Voluntary Disclosures
Give-Aways

- Not all privacy problems are due to evil social networking sites and web sites
- Some information is given away
- People don’t always realize the consequences of what they say online
War 2.0

“Israel’s Army Radio reported on Wednesday that a raid on suspected militants in the West Bank planned for Wednesday was called off by the country’s military because a soldier posted details of the operation on Facebook.

“The Israeli newspaper Haaretz explained that the soldier posted a status update letting friends know that his unit was preparing to go to a West Bank village near Ramallah: ‘On Wednesday we clean up Qatanah, and on Thursday, god willing, we come home,’ the soldier wrote.”
Inappropriate Publications Aren’t New

- During World War II, the *Chicago Tribune* published a story suggesting that the U.S. was reading Japan’s naval codes — which was true...
- (The Japanese never saw the story)
- What’s different now?
The Difference

- No gatekeeper
- No single person to hold accountable (Roosevelt wanted to use the Marines to shut down the *Chicago Tribune* and/or wanted to charge the publisher with treason)
- Accessible from anywhere in the world
- It’s the same things that make Web 2.0 useful for other reasons—publishing is now rapid and decentralized
Usenet

- The decentralized publication problem started with Usenet
- People engaged in discussions would often post proprietary material
- Most companies required preclearance for publication—but was Usenet “publishing” or “talking with friends”? 
- The social dynamic was the latter, but what was posted was rapidly distributed worldwide.
The Web Made it Worse

- Inappropriate content was now permanent
- Search engines could find it
- Better yet—search engines could find corporate markings for proprietary documents
  - Search for phrases like “IBM Confidential” or “AT&T Proprietary”
- Home in on the good stuff...
Unofficial Collaboration Channels

- Often, official mechanisms for sharing data don’t work well
- Simple solution: put the files on a web site and *assume* that no one else will see them
- But web servers will auto-list directories and search engines can find things...
# Autolisting Directories

## Index of /~smb/foo

<table>
<thead>
<tr>
<th>Name</th>
<th>Last modified</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent Directory</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>test1.txt</td>
<td>08-Mar-2010 22:44</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>test2.txt</td>
<td>08-Mar-2010 22:44</td>
<td>7</td>
<td></td>
</tr>
</tbody>
</table>

Peer-to-Peer Filesharing

- Peer-to-peer file-sharing programs are designed to share files with minimal effort
- But what files?
- The goal—let’s be honest—was to share MP3s and movies
- Some programs’ default configuration shared all file types in certain directories.
- Do people put their music in My Documents?
Apparently, Some Do…

- Empirically, we do see documents on file-sharing networks
- The FTC notified about 100 organizations that sensitive customer and employee data was being shared that way
- “They might accidentally choose to share drives or folders that contain sensitive information, or they could save a private file to a shared drive or folder by mistake, making that private file available to others. In addition, viruses and other malware can change the drives or folders designated for sharing, putting private files at risk. As a result, instead of just sharing music, a user’s personal tax returns, private medical records or work documents could end up in general circulation on P2P networks.” (FTC)
A New Law?

- Congress considered a bill to require warnings about P2P programs
- Program must provide “clear and conspicuous notice that such program allows files on the protected computer to be made available for searching by and copying to one or more other computers”
- Such programs must not make themselves unduly hard to remove
You Can’t Call it Back

- Once something is on the Net, it’s probably there forever
- Email with the text “XXX wishes to recall the message "YYYY"” is ineffective on anything other than Microsoft Exchange
- In fact, it only draws more attention to the message...
Sexting

- People—not frequently teenage girls—take “suggestive” photos of themselves with their phones and send them to their (boy)friends
- (It’s not just teenage girls—don’t forget Anthony Weiner and his antics)
- The recipients display lots of class and circulate the pictures to several dozen of their closest, most trusted friends
- These “friends”, of course, share them further
- One result in several jurisdictions: threatened or actual child pornography charges
- Also: revenge porn
It’s Not Just Teens

- In 2001, a British attorney at a large multinational law firm forwarded a complimentary—but extremely intimate—email from his girlfriend, because he wanted to brag about his “attributes”
- One of his friends sent it further, saying that he felt “honour bound” to redistribute it
- The email rapidly became very public
- The attorney was fired; several of the forwarders were disciplined
What Happened?

