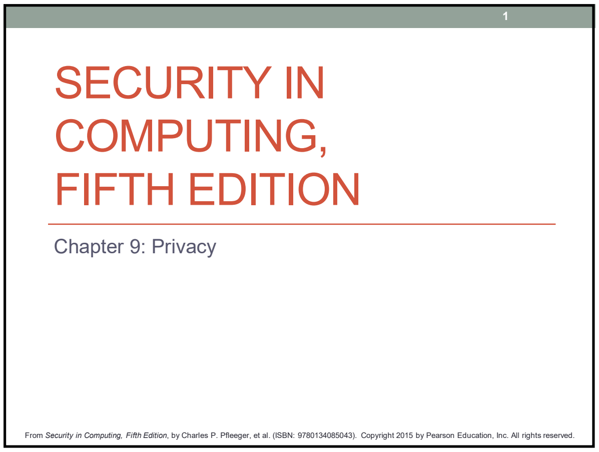


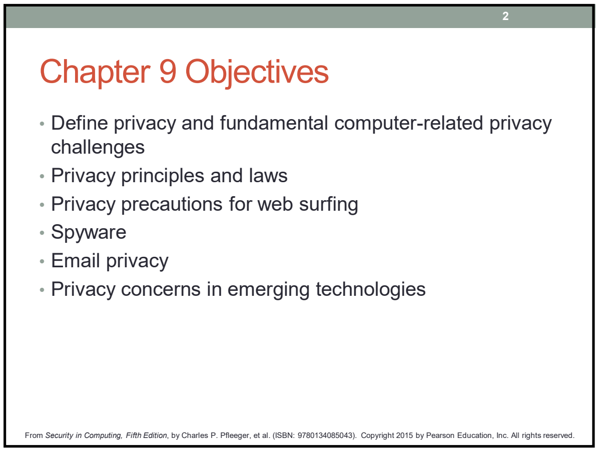
1

SECURITY IN COMPUTING, FIFTH EDITION

Chapter 9: Privacy

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

1



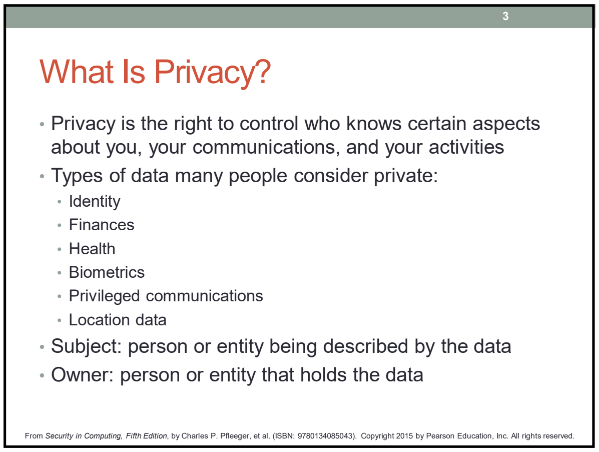
2

Chapter 9 Objectives

- Define privacy and fundamental computer-related privacy challenges
- Privacy principles and laws
- Privacy precautions for web surfing
- Spyware
- Email privacy
- Privacy concerns in emerging technologies

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

2



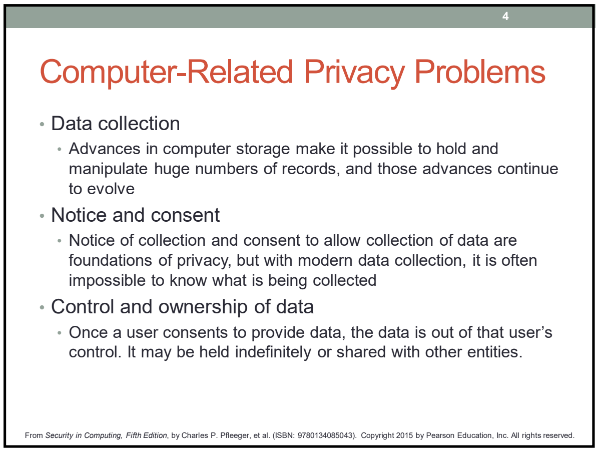
3

What Is Privacy?

