

---

# Privacy is NOT a Spectator Sport

Scott Bradner

2/25/2010

# Agenda

---

- ◆ Orwell mispredicted
- ◆ privacy law
- ◆ privacy & the Internet
- ◆ making it worse

# George Orwell

---

- ◆ the government was Big Brother in “1984” (1949)  
could watch and listen to everyone - almost all the time

*You had to live -- did live, ... -- in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.*

- ◆ it is not the government that knows all in today's world  
but someone does (more on this later)

# History of Privacy

---

- ◆ not much privacy in small towns/settlements  
‘everyone knows what everyone is doing’
- ◆ not much privacy from kings etc  
e.g., Magna Carta required due process but not privacy
- ◆ some privacy in early English law  
‘home is castle’ (1499)  
eaves-droppers that spread “*mischievous tails*” “*are a common nuisance*” & can be fined  
Blackstone: book 4, chap 13 (1769)



# Privacy & U.S. Law

---

- ◆ “*The Right to Privacy*” was the subject of 1890 Warren & Brandeis Harvard Law Review article
- privacy is a personal right of a natural person
- six “general rules” on privacy
  - 1: public interest overrides the right to privacy
  - 2: privileged communication does not void right to privacy
  - 3: generally no regress for talking (without publication)
  - 4: publication of facts by subject voids a right to privacy
  - 5: truth is not a defense against a breach of a right to privacy
  - 6: an absence of malice not a defense against a breach of a right to privacy

# Privacy & the U.S. Constitution

---

- ◆ word “privacy” is not in the U.S. Constitution
- ◆ but the Supreme Court have found that a right of privacy is implied by a number of the amendments in the Bill of Rights
- ◆ privacy called a “*penumbra right*” in Griswold v. Connecticut (1965)
  - penumbra: “*a body of rights held to be guaranteed by implication in a civil constitution*” Merriam-Webster Dictionary
- ◆ the Supreme Court has found that the Constitution protects a “*zone of privacy*” in two areas
  - independence in making certain types of decisions
  - avoiding disclosure of personal matters

# Supreme Court and Privacy

---

- ◆ key case: Katz v. U.S. (1967)

- government wiretapped a phone booth w/o warrant

- Supreme Court found that government violated the Fourth Amendment (unreasonable searches and seizures)

- in doing so, moved the right to privacy from a place (e.g., home) to a person

- added the 'reasonable assumption' of privacy test

- 1: did person exhibit personal expectation to privacy

- 2: does society recognize the expectation as reasonable

# US Privacy Related Law

---

- ◆ mostly, limits on power of government

  - privacy of postal mail - 1782, 1825, 1877

  - privacy of census - 1919

  - Communications Act - 1934

    - prohibit government disclosure of communications

  - Privacy Act - 1974

    - limit what info government can collect about citizens

  - Right to Financial Privacy Act - 1978

    - require subpoena to get financial records

  - Privacy Protection Act - 1980

    - require subpoena to get unpublished media work

# US Privacy Related Law, Contd.

---

- ◆ some targeted limits on non-government action

  - Wiretap Act - 1968

    - extended wiretap restrictions to states and individuals

  - Fair Credit Reporting Act - 1970

    - limit who can get credit info

  - Family Educational Rights and Privacy Act - 1974

    - protect student records

  - National Research Act - 1974

    - protect human subjects

  - Cable Communications Policy Act - 1984

    - protects privacy of cable subscribers



# US Privacy Related Law, Contd.

---

## ◆ more targeted limits on non-government action

Employee Polygraph Protection - 1988

limit use of lie detectors in private sector

Video Privacy Protection Act - 1988

protect privacy of video tape rental records

Driver's Privacy Protection Act - 1994

block states from releasing driver's license info.

