### Right to Privacy?

- **Article 12** No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

UN, Universal Declaration of Human Rights

- Privacy not mentioned, *per se*, in US Constitution, but rights upheld by SCOTUS

### Privacy and the Internet

I smile every time someone says, "Privacy is dead" or the "Facebook generation doesn't care about privacy." If there is one issue that people feel passionately about today, that literally unites everyone who goes online, it is the interest in privacy.

Marc Rotenberg
EPIC

You already have zero privacy, get over it.

Scott McNealy
Sun

### Zuckerberg on Privacy?

Off record chat w/ Facebook employee. Me: How does Zuck feel about privacy? Response: [laughter] He doesn’t believe in it.

nickbilton
NEA Bilton

### Privacy once upon a time …

Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops."
Privacy, continued

It is our purpose to consider whether the existing law affords a principle which can properly be invoked to protect the privacy of the individual; and, if it does, what the nature and extent of such protection is.

Of the desirability -- indeed of the necessity -- of some such protection, there can, it is believed, be no doubt.

The Right to Privacy, Samuel Warren and Louis Brandeis, Harvard Law Review, 1890

Privacy Continued

The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery. To satisfy a prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers.

Privacy, Technology and the Internet

- What does government know about you?
  - http://epic.org/
  - Resources:
    - http://www.privacyrights.org/fs/fs18-cyb.htm
    - http://snoop.cdt.org/

- What is FISA/FISC? What is the NSA?
  - Where do we look for information?
    - http://en.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Court

Court cases and privacy

What does it mean to “spy”?
What can the government do?
What can companies do?
Kyllo v United States

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. (4th Amendment to US Constitution)

- police look at everything

Kyllo Details

- Police suspicious, imager finds surplus heat
  - Based on image, get warrant, find plants
  - Upheld on appeal (no intimate details, no attempt to conceal), SCOTUS overturns
- Thermal imager/technology violated privacy
  - Compare California v. Ciraolo, 1986, aerial surveillance from 1,000 ft,
  - Compare Katz v. US, 1967, gambling by phone, phone-booth is private

Privacy, Anonymity, Security

- How can we get better privacy?
  - What is private browsing? Chrome, FF, IE?
  - Can we surf the web anonymously?
    - What does this mean?
- What about cookies? What, where, when,...?
  - Can you browse without them?
  - Can you delete when done?
  - Flash and LSOs (local shared objects)

Cookies: Big picture overview

- Cookies help http
  - http is stateless

server

client

get fb.com

content back

1.3.2.4

Cart??

Buy this, buy that!

DELETE COOKIES!!
Cookie overview continued

  - Reasonable overview
- Cookie is a small textfile, not code/executable
  - Expires at end of session or in the future
  - Stored on your computer
  - Comes from a server you “visit”
    - Third party cookies
- How can a cookie track you? It can’t (well, ok)
  - Helps client-server back and forth and ...

- [www.tmz.com](http://www.tmz.com)
  - 100+ cookies!
    - pubmatic.com
    - tmz.com
    - advertising.com
    - doubleclick.net
    - revsci.net

- Dependencies:
  - Content comes from many places
  - Scripts, content, images, ads

### College Newspaper Cookies 2009

<table>
<thead>
<tr>
<th>School Paper</th>
<th># cookies</th>
<th>Cookie Sites</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duke Chronicle</td>
<td>8</td>
<td>Duke, Google</td>
</tr>
<tr>
<td>Daily Tarheel</td>
<td>15</td>
<td>Tarheel, doubleclick, youtube,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>facebook, Google</td>
</tr>
<tr>
<td>Stanford Daily</td>
<td>9</td>
<td>Stanford, Google, Sharethis</td>
</tr>
<tr>
<td>Harvard Crimson</td>
<td>20</td>
<td>Harvard, tribalfusion, Google,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>adtmt, burstnet, quantserv,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>doubleclick,</td>
</tr>
<tr>
<td>Daily Dartmouth</td>
<td>8</td>
<td>Dartmouth, paperg, Google</td>
</tr>
<tr>
<td>Yale Daily News</td>
<td>13</td>
<td>Yale, Google, doubleclick,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>quantserve, youtube</td>
</tr>
<tr>
<td>MIT</td>
<td>7</td>
<td>MIT, Google</td>
</tr>
</tbody>
</table>

