Information Technology Fundamentals

Mohammad Hossein Manshaei
manshaei@gmail.com

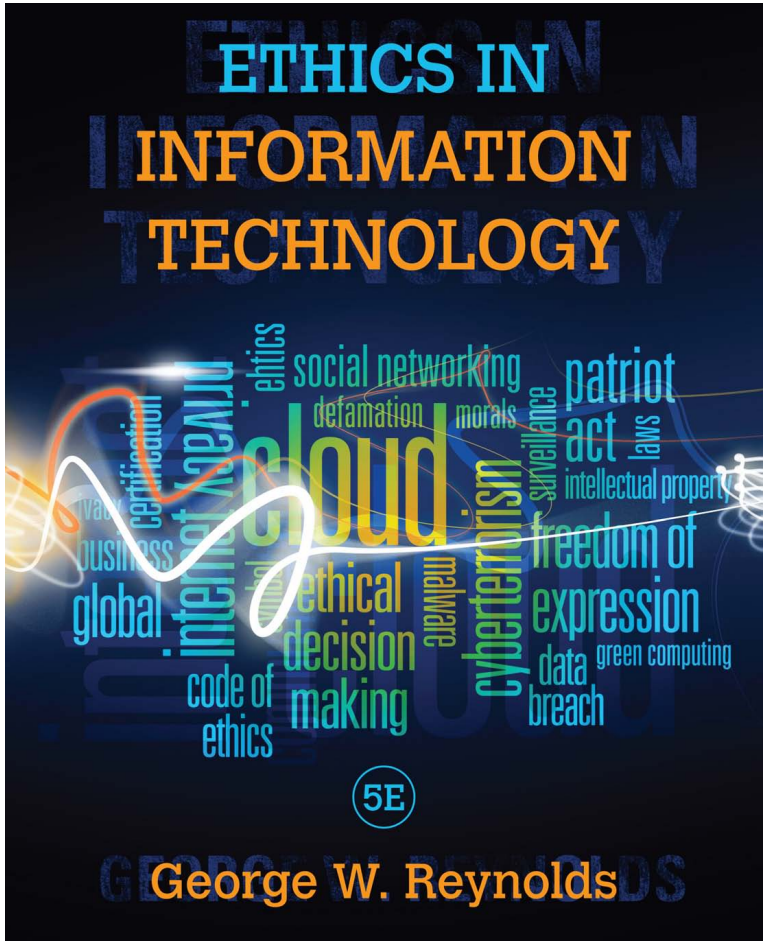
Information Assurance & Security: Key Privacy Issues
Module 7: Part 3

Module 7. Main Objectives

1. Define Main Concepts of Information Privacy
2. Review Privacy Laws, Applications, and Key issues

Main Reference

- George W. Reynolds, 2011. **Ethics in Information Technology.** Engage Learning.



Contents

- ➢ Key Privacy and Anonymity Issues
  - ◇ Identity Theft
  - ◇ Electronic Discovery
  - ◇ Consumer Profiling
  - ◇ Treating Consumer Data Responsibility
  - ◇ Work Place Monitoring
  - ◇ Advanced Surveillance Technology
- ➢ Case Study: Google

Identity Theft

- Theft of key pieces of personal information to gain access to a person's financial accounts
- Information includes:
  - Name
  - Address
  - Date of birth
  - Social Security number (SSN)
  - Passport number
  - Driver's license number
  - Mother's maiden name

Identity Theft (continued)

- Fastest growing form of fraud in the United States
- Lack of initiative in informing people whose data was stolen
- Over 225 million electronic records containing personal data were stolen between January 2005 and May 2008

Recommendations for Safeguarding Your Identity Data

Recommendation	Explanation
Completely and irrevocably destroy digital identity data on used equipment	As it is possible to undelete files and recover data, take necessary actions to ensure that all data is destroyed when you dispose of used computers and data storage devices; consider the use of special software, such as Shred XP
Shred everything	Identity thieves are not above "dumpster diving"—going through your garbage to find financial statements and bills in order to obtain confidential personal information
Require retailers to request a photo ID when accepting your credit card	Writing "Request Photo ID" on the back of your credit cards should prompt retailers to request a photo ID before accepting your card
Beware shoulder surfing	Ensure that nobody can look over your shoulder when you enter or write down personal information—at an ATM, filling out forms in public places, and so on
Minimize personal data shown on checks	Do not include a Social Security number or driver's license number on your checks
Minimize time that mail is in your mailbox	Do not leave paid bills in your mailbox for postal pickup; collect mail from your mailbox as soon as possible after it is delivered
Do not use debit cards to pay for online purchases	Victims of credit card fraud are liable for no more than $50 in losses; debit card users can have their entire checking account wiped out
Treat your credit card receipts safely	Always take your credit card receipts from the retailer and keep them for reconciliation purposes; dispose of them by shredding them
Use hard-to-guess passwords and PINs	Do not use names or words in passwords; include a mix of capital and small letters with at least one special character ($, #, *)

Identity Theft: Approaches

1. Create a data breach to steal hundreds, thousands, or even millions of personal records
2. Purchase personal data from criminals
3. Use phishing to entice users to willingly give up personal data
4. Install spyware capable of capturing the keystrokes of victims.

