

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



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.



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.

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

Privacy, the Internet, and Technology

- Privacy in our home, privacy on our hard-drive, privacy in our network habits (home?)
 - What does “privacy” mean in these contexts?
- Best way to keep information private
 - Don’t use the Internet
 - Understand privacy policy
- Trust: industry, government, friends, tech.

Privacy, Technology and the Internet

- What does government know about you?
 - <http://epic.org/>
 - Dated:
 - <http://www.cdt.org/privacy/quiz/>
 - <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? 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)

Anonymous Remailer, Web surfing

- **What does “anonymous” mail mean?**
 - Receiver doesn’t know sender?
 - No one can track the email?
- Anonymous remailer
 - <http://mixminion.net/>
 - Craigslist, is this anonymous? Pseudo?

Ethical? Smart?



» Spouse Monitoring

Keep tabs on your spouse's suspicious behavior. Now with the Mac Spy software -- Aobo Mac OS 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.



CompSci 82, Fall 2009



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?

CompSci 82, Fall 2009

10.14

Cryptography

● For encryption to work

- Not too 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"

CompSci 82, Fall 2009

10.15

PKI: Public Key Infrastructure

● From PGP to Hushmail

- PGP is "pretty good privacy", Phil Zimmerman
- <http://www.philzimmermann.com/EN/contact/index.html>
- <http://www.philzimmermann.com/EN/audiovideo/index.html>

- Distributed as book due to "munitions export restrictions" (1990's, 40 bit)
- Web of trust for public key/private key

● How do we circumvent these systems?

- Keylogging software by federal agents

CompSci 82, Fall 2009

10.16

Can you send encrypted email?

- “Why Johnny Can’t Encrypt”



Compsci 82, Fall 2009

10.17

Certificate of trust, SSL?, MD5?



10.18

In Re Boucher 2007 WL 4246473



Compsci 82, Fall 2009

10.19