Chapter 12
Privacy and Digital Security
Privacy

- Right of people to choose freely under what circumstances and to what extent they will reveal themselves, their attitude, and their behavior to others.

- **Threats** to Privacy: **Government** and **business**

- Voluntary Disclosure: Choose to reveal information in return for real benefits (doctor, credit card company)

- Personal information, communication, territory, bodies
Controlling Use of Information

1. **No uses.** Information should be deleted when store is finished

2. **Approval or Opt-in.** Store can use for other purposes with customer's approval

3. **Objection or Opt-out.** Store can use for other purposes if customer does not object

4. **No limits.** Information can be used any way store chooses

5. Fifth possibility is **internal use** - store can use information to continue conducting business with you

**USA: 3 or 4**

**Non-USA: 1 or 2**
Targeted by Target retailer

- **Big Data (data mining)** - statistical analysis of huge information archives
  - Target tracks purchases of loyalty card customers
    - Is a woman pregnant from buying habits?
    - Developed ‘pregnancy prediction’ score by analyzing purchases
  - Potentially dangerous and humiliating invasion of privacy, appears to be within US privacy laws
Cookie Monster

www.nasm.si.edu  FALSE / FALSE  2052246450  CFTOKEN  89367880

• **Cookie:** Record with 7 fields of information uniquely identifying a client’s session across series of independent client/server events. Cookie is stored on client's hard drive.

• **Abuse:** 3rd party cookie
  - 3rd party advertisers on web site enter client/server relationship with customer as page loads
  - Advertiser can set and access cookies when user views other websites that advertiser uses

• **Browser options:**
  - **Turn off** cookies (no online banking)
  - **Ask** each time a server wants to set a cookie
  - **Accept** all cookies

![Figure 12.1 Server’s view of the client/server relationship.](image)
Tracking

- **Tell websites I do not want to be tracked**

History

- Firefox will: **Use custom settings for history**
- **Always use private browsing mode**
  - **Remember my browsing history**
  - **Remember download history**
  - **Remember search and form history**
  - **Accept cookies from sites**
    - **Accept third-party cookies**
      - Keep until: **they expire**
- **Clear history when Firefox closes**

Location Bar

- When using the location bar, suggest: **Bookmarks**
Do Not Track

Table 12.2 Finding the “Do Not Track” Setting In Popular Browsers

<table>
<thead>
<tr>
<th>Browser</th>
<th>Setting Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firefox</td>
<td>Preferences &gt; Privacy</td>
</tr>
<tr>
<td>Internet Explorer</td>
<td>Tools (*) &gt; Safety &gt; Tracking Protection</td>
</tr>
<tr>
<td>Safari (5.1 and later)</td>
<td>Preferences &gt; Advanced &gt; Click “Show Develop menu in menu bar” &gt; Develop</td>
</tr>
</tbody>
</table>

- **Online**
  - Google’s Chrome browser does **not** support user requests **not to track**.
  - Private browsing – client side session cookies/history/cached files deleted (InPrivate:Edge, Incognito: Chrome, Private browsing: Firefox/Safari)

- **Cell Phone**
  - Position, physical location, movements
The Right To Be Forgotten

• Escape your past on-line?
  – Arrest was cleared, minor committed crime (long ago), silly video from college

• Google finds them

• Sources add notation?

• Search engines bury link?

• EU court of justice backed an individual's "right to be forgotten" as part of existing data directive

