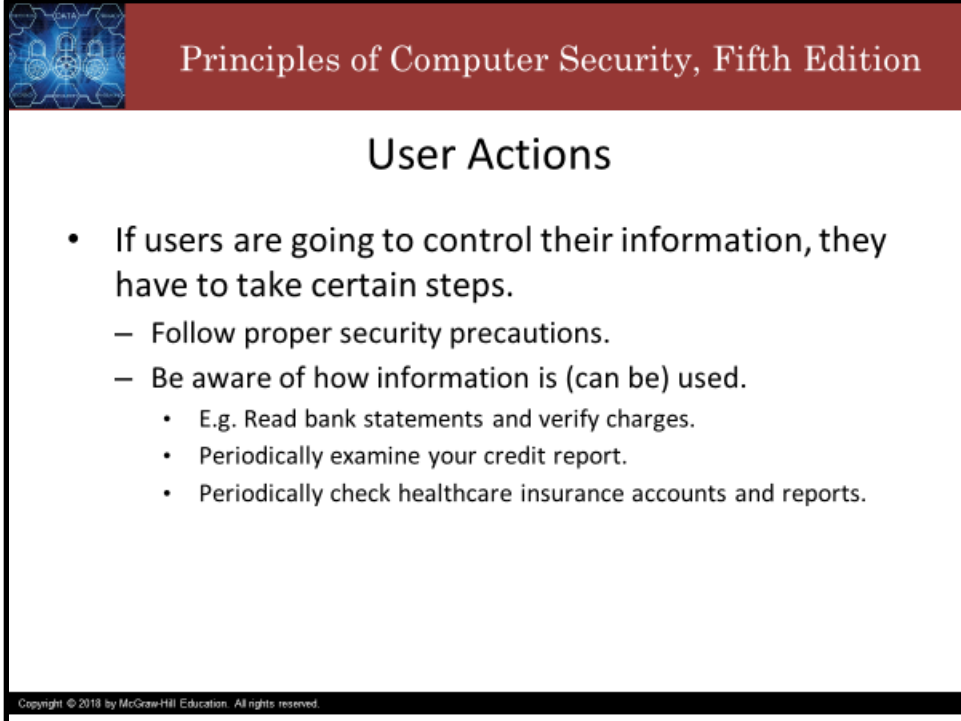
They may store it for future use, for record purposes, or for other uses.

If they fail to adequately protect the information from loss or disclosure, then the owner no longer has authorized the uses it may be employed in.

Data disclosures and information thefts both result in unauthorized use of information.

Users can take actions to both protect their information and to mitigate risk from unauthorized sharing and use of their information.

## Slide 3



Principles of Computer Security, Fifth Edition

### User Actions

- If users are going to control their information, they have to take certain steps.
  - Follow proper security precautions.
  - Be aware of how information is (can be) used.
    - E.g. Read bank statements and verify charges.
    - Periodically examine your credit report.
    - Periodically check healthcare insurance accounts and reports.

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

If users are going to control their information, they have to take certain steps.

Proper security precautions must be followed, such as using privacy-enhancing technology, practicing safe browsing, and using good operational security practices (y'all need to hide ya kids, hide yo wife, and hide yo husband cuz they data mining everybody out here).

Users must also be aware of how their information can be used. Data is valuable because it is useful.

The two main types of information that have immediate value are financial and medical.