- Privacy is the right to control who knows certain aspects about you, your communications, and your activities
- Types of data many people consider private:
  - Identity
  - Finances
  - Health
  - Biometrics
  - Privileged communications
  - Location data
- Subject: person or entity being described by the data
- Owner: person or entity that holds the data

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

3



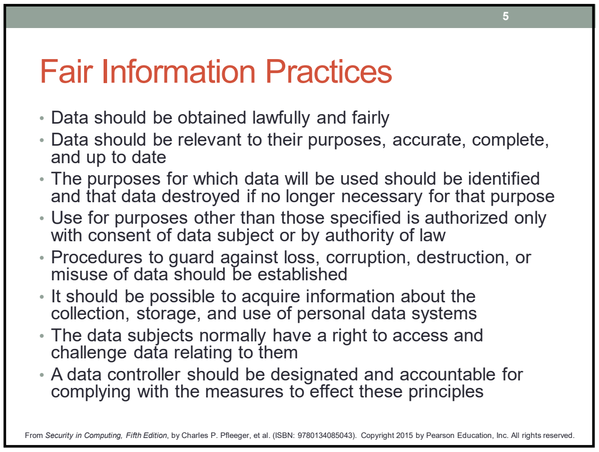
4

Computer-Related Privacy Problems

- Data collection
  - Advances in computer storage make it possible to hold and manipulate huge numbers of records, and those advances continue to evolve
- Notice and consent
  - Notice of collection and consent to allow collection of data are foundations of privacy, but with modern data collection, it is often impossible to know what is being collected
- Control and ownership of data
  - Once a user consents to provide data, the data is out of that user's control. It may be held indefinitely or shared with other entities.

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

4



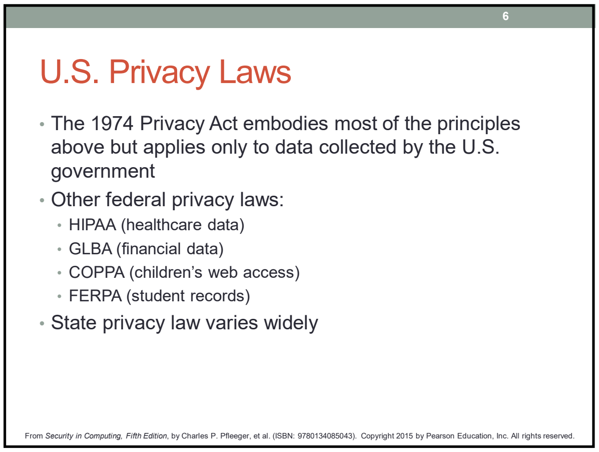
5

Fair Information Practices

- Data should be obtained lawfully and fairly
- Data should be relevant to their purposes, accurate, complete, and up to date
- The purposes for which data will be used should be identified and that data destroyed if no longer necessary for that purpose
- Use for purposes other than those specified is authorized only with consent of data subject or by authority of law
- Procedures to guard against loss, corruption, destruction, or misuse of data should be established
- It should be possible to acquire information about the collection, storage, and use of personal data systems
- The data subjects normally have a right to access and challenge data relating to them
- A data controller should be designated and accountable for complying with the measures to effect these principles