### College Newspaper Cookies 2010

<table>
<thead>
<tr>
<th>School Paper</th>
<th># cookies</th>
<th>Cookie Sites</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duke Chronicle</td>
<td>(8) 11</td>
<td>Duke, oncampusweb, adtmt,</td>
</tr>
<tr>
<td>Daily Tarheel</td>
<td>(15) 10</td>
<td>Tarheel, oncampusweb,</td>
</tr>
<tr>
<td>Stanford Daily</td>
<td>(9) 12</td>
<td>Stanford, oncampusweb,</td>
</tr>
<tr>
<td>Harvard Crimson</td>
<td>(20) 17</td>
<td>Harvard, oncampusweb, doubleclick,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>quantserv,</td>
</tr>
<tr>
<td>Daily Dartmouth</td>
<td>(8) 18</td>
<td>Dartmouth, paperg, oncampusweb,</td>
</tr>
<tr>
<td>Yale Daily News</td>
<td>(13) 17</td>
<td>Yale, oncampusweb, youtube,</td>
</tr>
<tr>
<td>MIT</td>
<td>(7) 4</td>
<td>MIT</td>
</tr>
</tbody>
</table>
College Newspaper Cookies 2011

<table>
<thead>
<tr>
<th>School Paper</th>
<th># cookies</th>
<th>Cookie Sites</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duke Chronicle</td>
<td>(8,11) 8</td>
<td>Duke, oncampusweb</td>
</tr>
<tr>
<td>Daily Tarheel</td>
<td>(15,10) 8</td>
<td>Tarheel, oncampusweb</td>
</tr>
</tbody>
</table>
| Stanford Daily      | (9,12) 14 | Stanford, doubleclick, serving-
                        | sys                               |
| Harvard Crimson     | (20,17) 17| oncampusweb, thecrimson,      |
                        |           | doubleclick, serving-sys, rfiub|
| Daily Dartmouth     | (8,18) 44 | thedartmouth, paperg, …,      |
                        |           | doubleclick, serving-sys, rfiub|
| Yale Daily News     | (13,17) 12| yaledailynews, oncampusweb,   |
                        |           | doubleclick, …                 |
| MIT                 | (7,4) 4   | tech.mit.edu                   |

Privacy to Security via Cryptography

- **Keeping digital information private?**
  - Keep it to ourselves
  - Don’t go online
  - Use cryptography to protect it

- **When should we really insist on security?**
  - Facebook? Gmail?
  - Bank?
  - Other?

Cryptography

- **For encryption to work**
  - Not to hard to encrypt (time, money)
  - Easy to decrypt if allowed (time, money)
  - Impossible to decrypt if not allowed (??)

- **Mathematics is the basis for cryptography**
  - Very hard to factor numbers
  - Easy to determine if a number is prime
  - No “security through obscurity”

PKI: Public Key Infrastructure

- **From PGP to Hushmail**
  - PGP is “pretty good privacy”, Phil Zimmerman
  - Distributed as book due to “munitions export restrictions” (1990’s, 40 bit)
  - Web of trust for public key/private key

- **How do circumvent these systems?**
  - Keylogging software by federal agents
Can you Encrypt? Decrypt?

- “Why Johnny Can’t Encrypt”

Anonymous Web surfing

- What does “anonymous” mean?
  - Receiver doesn’t know sender?
  - Track browsing?
- Tor (The Onion Router?)
  - Naval Research Lab
  - EFF
  - 501(3)(c)
  - Advantages? Disadvantages?

In Re Boucher 2007 WL 4246473

- PGP

Ethical? Smart?

- Spouse Monitoring
  - Keep tabs on your spouse’s suspicious behavior. Now with the Mac Spy software – Aobo Mac GS X Keylogger for Mac, you can know the truth...
- Parental Control
  - With the Mac Keylogger, you can see what your children are doing on your Mac, protect them from bad guys.