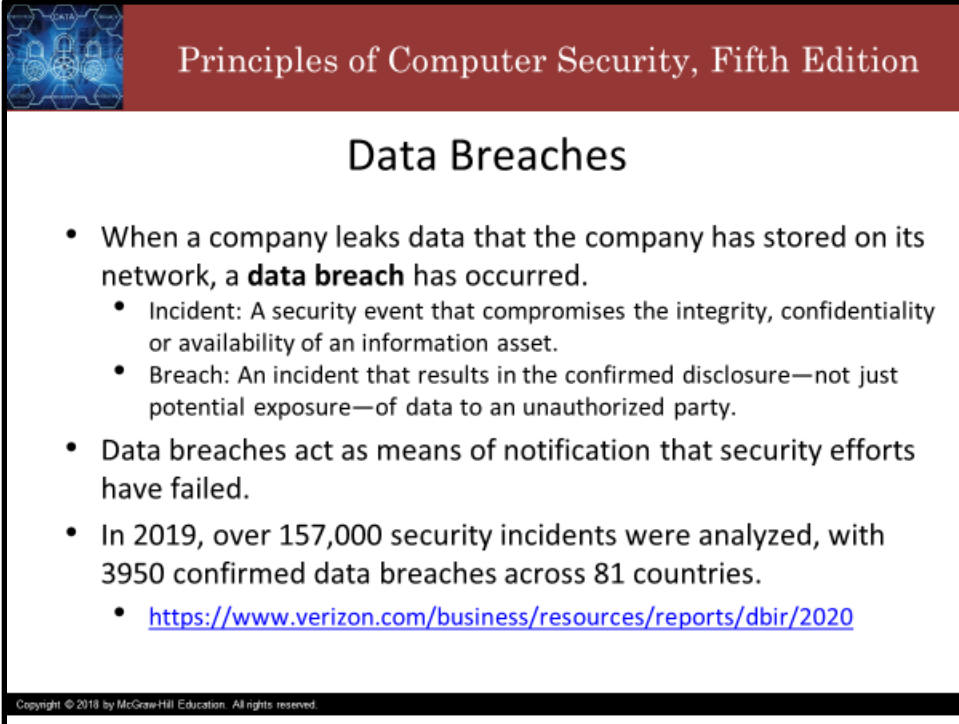
Financial information, such as credit card information, identity information, and banking information, can be used by criminals to steal from others.

Many times the use of identity or financial information will show up on the systems of record associated with the information. This is why it is important to actually read bank statements and verify charges.



You should also periodically request and examine your credit report to verify accuracy and look for unauthorized activity. Likewise, you should periodically check healthcare insurance accounts and reports to make sure all of the activity is accurate and yours.

## Slide 4



Principles of Computer Security, Fifth Edition

### Data Breaches

- When a company leaks data that the company has stored on its network, a **data breach** has occurred.
  - Incident: A security event that compromises the integrity, confidentiality or availability of an information asset.
  - Breach: An incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party.
- Data breaches act as means of notification that security efforts have failed.
- In 2019, over 157,000 security incidents were analyzed, with 3950 confirmed data breaches across 81 countries.
  - <https://www.verizon.com/business/resources/reports/dbir/2020>

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

When data that a company has stored on its network is disclosed to unauthorized actors, a data breach has occurred.

Unfortunately, data breaches too often act as an all-too-painful notification that security efforts have failed. A sort of coming home to find all your stuff is gone (and all the stuff you had borrowed from others) and only then realizing that your practice of leaving the door unlocked was not a suboptimal idea.

Verizon regularly publishes a data breach investigation report, examining the root causes behind hundreds of breach events.

In 2020, over 157,000 security incidents during 2019 were analyzed, with 3950 confirmed data breaches across 81 countries.

Verizon found that 78% of data breaches follow one of 8 distinct patterns:

1. Web applications (~30%)
2. Miscellaneous errors (~20%)
3. Crimeware (~10%)
4. Privilege Misuse (~10%)
5. Lost and Stolen Assets (~5%)
6. Cyber-Espionage (~5%)
7. Point of Sale (~1%)
8. Payment Card Skimmers (~1%)

The denial of service bucket is basically empty for breaches since if nobody can access the data, then it can't be stolen.

The everything else bucket, which consists mainly of social engineering attacks, accounts for over 20% of data breaches. Over the last several years, the number of breaches in this bucket has been increasing steadily.

## Slide 5

**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.

**SOON...**

THE PRESS IS HERE FOR THE PRODUCT LAUNCH! REMEMBER, PEOPLE ARE WARY OF SMART DEVICES, SO WE WANT TO STRIKE A NONTHREATENING TONE.

HANG ON, DID YOU SAY NON-THREATENING? YES, WHY- NOTHING. IT'S PROBABLY FINE.

THEY SAY TECHNOLOGY CAN CHANGE THE WORLD, FOR GOOD OR FOR EVIL. OUR NEW PRODUCT WILL SHOW HOW TRUE THAT IS. WE HEAR THE PLAINITIVE CRIES OF OUR CUSTOMERS. WE WANT TO GIVE THEM WHAT THEY DESERVE.

NOW, LET US EXPOSE OUR PRODUCT TO THE ATMOSPHERE FOR THE FIRST TIME, SURPRISING AND DELIGHTING CUSTOMERS WITHIN A FIVE-BLOCK RADIUS.

I'M LEAVING.

NO, DON'T WORRY! A STAGGERING NUMBER OF PEOPLE WILL SURVIVE!

<https://xkcd.com/2473/>

Thank you and take care.