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

5



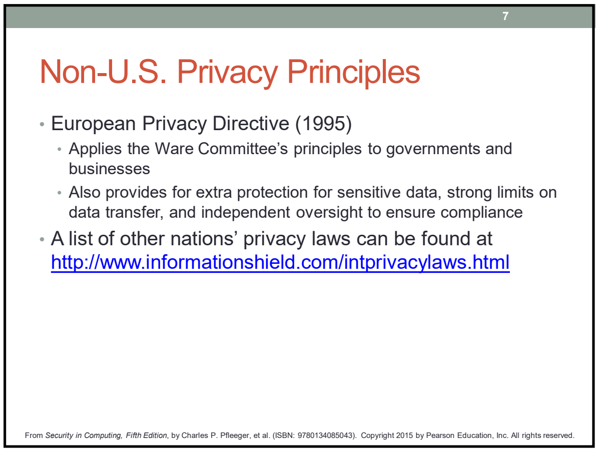
6

U.S. Privacy Laws

- The 1974 Privacy Act embodies most of the principles above but applies only to data collected by the U.S. government
- Other federal privacy laws:
  - HIPAA (healthcare data)
  - GLBA (financial data)
  - COPPA (children's web access)
  - FERPA (student records)
- State privacy law varies widely

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

6



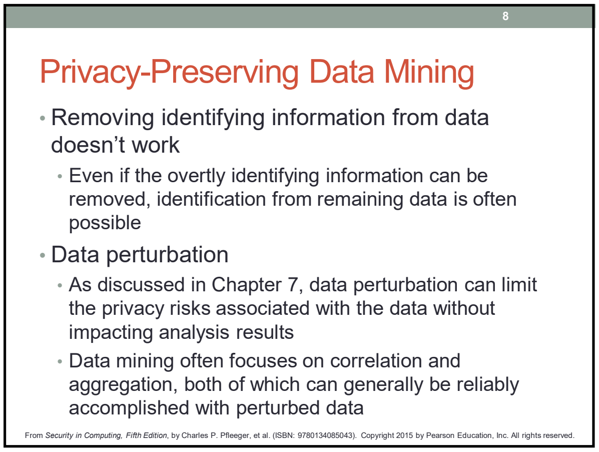
7

Non-U.S. Privacy Principles

- European Privacy Directive (1995)
  - Applies the Ware Committee’s principles to governments and businesses
  - Also provides for extra protection for sensitive data, strong limits on data transfer, and independent oversight to ensure compliance
- A list of other nations’ privacy laws can be found at http://www.informationshield.com/intprivacylaws.html

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

7



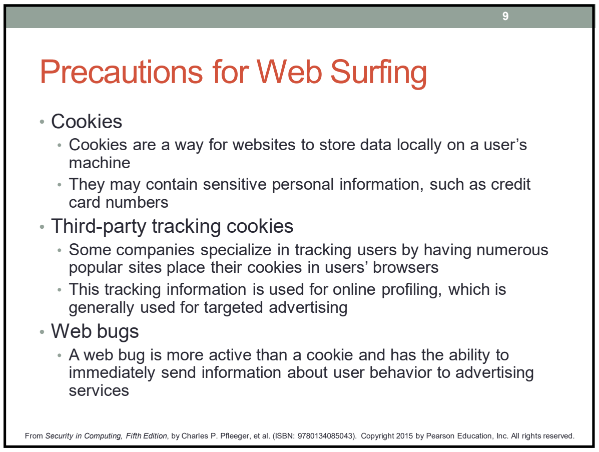
8

Privacy-Preserving Data Mining

- Removing identifying information from data doesn’t work
  - Even if the overtly identifying information can be removed, identification from remaining data is often possible
- Data perturbation
  - As discussed in Chapter 7, data perturbation can limit the privacy risks associated with the data without impacting analysis results
  - Data mining often focuses on correlation and aggregation, both of which can generally be reliably accomplished with perturbed data