• France's Commission Nationale de l'Informatique et des Libertés (CNIL) requiring right be applied to Google domains, which Google is fighting
<table>
<thead>
<tr>
<th></th>
<th>Verizon</th>
<th>T-Mobile</th>
<th>AT&amp;T/Cingular</th>
<th>Sprint</th>
<th>Nextel</th>
<th>Virgin Mobile</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Subscriber Information</strong></td>
<td>Post-paid: 3–5 years</td>
<td>5 years</td>
<td>Depends on length of service</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>Unlimited</td>
</tr>
<tr>
<td><strong>Call detail records</strong></td>
<td>1 rolling year</td>
<td>Pre-paid: 2 years, Post-paid: 5 years</td>
<td>Pre-paid: varies, Post-paid: 5–7 years</td>
<td>18–24 months</td>
<td>18–24 months</td>
<td>2 years</td>
</tr>
<tr>
<td><strong>Cell towers used by phone</strong></td>
<td>1 rolling year</td>
<td>Officially 4–6 months, really a year or more.</td>
<td>From July 2008</td>
<td>18–24 months</td>
<td>18–24 months</td>
<td>Not retained — obtain through Sprint</td>
</tr>
<tr>
<td><strong>Text message detail</strong></td>
<td>1 rolling year</td>
<td>Pre-paid: 2 years, Post-paid: 5 years</td>
<td>Post paid: 5–7 years</td>
<td>18 months (depends on device)</td>
<td>18 months (depends on device)</td>
<td>60–90 days</td>
</tr>
<tr>
<td><strong>Text message content</strong></td>
<td>3–5 days</td>
<td>Not retained</td>
<td>Not retained</td>
<td>Not retained</td>
<td>Not retained</td>
<td>90 days (search warrant required with “text of text” request)</td>
</tr>
<tr>
<td><strong>Pictures</strong></td>
<td>Only if uploaded to Web site (customer can add or delete pictures any time)</td>
<td>Can be stored online and are retained until deleted or service is canceled</td>
<td>Not retained</td>
<td>Contact provider</td>
<td>Contact provider</td>
<td>Not retained</td>
</tr>
<tr>
<td><strong>IP session information</strong></td>
<td>1 rolling year</td>
<td>Not retained</td>
<td>Only retained on non-public IPs for 72 hours. If public IP, not retained.</td>
<td>60 days</td>
<td>60 days</td>
<td>Not retained</td>
</tr>
<tr>
<td><strong>IP destination information</strong></td>
<td>90 days</td>
<td>Not retained</td>
<td>Only retained on non-public IPs for 72 hours. If public IP, not retained.</td>
<td>60 days</td>
<td>60 days</td>
<td>Not retained</td>
</tr>
<tr>
<td><strong>Bill copies (post-paid only)</strong></td>
<td>3–5 years, but only last 12 months readily available</td>
<td>Not retained</td>
<td>5–7 years</td>
<td>7 years</td>
<td>7 years</td>
<td>n/a</td>
</tr>
<tr>
<td><strong>Payment history (post-paid only)</strong></td>
<td>3–5 years, check copies for 6 months</td>
<td>5 years</td>
<td>Depends on length of service</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>n/a</td>
</tr>
<tr>
<td><strong>Store Surveillance Videos</strong></td>
<td>Typically 30 days</td>
<td>2 weeks</td>
<td>Depends. Most stores carry for 1–2 months</td>
<td>Depends</td>
<td>Depends</td>
<td>n/a</td>
</tr>
<tr>
<td><strong>Service Applications</strong></td>
<td>Post-paid: 3–5 years</td>
<td>Not retained</td>
<td>Not retained</td>
<td>Depends</td>
<td>Depends</td>
<td>Not retained</td>
</tr>
</tbody>
</table>
Government, as Usual

• June 2013, Edward Snowden revealed:
  • U.S. government collecting complete metadata phone carrier records
  • Unknown if allegations are true?
  • Collecting online activity from Facebook, Microsoft, Google, …
  • Included data to calls to other countries with OECD laws in place
• EU issued EDPD (European Data Protection Directive) benchmark law incorporating OECD principles
  • Data about EU citizens be protected by standards of law when it leaves their country
• Patriot Act - crime to say data gathering is occurring
Identity Theft

• Crime of posing as someone else for fraudulent purposes

• Using information about person like credit card numbers, social security numbers

• Americans do not enjoy Security Principle of the Fair Information Practices
  – Those who hold private information are obligated to maintain its privacy against unauthorized access and other hazards
Computer Security: The Risks

• **Mischief**: Infecting a computer, causing a nuisance, erasing files, trashing files, etc.

