Digital Footprints
The Web, Social Media, and your privacy!
### ASCII Table

<table>
<thead>
<tr>
<th>Decimal</th>
<th>ASCII</th>
<th>Character</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0000</td>
<td>U</td>
<td></td>
</tr>
<tr>
<td>0001</td>
<td>L</td>
<td></td>
</tr>
<tr>
<td>0010</td>
<td>!</td>
<td></td>
</tr>
<tr>
<td>0011</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0100</td>
<td>@</td>
<td></td>
</tr>
<tr>
<td>0101</td>
<td>P</td>
<td>R</td>
</tr>
<tr>
<td>0110</td>
<td>~</td>
<td>a</td>
</tr>
<tr>
<td>0111</td>
<td>p</td>
<td></td>
</tr>
<tr>
<td>1000</td>
<td>b</td>
<td></td>
</tr>
<tr>
<td>1001</td>
<td>d</td>
<td></td>
</tr>
<tr>
<td>1010</td>
<td>a</td>
<td></td>
</tr>
<tr>
<td>1011</td>
<td>o</td>
<td></td>
</tr>
<tr>
<td>1100</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>1101</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td>1110</td>
<td>á</td>
<td></td>
</tr>
<tr>
<td>1111</td>
<td>ò</td>
<td></td>
</tr>
</tbody>
</table>
UTF-8: When ASCII just isn't enough

- UTF (Uniform Transformation Format): a variable-width encoding that can represent every character in the Unicode Character Set
- 1,112,064 of them!!!
- UTF-8 is the dominant character encoding on the Web, required to be supported by all browsers
- Yes it includes a character for pile of poo... U+1F4A9
Key ideas from last time

- Computational Thinking
  - Functional abstraction
  - Subroutines (F1 and F2 help out)

- Representing data in computers
  - Bits, bytes, ASCII, UTF-8
    - Maybe everything can be represented with bits...
  - Presence or Absence of signal
    - mechanical, electrical, color, light, blinking an eye, finger up/down, yes/no, true/false, 0/1
  - Hollerith tabulating machine => transistors
Digital Footprints
The Web, Social Media, and your privacy!
Blown to Bits: Chapter 2
1984 is here and we like it
Name three cases of information going viral that could never have happened 15 years ago.
Privacy: definitions

• **Privacy**: The condition of being free from being observed by other people
  - But this is never true any more...

• **Privacy**: The right of people to choose under what circumstances and to what extent they reveal themselves, their attitude, and their behavior to others
  - Individuals choose what data to reveal, how it can be used
  - Penalties for misuse
Principles of Fair Information Practice

- **Openness**
  - No programs whose existence is secret
- **Disclosure**
  - You can find out what information they know about you
- **Secondary use**
  - They can only use the data as you originally agreed
- **Correction**
  - You can correct bad information about yourself
- **Security**
  - Collectors of data responsible for securing it properly
Technology doesn't violate privacy

- People violate privacy
  - Technology just makes it easier/faster/scaled up
Who is making money from your data?
Who is making money from your data?

- Google
- Facebook
- Amazon
- Netflix
What are you supposed to learn?

• What is a digital footprint?
• What technology advances in the last 10 years have made “Big Brother” possible
• Which organizations try to protect your privacy
• Why you should read the terms and conditions for apps you download
  – Never know what they will say.
    • Pulse asks you to give permission to track every number you call
    • Pandora asks you for permission to retrieve all your contacts
    • Angry Birds tracks your location using GPS while you play
• Why you should consider what you put on public sites like Facebook
  – Are you sure your privacy settings are as you want them?
What is your digital footprint?