1. Data Breach

Date incident was reported	Number of records involved	Organization(s) involved
March 17, 2012	150 million	Shanghai Roadway D&B Marketing Services, Ltd.
January 20, 2009	130 million	Heartland Payment Systems, Tower Federal Credit Union, Beverly National Bank
January 17, 2007	94 million	The TJX Companies
June 1, 1984	90 million	TRW, Sears Roebuck
April 26, 2011	77 million	Sony Corporation
June 19, 2005	40 million	CardSystems, Visa, MasterCard, American Express
December 26, 2011	40 million	Tianya
July 28, 2011	35 million	SK Communications, Nate, Cyworld

Source Line: Open Security Foundation's DataLossDB, http://datalossdb.org.

2. Purchase of Personal Data

- Credit card numbers can be purchased in bulk quantity for as little as $0.40 each
- Logon name and PIN for e-banking can be had for just $10
- A full set of identity information—including date of birth, address, Social Security number, and telephone number—sells for between $1 and $15.

3. Phishing

- Attempt to steal personal identity data
- By tricking users into entering information on a counterfeit Web site
- Spear-phishing - a variation in which employees are sent phony e-mails that look like they came from high-level executives within their organization

4. Spyware

- Keystroke-logging software
- Enables the capture of:
  - Account usernames
  - Passwords
  - Credit card numbers
  - Other sensitive information
- Operates even if an infected computer is not connected to the Internet
- Identity Theft and Assumption Deterrence Act of 1998 was passed to fight fraud

Contents

- ➢ Key Privacy and Anonymity Issues
  - ◇ Identity Theft
  - ◇ Electronic Discovery
  - ◇ Consumer Profiling
  - ◇ Treating Consumer Data Responsibility
  - ◇ Work Place Monitoring
  - ◇ Advanced Surveillance Technology
- ➢ Case Study: Google

Electronic Discovery

- **Discovery** is part of the pretrial phase of a lawsuit in which each party can obtain evidence from the other party by various means, including requests for the production of documents.
- **Electronic discovery (e-discovery)** is the collection, preparation, review, and production of electronically stored information for use in criminal and civil actions and proceedings
  - **Electronically Stored Information:** Emails, drawings, graphs, Web pages, photographs, word-processing files, sound recordings, and databases stored on any form of electronic storage device, including hard drives, CDs, and flash drives.

E-Discovery Software

- Analyze large volumes of ESI quickly to perform early case assessments
- Simplify and streamline data collection from across all relevant data sources in multiple data formats
- Cull large amounts of ESI to reduce the number of documents that must be processed and reviewed
- Identify all participants in an investigation to determine who knew what and when

Contents

- ➢ Key Privacy and Anonymity Issues
  - ◇ Identity Theft
  - ◇ Electronic Discovery
  - ◇ Consumer Profiling
  - ◇ Treating Consumer Data Responsibility
  - ◇ Work Place Monitoring
  - ◇ Advanced Surveillance Technology
- ➢ Case Study: Google

Consumer Profiling

- Companies openly collect personal information about Internet users
- Cookies
  - Text files that a Web site puts on a user's hard drive so that it can remember the information later
  - "Do Not Track" Option in browsers
- Tracking software
- Similar methods are used outside the Web environment
- Databases contain a huge amount of consumer behavioral data

Consumer Profiling (continued)

- Affiliated Web sites
  - Group of Web sites served by a single advertising network
- Customized service for each consumer
- Types of data collected while surfing the Web
  - GET data
  - POST data
  - Click-stream data

Consumer Profiling (continued)

- Four ways **to limit or even stop the deposit of cookies** on hard drives
  - Set the browser to limit or stop cookies
  - Manually delete them from the hard drive
  - Download and install a cookie-management program
  - Use anonymous browsing programs that don't accept cookies

Personalization Software

- Used by marketers to optimize the number, frequency, and mixture of their ad placements
  - Rules-based
  - Collaborative filtering
  - Demographic filtering
  - Contextual commerce