• **Information theft**: Stealing personal information

• **Spying**: Surreptitiously recording videos of user, logging keystrokes, compromising secure online activities

• **Resource theft**: Taking over a computer
Figure 12.1 Data Privacy Map


Comparison of privacy and data protections by country.
Manage your Privacy

• Purchase up-to-date virus checking software
• Adjust cookie preferences to match your comfort level
• Read privacy statement of any website before you give it information
• Review protections against phishing scams
• Patronize reputable companies for music, software, etc.
• Be skeptical
• Stay familiar with current assaults on privacy: epic.org
• Lobby for US adoption of OECD’s Fair Information Practices
  - data controller (person/office setting policies) must interact with individuals about their information, and must be accountable for those policies and actions
<table>
<thead>
<tr>
<th>Limited Collection</th>
<th>There should be limits to the personal data collected; data should be collected by fair and lawful means, and with the knowledge and consent of the person whenever possible.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>The purposes for collecting personal data should be stated when it is collected; the uses should be limited to those purposes.</td>
</tr>
<tr>
<td>Quality</td>
<td>The data should be relevant to the purpose of collection; it should be accurate, complete, and up-to-date.</td>
</tr>
<tr>
<td>Use Limitation</td>
<td>Personal data should not be disclosed or used for purposes other than stated in the Purpose Principle, except with the consent of the individual or by the authority of law.</td>
</tr>
<tr>
<td>Security</td>
<td>Personal data should be protected by reasonable security measures against risks of disclosure, unauthorized access, misuse, modification, destruction, or loss.</td>
</tr>
<tr>
<td>Openness</td>
<td>There should be general openness of policies and practices about personal data collection, making it possible to know of its existence, kind, and purpose of use, as well as the contact information for the data controller.</td>
</tr>
<tr>
<td>Participation</td>
<td>An individual should be able to (a) determine if the data controller has information about him or her, and (b) discover what it is. If the request is denied, the individual should be allowed to challenge the denial.</td>
</tr>
<tr>
<td>Accountability</td>
<td>The data controller should be accountable for complying with these principles.</td>
</tr>
</tbody>
</table>
Malware — Software harms computers