- Where are you revealing stuff you'd rather not have open to the world?
  - Facebook
  - Credit card information
  - Cooking
  - Purchases
  - Embarrassing stuff
  - Porn download tracking
  - Location information
  - Google search history
  - Email contents
  - Apps you buy
How did we get here?
Integrated circuits

NVIDIA GK110
7.1 billion transistors

cheaper fabrication
greater complexity
miniaturization
Chips for everyone!
First: Allows personal computers

- Ken Olsen (founder of DEC)
  - “There is no reason for any individual to have a computer in their home” (1977)

- Xerox Star, 1981, first PC, mouse [failed]

- Apple Macintosh
  - First commercially successful personal computer with a mouse and graphical interface
Next: Smaller ICs => Phones
The Internet

- Invented in 1969 for military purposes (took 20 years to get out of lab)
- Started with ASCII terminal interface
  - FTP (file transfer protocol), Gopher
Connectivity Changes the World

General mechanism to communicate digital data – doesn't matter what it is.
Early 90s: WWW + http

- World Wide Web: An interface for humans!
- All computers 'speak' a common language:
  - hyper-text transport protocol (HTTP)
- Content points to other content
  - Links! (PageRank comes later)
  - UTF allows any language
Everything we know is online

- Newspapers
- Scientific articles
- Books
- Encyclopedias (Wikipedia)
- Dictionaries and Thesauruses
- Art
Why the WWW is so brilliant

- WWW = the servers + the data
- All computers use one standard protocol (HTTP)
  - Everyone can communicate
- Publishing and accessing information is decentralized
  - No limits on what is possible to say or search for
- Critical mass of data
Seeing Other People's Data

WWW exploits one protocol, neutralizes differences at endpoints
Digital Footprint

- Digital Footprint
  - Where you go, what you do on web
  - “Data trail left by interactions in a digital environment”
  - Visits to webpages
  - What you clicked on
  - Search terms
  - Location, IP address
  - Comments made

- Allows data mining, profiling
  - Recommendations, personalisation, offers, contextual adaptation
Footprint Example: Harry Potter leak

- Photos of all 759 pages of U.S. edition of *Deathly Hallows* leaked online prior to release
- Scholastic investigates source
- Photos contained EXIF metadata
  - including serial number of camera used (Canon Rebel)
Boston Marathon Bombing
Boston Marathon bombing suspects caught on camera, FBI seeks help in identifying them

Two suspects have been narrowed down but their identities remain unknown. FBI hopes the public can help locate the two men who experts believe may be homegrown terrorists.

BY MARK MORALES IN BOSTON AND DANIEL BECKMAN AND LARRY MCGHANE / NEW YORK DAILY NEWS
PUBLISHED: THURSDAY, APRIL 18, 2013, 10:23 AM
UPDATED: FRIDAY, APRIL 19, 2013, 2:46 AM
People turned to social media over traditional news outlets.

Police scanners broadcast online.

Several suspects wrongfully accused on Twitter, 4Chan, Reddit, blogs, traditional news agencies

“Activity on Reddit fueled online witch hunts and dangerous speculation which spiraled into very negative consequences for innocent parties. The Reddit staff and the millions of people on Reddit around the world deeply regret that this happened.”

– Erik Martin

(No other news organizations apologized for spreading false accusations)
So how did we get here?

- IC
  - Cheap
  - Personal
  - Miniaturization
- Internet, WWW
- Digitization of content
- Mobile

Same technology that is amazing and useful and fun and affordable also enables Big Brother.
It's easier than you think for your privacy to be violated without you knowing it.
Thanks to its unrivalled App Store, the iPhone can record your guitar playing, order your shopping for you and even check your blood pressure. The iPhone 4S (or the iPhone 4, if you're naughty) will do practically anything you want, simply by shouting at it.

One thing it won't do, however, which has left many iPhone adopters flummoxed, is record phone calls—a task that some mobiles, such as the venerable Sony Ericsson K850i, have managed with ease since 2007.
Your phone records where you've been, who you've called


- Apple's iPhone:
  - Periodically saves location data to secret file on device
  - Data backed up to laptop during sync
  - Started with iOS 4 (2010)

- Implication
  - anyone with physical access to your iPhone or laptop can track everywhere you've been in the last 4 years
Cell phone mics and cameras can be remote activated

FBI taps cell phone mic as eavesdropping tool

REPORT: THE NSA CAN SECRETLY ACTIVATE AN IPHONE’S MICROPHONE, CAMERA... AND THAT’S NOT ALL

The National Security Agency can remotely activate an iPhone’s camera and microphone without the user knowing, according to a leaked document obtained by German news magazine Der Spiegel.

Related: Apple, NSA
Mobile Monitor: a scary app!

Who is protecting privacy?