Health Insurance Portability and Accountability Act - 1996

protect medical records

Gramm-Leach-Bliley Act - 1999

protect privacy of financial information

# US Privacy Related Law, Contd.

---

- ◆ enabling government action

  - Communications Assistance for Law Enforcement Act -  
(CALEA) 1994

    - requires telephone companies be able to wiretap their customers

  - USA-PATRIOT Act - 2001

    - surveillance support

  - CALEA expansion - 2005, 2006

    - extend wiretap requirements to Internet service providers

- ◆ note that adding wiretapping features makes  
systems vulnerable to hacking

  - e.g., Greek cell phones & (maybe) Google hacking

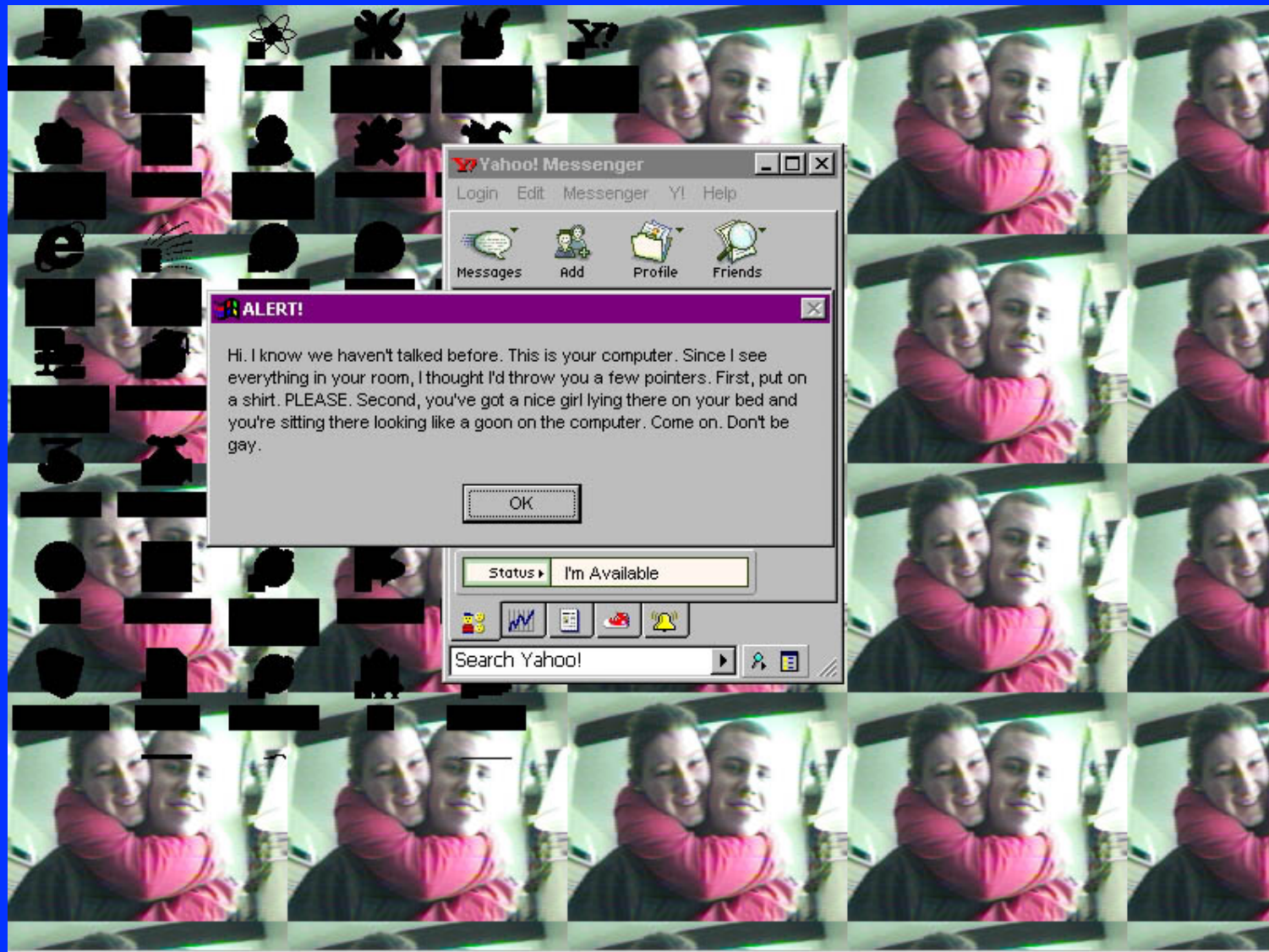
# Just Because You Can

---

- ◆ many in government seem to think that just because they have the technical ability do something it is OK to do so
  - e.g., just because it is possible to record all email some people in law enforcement want to do so, even if they would never propose to do the same for physical mail
  - e.g., law enforcement request for 2-year ISP retention of all IP addresses accessed by customers
  - e.g., officials at the Lower Merion School District are accused of spying on students at home through loaner laptops