- **Virus**: “hides” in shared program (i.e. game), “reproduces” itself, and inserts code to “execute” (i.e. boot sector)
- **Worm**: “reproduce” itself and sends copy to contact list (often embedded in email attachment)
- **Trojan**: hides inside another useful program, and performs secret operations (keyloggers, ransomware, bankers)
- **Exploit**: takes advantage of security hole (Backdoor access enters computer and reconfigures for remote control)
  - Uses your computer/Internet connection, send spam, or other practices (zombie: compromised computer)
  - Grab secure information from your computer (passwords, account numbers, …)
<table>
<thead>
<tr>
<th>File Extension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.386</td>
<td>Virtual Device Driver (Windows 386 enhanced mode)</td>
</tr>
<tr>
<td>.3gr</td>
<td>VGA Graphics Driver/configuration files</td>
</tr>
<tr>
<td>.add</td>
<td>Adapter Driver file</td>
</tr>
<tr>
<td>.ade</td>
<td>Microsoft Access project extension</td>
</tr>
<tr>
<td>.asp</td>
<td>Active Server Page</td>
</tr>
<tr>
<td>.bas</td>
<td>Microsoft Visual Basic class module</td>
</tr>
<tr>
<td>.bat</td>
<td>Batch file</td>
</tr>
<tr>
<td>.chm</td>
<td>Compiled HTML Help file</td>
</tr>
<tr>
<td>.cmd</td>
<td>Microsoft Windows NT command script</td>
</tr>
<tr>
<td>.com</td>
<td>Microsoft MS-DOS program</td>
</tr>
<tr>
<td>.cpl</td>
<td>Control Panel extension</td>
</tr>
<tr>
<td>.crt</td>
<td>Security certificate</td>
</tr>
<tr>
<td>.dbx</td>
<td>Database Index</td>
</tr>
<tr>
<td>.dll</td>
<td>Dynamic Link Library</td>
</tr>
<tr>
<td>.exe</td>
<td>Program file</td>
</tr>
<tr>
<td>.fon</td>
<td>Font file</td>
</tr>
<tr>
<td>.hlp</td>
<td>Help file</td>
</tr>
<tr>
<td>.hta</td>
<td>HTML program</td>
</tr>
<tr>
<td>.inf</td>
<td>Setup information</td>
</tr>
<tr>
<td>.ins</td>
<td>Internet Naming Service</td>
</tr>
<tr>
<td>.isp</td>
<td>Internet communication settings</td>
</tr>
<tr>
<td>.js</td>
<td>JavaScript file</td>
</tr>
<tr>
<td>.jse</td>
<td>JavaScript encoded-script file</td>
</tr>
<tr>
<td>.lnk</td>
<td>Shortcut</td>
</tr>
<tr>
<td>.mdb</td>
<td>Microsoft Access program</td>
</tr>
<tr>
<td>.mde</td>
<td>Microsoft Access MDE database</td>
</tr>
<tr>
<td>.msc</td>
<td>Microsoft Common Console document</td>
</tr>
<tr>
<td>.msi</td>
<td>Microsoft Windows Installer package</td>
</tr>
<tr>
<td>.msp</td>
<td>Microsoft Windows Installer patch</td>
</tr>
<tr>
<td>.mst</td>
<td>Microsoft Windows Installer transform</td>
</tr>
<tr>
<td>.ocx</td>
<td>Microsoft Object Linking</td>
</tr>
<tr>
<td>.pcd</td>
<td>Corel Adaptec CD Creator image file</td>
</tr>
<tr>
<td>.pif</td>
<td>Shortcut to MS-DOS program</td>
</tr>
<tr>
<td>.reg</td>
<td>Registration entries</td>
</tr>
<tr>
<td>.scr</td>
<td>Screen saver</td>
</tr>
<tr>
<td>.sct</td>
<td>Windows Script Component</td>
</tr>
<tr>
<td>.shb</td>
<td>Shell Scrap object</td>
</tr>
<tr>
<td>.shs</td>
<td>Shell Scrap object</td>
</tr>
<tr>
<td>.url</td>
<td>Internet shortcut</td>
</tr>
<tr>
<td>.vb</td>
<td>Visual Basic Script file</td>
</tr>
<tr>
<td>.vbe</td>
<td>Visual Basic Script-encoded file</td>
</tr>
<tr>
<td>.vbs</td>
<td>Visual Basic Script file</td>
</tr>
<tr>
<td>.vxd</td>
<td>Microsoft Windows Virtual Device Driver</td>
</tr>
<tr>
<td>.wsc</td>
<td>Windows Script Component</td>
</tr>
<tr>
<td>.wsf</td>
<td>Windows Script File</td>
</tr>
<tr>
<td>.wsh</td>
<td>Windows Script Host Settings file</td>
</tr>
</tbody>
</table>
Prevention: Safe Computing Checklist

- Turn off Bluetooth when not in use
- Keep phone and other computers locked
- Do not automatically click on email attachments
- Avoid entering sensitive information in a pop-up
- Is it really FREE? Think again (download)
- Know where URL is going
- Be somewhat skeptical
- Careful visiting notorious sites (sports, music…)
- Use two-factor authentication:
  (password + physical key or biometric)
Bad Happens