- American Civil Liberties Union (ACLU)
- Electronic Privacy Information Center (EPIC)
- Electronic Frontier Foundation (EFF)

Law and policy evolve rapidly:
- New technology
- New surprising privacy developments come to light
Edward Snowden

- Revealed widespread operations of the NSA to collect data on everyone in the world
- Revealed that government is collecting metadata from major phone companies
- NSA PRISM, XKeyscore, Tempora, Evil Olive programs
  - Direct access to Microsoft, Google, Facebook, Apple servers
  - Hacked internet backbones in Beijing, Hong Kong
  - Britain's GCHQ involved
  - 1 billion cell calls tracked every day

Hero or enemy?
Are you revealing only what you want to reveal?
Facebook Privacy Policy circa 2005:
No personal information that you submit to Thefacebook will be available to any user of the Web Site who does not belong to at least one of the groups specified by you in your privacy settings.

Facebook Privacy Policy circa 2006:
We understand you may not want everyone in the world to have the information you share on Facebook; that is why we give you control of your information. Our default privacy settings limit the information displayed in your profile to your school, your specified local area, and other reasonable community limitations that we tell you about.
Facebook Privacy Policy circa 2007:

Profile information you submit to Facebook will be available to users of Facebook who belong to at least one of the networks you allow to access the information through your privacy settings (e.g., school, geography, friends of friends). Your name, school name, and profile picture thumbnail will be available in search results across the Facebook network unless you alter your privacy settings.
Facebook Privacy Policy circa Nov. 2009:
Facebook is designed to make it easy for you to share your information with anyone you want. You decide how much information you feel comfortable sharing on Facebook and you control how it is distributed through your privacy settings. You should review the default privacy settings and change them if necessary to reflect your preferences. You should also consider your settings whenever you share information. ...

Information set to “everyone” is publicly available information, may be accessed by everyone on the Internet (including people not logged into Facebook), is subject to indexing by third party search engines, may be associated with you outside of Facebook (such as when you visit other sites on the internet), and may be imported and exported by us and others without privacy limitations. The default privacy setting for certain types of information you post on Facebook is set to “everyone”. You can review and change the default settings in your privacy settings.
Facebook Privacy Policy circa Dec. 2009:
Certain categories of information such as your name, profile photo, list of friends and pages you are a fan of, gender, geographic region, and networks you belong to are considered publicly available to everyone, including Facebook-enhanced applications, and therefore do not have privacy settings. You can, however, limit the ability of others to find this information through search using your search privacy settings.
Facebook Privacy Policy circa 2010:

When you connect with an application or website it will have access to General Information about you. The term General Information includes your and your friends' names, profile pictures, gender, user IDs, connections, and any content shared using the Everyone privacy setting. ... The default privacy setting for certain types of information you post on Facebook is set to “everyone”. ... Because it takes two to connect, your privacy settings only control who can see the connection on your profile page. If you are uncomfortable with the connection being publicly available, you should consider removing (or not making) the connection.
Are you revealing only what you want to reveal?
Girls Around Me is a revolutionary new city scanner app that turns your town into a dating paradise. Use it to see where hot girls and guys are hanging out in your area, view their photos and make contact!

NOTE: You need to have a Foursquare account to use Girls Around Me!

Create foursquare account
The iPhone's Fingerprint Scanner Has Shady Government Ties, Anonymous Says

By Patrick McGuire

Yesterday, just as the US government shut itself down and put 800,000 people temporarily out of work, the hacktivist group Anonymous—who the FBI wrongly declared to be dead in August—released a video statement with an accompanying Pastebin document claiming that there are definitive links between AuthenTec, the company that developed the iPhone 5S's fingerprint scanner, and the US government.
What are you supposed to learn?

- What is a digital footprint?
- What technology advances in the last 10 years have made “Big Brother” possible
- Which **organizations** try to protect your privacy
- Why you should read the **terms and conditions** for apps you download
  - Never know what they will say.
    - *Pulse* asks you to give permission to **track every number you call**
    - *Pandora* asks you for permission to **retrieve all your contacts**
    - *Angry Birds* **tracks your location** using GPS while you play
- Why you should consider what you put on public sites like Facebook
  - Are you sure your privacy settings are as you want them?
End