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

8



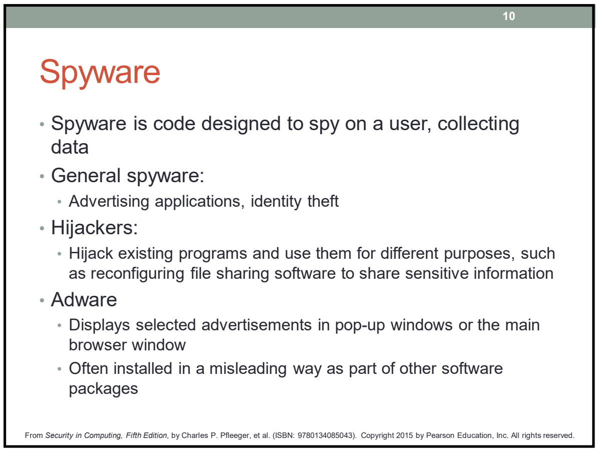
9

Precautions for Web Surfing

- Cookies
  - Cookies are a way for websites to store data locally on a user’s machine
  - They may contain sensitive personal information, such as credit card numbers
- Third-party tracking cookies
  - Some companies specialize in tracking users by having numerous popular sites place their cookies in users’ browsers
  - This tracking information is used for online profiling, which is generally used for targeted advertising
- Web bugs
  - A web bug is more active than a cookie and has the ability to immediately send information about user behavior to advertising services

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

9



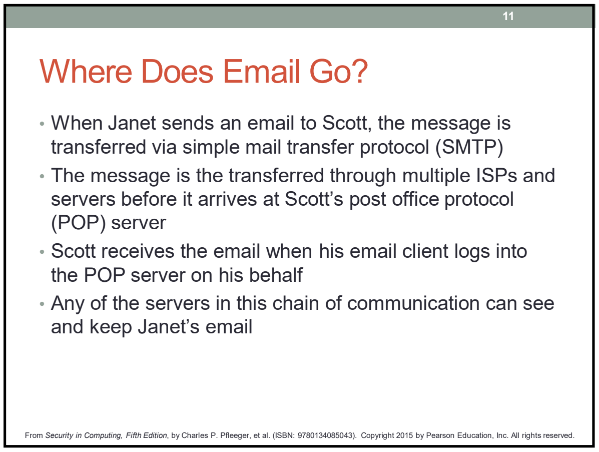
10

Spyware

- Spyware is code designed to spy on a user, collecting data
- General spyware:
  - Advertising applications, identity theft
- Hijackers:
  - Hijack existing programs and use them for different purposes, such as reconfiguring file sharing software to share sensitive information
- Adware
  - Displays selected advertisements in pop-up windows or the main browser window
  - Often installed in a misleading way as part of other software packages

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

10



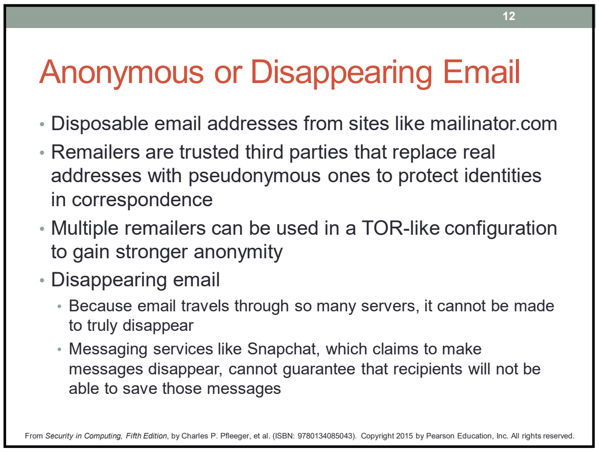
11

Where Does Email Go?

- When Janet sends an email to Scott, the message is transferred via simple mail transfer protocol (SMTP)
- The message is the transferred through multiple ISPs and servers before it arrives at Scott's post office protocol (POP) server
- Scott receives the email when his email client logs into the POP server on his behalf
- Any of the servers in this chain of communication can see and keep Janet's email