- Imagine a wandering bard, spreading a “naughty” rumor wherever he goes
- Imagine a monk in a scriptorium making several copies of such stories and sending them out by courier
- Someone takes a letter to the copier room, makes lots of copies, and mails them
- What is the bandwidth in recipients/second?
- A qualitative difference in speed has become a qualitative difference
Can We Create Time-Limited Email?

- General approach: encrypt the email with some key; destroy the key after a certain interval
- To read the email, the recipient first has to either retrieve the key or upload the mail to a decryption server
- In either case, the message is displayed on the recipient’s screen, which can be copied
- If nothing else, the recipient can use another device to photograph the screen
- Yes, that’s true of Snapchat...
The Converse Problem

- On the other hand, creating a message which can’t be read until a certain time is (in principle) easy
- Launch satellites with private cryptographic keys into the L4 and L5 Earth-Sun Lagrange points
- Multiply-encrypt the message, alternating between the public keys for each of the two satellites
- Each leg—they’re 8 light-minutes from earth, and 13.86 light-minutes apart—can do one decryption; there’s no way to talk faster than the speed of light
Social Networks

- Facebook et al. are personal places
- People post things about themselves and their friends
- Such postings can follow them around
What’s the Problem?

- Secondary use—personal data is being used when judging employment suitability
- Persistence of data—data has a long lifetime
- The “Wayback Machine”: www.archive.org
# The Wayback Machine

<table>
<thead>
<tr>
<th>Date</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 11, 2005</td>
<td>*</td>
</tr>
<tr>
<td>Jan 11, 2005</td>
<td>*</td>
</tr>
<tr>
<td>Feb 12, 2005</td>
<td>*</td>
</tr>
<tr>
<td>Feb 12, 2005</td>
<td>*</td>
</tr>
<tr>
<td>Mar 09, 2005</td>
<td></td>
</tr>
<tr>
<td>Sep 07, 2005</td>
<td>*</td>
</tr>
<tr>
<td>Sep 10, 2005</td>
<td></td>
</tr>
<tr>
<td>Sep 14, 2005</td>
<td></td>
</tr>
<tr>
<td>Sep 17, 2005</td>
<td></td>
</tr>
<tr>
<td>Sep 23, 2005</td>
<td></td>
</tr>
<tr>
<td>Oct 18, 2005</td>
<td></td>
</tr>
<tr>
<td>Oct 28, 2005</td>
<td></td>
</tr>
<tr>
<td>Nov 09, 2005</td>
<td>*</td>
</tr>
<tr>
<td>Dec 03, 2005</td>
<td>*</td>
</tr>
<tr>
<td>Dec 10, 2005</td>
<td></td>
</tr>
<tr>
<td>Dec 12, 2005</td>
<td></td>
</tr>
<tr>
<td>Dec 31, 2005</td>
<td></td>
</tr>
<tr>
<td>Jan 01, 2006</td>
<td></td>
</tr>
<tr>
<td>Jan 02, 2006</td>
<td></td>
</tr>
<tr>
<td>Jan 09, 2006</td>
<td></td>
</tr>
<tr>
<td>Feb 09, 2006</td>
<td></td>
</tr>
<tr>
<td>Apr 25, 2006</td>
<td></td>
</tr>
<tr>
<td>Jun 19, 2006</td>
<td></td>
</tr>
<tr>
<td>Aug 20, 2006</td>
<td></td>
</tr>
<tr>
<td>Aug 30, 2006</td>
<td></td>
</tr>
<tr>
<td>Aug 31, 2006</td>
<td></td>
</tr>
<tr>
<td>Sep 01, 2006</td>
<td></td>
</tr>
<tr>
<td>Sep 07, 2006</td>
<td>*</td>
</tr>
<tr>
<td>Sep 07, 2006</td>
<td>*</td>
</tr>
<tr>
<td>Sep 11, 2006</td>
<td>*</td>
</tr>
<tr>
<td>Sep 20, 2006</td>
<td></td>
</tr>
<tr>
<td>Sep 21, 2006</td>
<td>*</td>
</tr>
<tr>
<td>Sep 21, 2006</td>
<td>*</td>
</tr>
<tr>
<td>Sep 23, 2006</td>
<td></td>
</tr>
<tr>
<td>Sep 24, 2006</td>
<td></td>
</tr>
<tr>
<td>Oct 17, 2006</td>
<td></td>
</tr>
<tr>
<td>Dec 10, 2006</td>
<td></td>
</tr>
<tr>
<td>Feb 05, 2007</td>
<td></td>
</tr>
<tr>
<td>May 03, 2007</td>
<td></td>
</tr>
<tr>
<td>May 05, 2007</td>
<td></td>
</tr>
<tr>
<td>May 08, 2007</td>
<td></td>
</tr>
<tr>
<td>Jun 09, 2007</td>
<td>*</td>
</tr>
<tr>
<td>Aug 19, 2007</td>
<td>*</td>
</tr>
</tbody>
</table>
More Subtle Leaks