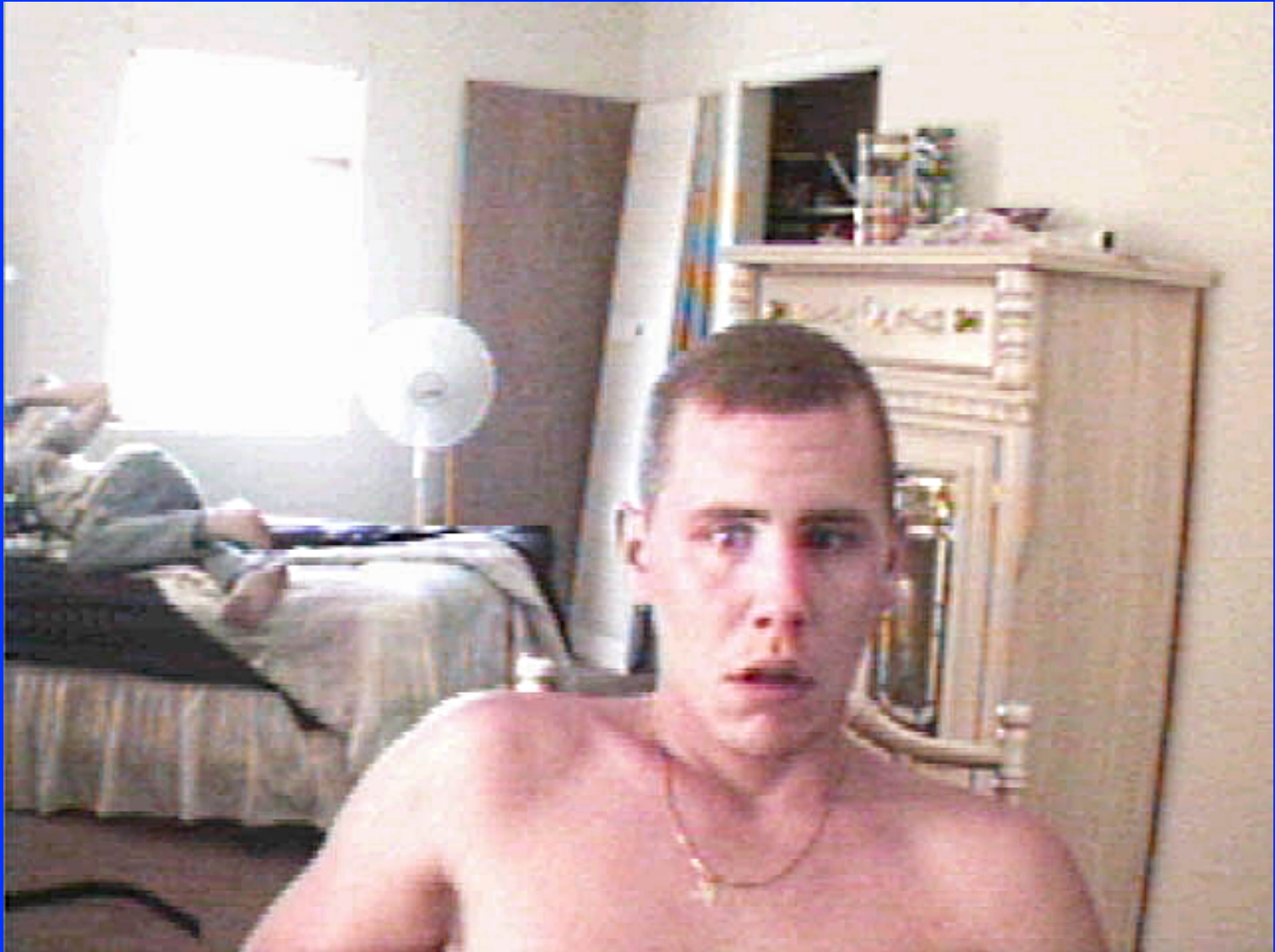


# One Morning You See On Your PC:



# What Your PC Sees

---



# Even if the Law Says “No”

---

- ◆ long history of people in law enforcement not obeying law

warrantless wiretaps

National Security Letters

spying on social activists

- ◆ is that bad? - ‘if you have nothing to hide’  
the US Constitution purposefully has limits on  
government power based on history