Contents

- ➢ Key Privacy and Anonymity Issues
  - ◇ Identity Theft
  - ◇ Electronic Discovery
  - ◇ Consumer Profiling
  - ◇ Treating Consumer Data Responsibility
  - ◇ Work Place Monitoring
  - ◇ Advanced Surveillance Technology
- ➢ Case Study: Google

Consumer Data Privacy

- Platform for Privacy Preferences (P3P)
  - Shields users from sites that don't provide the level of privacy protection desired

Treating Consumer Data Responsibly

- Strong measures are required to avoid customer relationship problems
- Code of Fair Information Practices
- 1980 OECD privacy guidelines
- Chief privacy officer (CPO)
  - Executive to oversee data privacy policies and initiatives

Manager's Checklist for Treating Consumer Data Responsibly

Question	Yes	No
Does your company have a written data privacy policy that is followed?		
Can consumers easily view your data privacy policy?		
Are consumers given an opportunity to opt in or opt out of your data policy?		
Do you collect only the personal information needed to deliver your product or service?		
Do you ensure that the information is carefully protected and accessible only by those with a need to know?		
Do you provide a process for consumers to review their own data and make corrections?		
Do you inform your customers if you intend to use their information for research or marketing and provide a means for them to opt out?		
Have you identified a person who has full responsibility for implementing your data policy and dealing with consumer data issues?		

Contents

- ➢ Key Privacy and Anonymity Issues
  - ◇ Identity Theft
  - ◇ Electronic Discovery
  - ◇ Consumer Profiling
  - ◇ Treating Consumer Data Responsibility
  - ◇ Work Place Monitoring
  - ◇ Advanced Surveillance Technology
- ➢ Case Study: Google

Workplace Monitoring

- Employers monitor workers
  - Ensures that corporate IT usage policy is followed
- Fourth Amendment cannot be used to limit how a private employer treats its employees
  - Public-sector employees have far greater privacy rights than in the private industry
- Privacy advocates want federal legislation
  - To keeps employers from infringing upon privacy rights of employees

Extent of Workplace Monitoring

Subject of workplace monitoring	Percent of employers that monitor workers	Percent of companies that have fired employees for abuse or violation of company policy
E-mail	43%	28%
Web surfing	66%	30%
Time spent on phone as well as phone numbers called	45%	6%

Contents

- ➢ Key Privacy and Anonymity Issues
  - ◇ Identity Theft
  - ◇ Electronic Discovery
  - ◇ Consumer Profiling
  - ◇ Treating Consumer Data Responsibility
  - ◇ Work Place Monitoring
  - ◇ Advanced Surveillance Technology
- ➢ Case Study: Google

Advanced Surveillance Technology

- Camera surveillance
  - U.S. cities plan to expand surveillance systems
  - "Smart surveillance system"
- Facial recognition software
  - Identifies criminal suspects and other undesirable characters
  - Yields mixed results
- Global Positioning System (GPS) chips
  - Placed in many devices
  - Precisely locate users

Contents

- Key Privacy and Anonymity Issues
  - Identity Theft
  - Electronic Discovery
  - Consumer Profiling
  - Treating Consumer Data Responsibility
  - Work Place Monitoring
  - Advanced Surveillance Technology
- Case Study: Google

Case Study: Google

- Google Street View
  - Find the nine-year-old girl kidnapped
  - A couple from Pennsylvania sued Google for posting photos of their home
  - Users combing through the mapping software came across a number of inappropriate shots
  - Used by pedophiles to find schools, parks, and homes where children live and play
- Google was the first company to extend the expiration of its cookies far into the future (2038) to track users
- Chrome: the company usually collects the user's IP address, the cookie identifier, and the search term

Google vs US Government

- In 2005, the Department of Justice (DOJ) did attempt to gain access to two months' worth of Google's data as part of its attempt to fight child pornography on the Web.

Google refused

1. Google had pledged to keep its users' personal information private and that to hand over data would violate the trust of the users.

2. Google contended that in handing over this data, the company would be forced to reveal trade secrets regarding its search technology.

3. Google questioned whether the reason behind the DOJ's demand was justifiable and in fact lawful

In March 2006, the judge ruled largely in Google's favor, allowing the DOJ access to part of Google's index of sites, but preventing it from accessing search-term data.

Google Docs Privacy Problem

- When one user tried to share a specific document with one additional person, the application shared the document not only with that person but with all the other people with whom the user had ever shared a document.


PRIVACY
is NOT a
CRIME