- Association patterns leak
- “Birds of a feather...”
- Democrats (mostly) friend Democrats, Republicans (mostly) friend Republicans, gays mostly friend gays, etc.
- An MIT study showed that gay males had many more openly gay Facebook friends than did straight males—and that this could be used to identify the sexuality of closeted men.
Protecting Facebook Data

• Facebook has elaborate privacy controls
• Many people are unaware of them
• They’re not easy to use well—there’s a serious usability problem
• Facebook says that 20M users changed some settings—at a time when they had 350M users
• One nice feature: it’s possible to see how anyone on your friend list will see your profile
They Keep Changing Things

- Facebook frequently changes its policies and mechanisms
- New defaults are more open
- This is a conscious decision by Facebook, which thinks that people want more openness
- Also: how will Facebook make money?
EXIF Tags

- JPGs contain a lot of metadata
- Some is about the photo:
  Exposure Time: 1/60 sec
  F-Number: f/4.5
  Exposure Program: Not Defined
  Exposure Bias: 0 EV
  Metering Mode: Pattern
  Light Source: Unknown
  Flash: Flash, Auto, Return Detected
  Focal Length: 44.00 mm
- But it can also include the camera model and serial number and GPS location
A Lunar Eclipse

(Photo by Matt Blaze)
Some of the Metadata

Altitude 22 m (72.18 ft)
Altitude Reference above sea level
Date Stamp Dec 21, 2010
GPS Version 2.2.0.0
Latitude 39° 57’ 36.042” N
Longitude 75° 9’ 32.808” W
Satellites 08
Time Stamp 07:46:24 UTC

Sharpness Normal
Shutter Speed Value 1/2
Subject Distance 4,294,967,295
Subject Distance Range unknown
Sub-second Time 37
Sub-second Time Digitized 37
Sub-second Time Original 37
White Balance Auto white balance
Image Number 2,728
Lens ID 150
Lens Info 400, 400, 2.8, 2.8
Lens Model 400.0 mm f/2.8
Serial Number 5016475

Artist Matt Blaze
Copyright MATT BLAZE / mab@crypto.com
Date Time Dec 21, 2010, 6:38:26 PM
Make NIKON CORPORATION
Model NIKON D3X
Orientation 1 (Normal)
Resolution Unit inches
Software Adobe Photoshop CS5 Macintosh
X Resolution 240
Y Resolution 240
Issues

- Carelessness
- Technological surprises
- Conversational nature
- Loss of control of information
Carelessness

- People don’t think through the consequences of what they post
- Aspects: audience; persistence; findability
Technology

- People don’t understand their technology—or technological changes
- Aspects: hidden data; surprising behavior; new algorithms
Conversations

- The net can feel like a private space for talking with friends
- People talk more freely among their friends
- Aspects: confusing context
Loss of Control

- Cost of access is lower
- Cost of copying and redistribution is very much lower
- Aspects: new technology; wide audiences; misplaced trust
- Privacy is defined as the ability to control what happens to your information
People Haven’t Adapated Yet

- Just as with malicious behavior, our behavior patterns have not yet adapted to the Net
- This is complicated by the general unawareness of underlying technologies and the rate of technological change