• **Turn off** computer/phone **immediately**

• Use a different computer to search symptoms, kind of site

• Use **external source** (CD/USB) for OS to reboot
Plan of Action

• What to do?
  1. Run current versions of software
  2. Install protective systems
     a) Updates when available
     b) Anti-virus SW (current)
  3. Set installed protections
     a) “Do Not Track” flag
     b) Wi-Fi router to security level of at least WPA2
     c) Password-protect phones/computers
  4. Beware to avoid difficulties
     a) Install only GOOD software
     b) Caution with attachments
     c) Password Protection
<table>
<thead>
<tr>
<th>Cleartext</th>
<th>Key</th>
<th>Cipher Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>Me</td>
<td>0100 1101</td>
<td>0101 1010 0100 1000</td>
</tr>
<tr>
<td>et</td>
<td>0110 0101</td>
<td>rY</td>
</tr>
<tr>
<td>@1</td>
<td>0100 0000</td>
<td>WFs</td>
</tr>
<tr>
<td>2:</td>
<td>0011 0010</td>
<td>0010 0101 0001 0111</td>
</tr>
<tr>
<td>15</td>
<td>0011 0001</td>
<td>%E Σ</td>
</tr>
<tr>
<td>@J</td>
<td>0100 0000</td>
<td>&amp;C N</td>
</tr>
<tr>
<td>oe</td>
<td>0110 1111</td>
<td>Wg</td>
</tr>
<tr>
<td>'s</td>
<td>0010 0111</td>
<td>xH</td>
</tr>
</tbody>
</table>

\[ 2: \oplus 0001 = 0010 \]

Figure 17.3. Encrypting the cleartext Meet@12:15@Joe's, using ASCII encoding of letter pairs, the key 0001 0111 0010 1101, and the operation of exclusive OR to produce the cipher text zHrYWFs%E Σ&CN WgxH0_.

(Decryption works in the opposite direction, as if the “⊕” and “=” symbols of the figure were exchanged.)
Simple Encryption Process

1) Convert into ASCII decimal www.branah.com/ascii-converter

   MEET @ 9
   77 69 69 84 32 64 32 57

2) Group into pairs, **multiply** each pair by **key**, 13:

   7769 \times 13 = 100997
   6984 \times 13 = 090792
   3264 \times 13 = 042432
   3257 \times 13 = 042341  \text{ (leading zeros make all numbers six digits.)}

3) Send products— 100997 090792 042432 042341 —to receiver

4) Receiver **divides** by the **key**, 13:

   100997/13 = 7769
   090792/13 = 6984
   042432/13 = 3264
   042341/13 = 3257

   and types in digits 77 69 69 84 32 64 32 57
to www.branah.com/asciiconverter program to get ASCII: MEET @ 9.

5) Finally, message is reassembled to original **cleartext**, MEET @ 9.
Figure 12.4 Schematic diagram of a cryptosystem. Using a key $K_{SR}$ known only to them, the sender encrypts the cleartext information to produce a cipher text, and the receiver decrypts the cipher text to recover the cleartext. In the middle, where the content is exposed and can be snooped, it is unintelligible.
RSA Public Key Cryptosystem

- Relies on prime numbers
- Any number factored into primes in only one way
- Choosing a Key:
  - Key has special properties
    - Must be the product of two different prime numbers, \( p \) and \( q \)
    - \( p \) and \( q \) must be about 64 or 65 digits long to produce a 129-digit public key
    - \( p \) and \( q \) must also be 2 greater than a multiple of 3
Encryption and Decryption

• **Encryption**: Transform to be no longer understandable

• **Decryption**: Reversing encryption process

• **Cryptosystem**: Combination of encryption and decryption methods

• **Cleartext** or **Plaintext**: Information before encryption

• **Cipher text**: Information in encrypted form

• **One-way cipher**:
  • Encryption system that cannot be easily reversed (used for passwords)
Backing Up a Personal Computer

• How and **What** to **Back Up**
  – Automatic backup software writes to external hard disk or “cloud”
  – Full/Partial backups (all / changes since full)
  – Manual backup
    – **Can be re-created** from some permanent source, like software (sent email copied and saved)
    – **Was saved** before but has not changed
    – **You don’t care** about
    – Evidence, email (sent folder, server, recipient)