Benjamin Franklin (1706–90)

***“Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety.”***



# Pushing at the Limits

---

- ◆ there are a number of current efforts by parts of the US government to say that Internet users do not meet the Katz case test in a number of places
  - i.e., have no reasonable expectation of privacy
  - e.g., email at an email provider
  - same for location information from cell phone providers
- ◆ if successful, then the government would not need a subpoena to demand the information

# US Privacy Related Law, Overview

---

- ◆ no systematic approach or basic concepts
- ◆ point solutions
  - e.g., video tape rentals, license information
- ◆ no meaningful regulation of the collection or use of information in private hands
  - e.g., credit card or supermarket loyalty card
  - only requirement: do what your privacy statement says
- ◆ other parts of the world approach the issue differently

# Convention on Human Rights (1950)

---

- ◆ European Convention on Human Rights

- ◆ Article 8

*“Everyone has the right to respect for his private and family life, his home and his correspondence”*

# EU Data Protection Directive - 1995

---

- ◆ comprehensive approach to privacy

*“Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.”* Data Protection Directive: Object of the Directive

- ◆ passed at EU level, implemented by each country

- ◆ applies to all, not just governments

# EU Data Protection Directive, contd

---

- ◆ conditions that must be met before personal data can be collected & processed
  - transparency - subject informed & gives consent or legally required, subject has access to data & can correct errors, data must be protected
  - legitimate purpose - processed only for specified, explicit and legitimate purposes
  - proportionality - processed only as much as needed for stated purpose
- ◆ data only moved outside of EU to places that *'provide an adequate level of protection'*
- ◆ note that the EU just blocked transfer of banking information to the US anti terror effort



# Meanwhile in the U.S

---

◆ everyone collects everything they can

supermarkets & other stores

toll booths

GPS navigation systems

credit card companies

cell phone companies

tax preparation sites

random web sites

Internet service providers

and then there is



(and Yahoo!, Bing, etc)



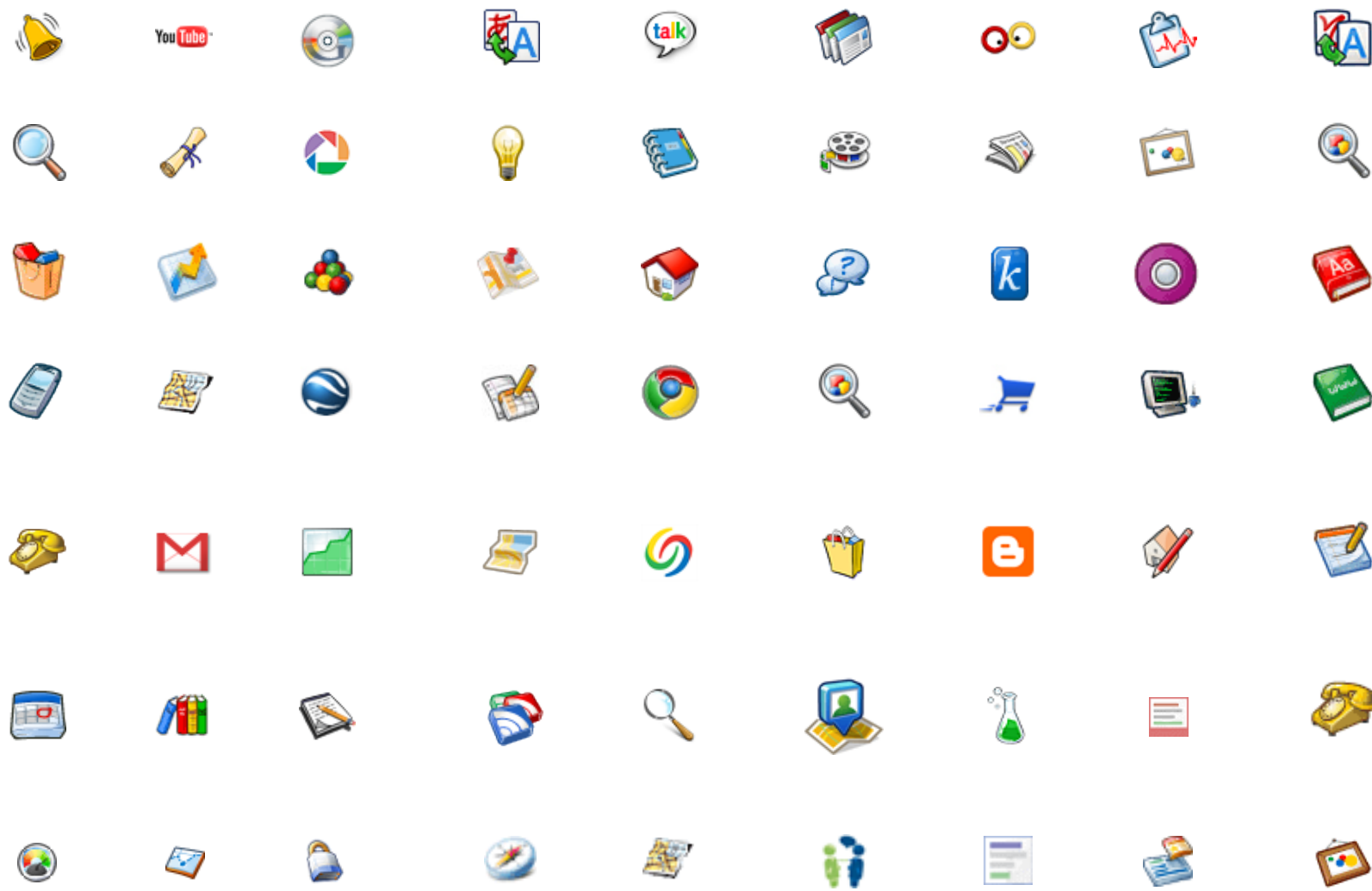
Should you care?