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

11



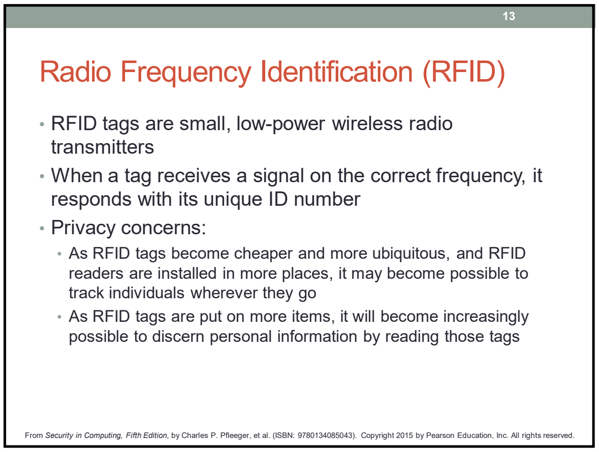
12

Anonymous or Disappearing Email

- Disposable email addresses from sites like mailinator.com
- Remailers are trusted third parties that replace real addresses with pseudonymous ones to protect identities in correspondence
- Multiple remailers can be used in a TOR-like configuration to gain stronger anonymity
- Disappearing email
  - Because email travels through so many servers, it cannot be made to truly disappear
  - Messaging services like Snapchat, which claims to make messages disappear, cannot guarantee that recipients will not be able to save those messages

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

12



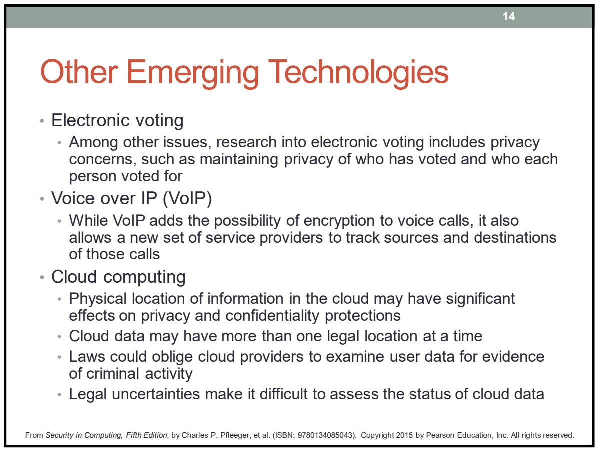
13

Radio Frequency Identification (RFID)

- RFID tags are small, low-power wireless radio transmitters
- When a tag receives a signal on the correct frequency, it responds with its unique ID number
- Privacy concerns:
  - As RFID tags become cheaper and more ubiquitous, and RFID readers are installed in more places, it may become possible to track individuals wherever they go
  - As RFID tags are put on more items, it will become increasingly possible to discern personal information by reading those tags

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

13



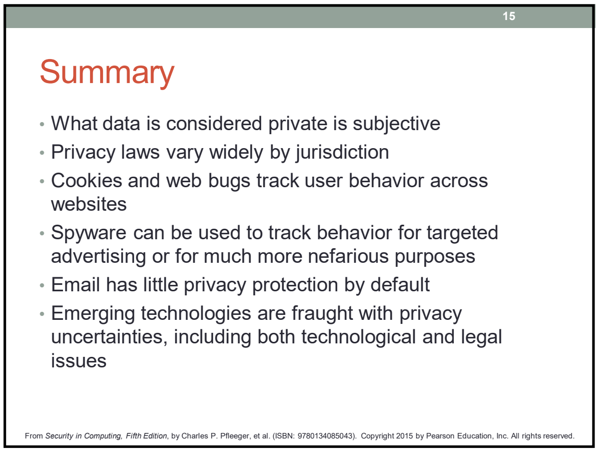
14

Other Emerging Technologies

- Electronic voting
  - Among other issues, research into electronic voting includes privacy concerns, such as maintaining privacy of who has voted and who each person voted for
- Voice over IP (VoIP)
  - While VoIP adds the possibility of encryption to voice calls, it also allows a new set of service providers to track sources and destinations of those calls
- Cloud computing
  - Physical location of information in the cloud may have significant effects on privacy and confidentiality protections
  - Cloud data may have more than one legal location at a time
  - Laws could oblige cloud providers to examine user data for evidence of criminal activity
  - Legal uncertainties make it difficult to assess the status of cloud data

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

14



15

Summary

- What data is considered private is subjective
- Privacy laws vary widely by jurisdiction
- Cookies and web bugs track user behavior across websites
- Spyware can be used to track behavior for targeted advertising or for much more nefarious purposes
- Email has little privacy protection by default
- Emerging technologies are fraught with privacy uncertainties, including both technological and legal issues

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

15