# Google

---

- ◆ Google as an example of (non) privacy on the Internet
- ◆ Google finds things that others publish about you
- ◆ Google monitors much of your usage of the 'net even if you do not search using Google
- ◆ Google is not the only player - it is just better at the data-about-you business than most of the other players

# The Googleverse



# Googleverse, contd.

---

## ◆ search

web, images, video, news, patents, blogs, shopping, maps, books, scholar, custom, earth, finance, phone numbers, directory, dictionary, GOOG-411...

## ◆ other services

alerts, checkout, health, code, blogger, calendar, docs, gmail, groups, knol, orkut, picasa, talk, translate, longitude, sketch, YouTube, ...

## ◆ tools

toolbar, chrome, desktop, reader, sites, notebook, analytics, AdSense, friend contact, apps, geospatial, postini, Buzz, iGoogle, SketchUp, ...

# Google Data

---

- ◆ most Google services and functions gather data about your activities

search: what you searched for, what you selected, in  
image search - what you did there

checkout: what you bought, from whom & where it went

analytics: where you go (even if you do not use Google  
search to get there)

alerts: what you are interested in

docs, blogger, calendar, gmail, talk, translate: content  
from docs & communications

groups, longitude, gmail, friend contact: friends

toolbar: everyplace you go



# Google Retention

---



- ◆ Google keeps information forever, but removes IP addresses after 9 months (Sept 2008) - Google calls it anonymization

“While we're glad that this will bring some additional improvement in privacy, we're also concerned about the potential loss of security, quality, and innovation that may result from having less data. As the period prior to anonymization gets shorter, the added privacy benefits are less significant and the utility lost from the data grows. So, it's difficult to find the perfect equilibrium between privacy on the one hand, and other factors, such as innovation and security, on the other. Technology will certainly evolve, and we will always be working on ways to improve privacy for our users, seeking new innovations, and also finding the right balance between the benefits of data and advancement of privacy.”

- ◆ do not say they remove the unique Google cookie
- ◆ may not be an effective anonymization  
e.g., AOL data release

# What Does This All Mean?

---

- ◆  knows
  - what you are interested in (search, analytics)
  - what you talk about (gmail)
  - what you write about (docs)
  - what you talk to people about (voice)
  - who you know/are friends with (gmail, docs, groups)
  - who you are (checkout, docs, groups, longitude)
  - where you are in meat space (longitude)
  - where you are in virtual space (all of the above)
- ◆ and  can put it all together



# Why?

---

- ◆ currently:

  - “to optimize search results”

  - “make ads even more relevant and useful”

- ◆ tomorrow

  - who knows - Google wants to be able to play with the data

# What is Wrong with This?

---

- ◆ what is wrong with Google knowing all?

  - can be required to help law enforcement

    - even in countries where this is a real problem

    - see Google's current conflict with China

  - can be required to help in civil cases

    - what was he looking at that I can use in a divorce case?

  - a dishonest Google employee can use info for blackmail

  - could have major privacy problems if Google gets hacked

  - Google's hubris can cause major missteps

    - e.g., Buzz not being opt-in

  - Google's management could change

# It is not Only Cookies

---

- ◆ configuring your browser to remove cookies helps web cookies, flash cookies, etc
  - ◆ makes it harder to track you but IP address still works
  - ◆ the fingerprint of your system is trackable as well system type & version, plugins, fonts, timezone, screen characteristics, etc
- my home system is unique in 662,792 systems tested at <https://panopticklick.eff.org/>

# State of Privacy on the Internet

---

- ◆ Scott McNealy, CEO Sun Microsystems

**“You have zero privacy anyway. Get over it.”**

- ◆ not quite true, not everybody knows everything about you (including, currently, the government)
- ◆ most information is seen as confidential by the companies that collected it
  - will release with a court order
  - & some sell the information
- ◆ so most of this information is not public

# Anonymity

---

- ◆ anonymity is protected by the US Constitution  
according to the US Supreme Court  
at least for political speech
- ◆ anonymity gets a bad rap  
you must be trying to hide something
- ◆ but anonymity important in many areas, e.g.,  
whistleblowers  
political dissidents (particularly in some countries)  
self help groups
- ◆ some anonymity tools available on the Internet  
e.g. Tor

# Ethics in the World of the Internet

---

## ◆ area 1 - data collectors

do they tell you what data they collect?

e.g., website privacy statements (none at [www.gvsu.edu](http://www.gvsu.edu))

do they tell you what they do with the data?

e.g., sell your grocery lists to insurance companies?

e.g., keep data long after there is any legit reason to do so

do they effectively protect your data?

e.g., put private records on unencrypted laptops



# Ethics, contd.

---

## ◆ area 2 - service providers

do they keep the rights of their users in mind?

e.g., Google not use opt-in on new services like Buzz

e.g., Facebook default settings

e.g., ISPs using secret deep packet inspection to target ads

## ◆ area 3 - software vendors

do vendors disclose data gathering by products

e.g., Sears toolbar

# Ethics, contd.

---

## ◆ area 4 - employers & schools

do they respect their employees and students?

e.g., secretly monitor network traffic & social networking sites

do they limit data access to business need to know?

e.g., open student records to all administrative staff

## ◆ area 5 - individuals

do individuals conduct themselves ethically?

e.g., Lori Drew pretending to be a young man and driving a vulnerable 13 year old girl to suicide

e.g., inventing facts and posting on gossip web sites



# You Do Not Have to Help

---

- ◆ it is truly amazing what some people reveal on social networking sites - e.g.,

Ashley Sullivan - crashed car when driving drunk, her boyfriend was killed in the crash, month later posted picture she titled “drunk in FL”, the judge took notice & sentenced her to more time in jail and on probation then he was going to

gang of teen aged girls posted a video of themselves beating another teen age girl - attackers arrested

boy posts video of himself abusing a cat

salesmen posted videos of 150 mph “test drives” - showing their faces

# Not Only Criminal Behavior

---

- ◆ posting of ‘normal’ activities can have an impact
  - party going
  - political opinions
  - rants
  - embarrassing photos
  - daily activities

# First Impressions

---

- ◆ first thing that many people do when about to meet someone new is to do a search
  - will you be happy with what a prospective boyfriend (or girlfriend) would find?
  - how about a prospective employer?
- ◆ survey of US, UK, Germany & France HR officers
  - 70% had rejected a job applicant based on info in social networking site
- ◆ some insurance companies do the same
- ◆ the Internet is forever, think first

# Conclusion

---

- ◆ I've painted a bleak picture
- ◆ but it is not as bad as it might seem

Google, which knows all, wants to keep the info to itself  
governments over reach and then (some) are restrained by  
new laws

individuals can learn