Consumer Privacy and Information Access

CIS 150: Fundamentals of Information Systems

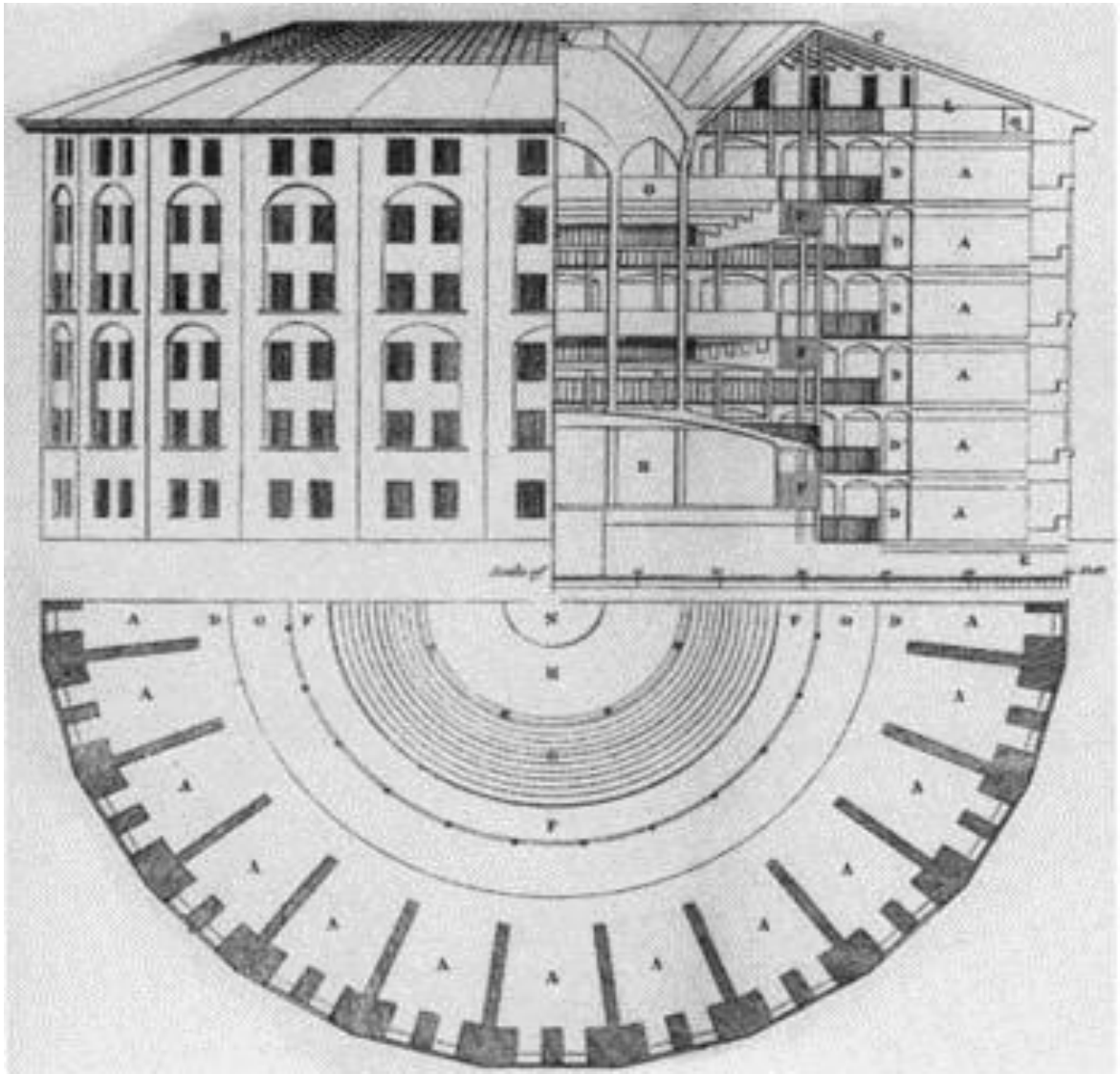
Today's Agenda

- What is the right to privacy?
- Have we created a panopticon?
  - The role of IT and privacy-invasive technologies
- Consumer privacy on the Internet
  - Is technology destroying consumer privacy rights?
  - How should firms handle consumer data?
  - What are some solutions to protecting consumer privacy? (technology, marketplace, industry norms, law)

Information Privacy

- Three (3) key aspects of privacy
  - Freedom from intrusion (being left alone)
  - Control of information about oneself
  - Freedom from surveillance (e.g., from being followed, tracked, watched, and eavesdropped on)
- What is information privacy?
  - The right of individuals to determine for themselves when, how, and to what extent information about them is communicated to others
- We often give up information privacy in return for benefits of dealing with strangers
  - Key benefits => convenience, more personalized service, and deals
  - Think about what you reveal everyday on Facebook, MySpace, etc.

What is a Panopticon?



Has IT Created a Panopticon?

- IT has:
  - Changed the scale of information collected and stored
    - » Digital files, MP3 file-compression format, high-volume, cheap digital storage media, scanners (which digitize data)
    - » Database (DB) approach (vs. the traditional file approach) that collects, stores, retrieves info quickly and cheaply
      - ◆ Traditional file approach (pre-1990s) stored data unlabeled and uncategorized as a continuous string of bytes with no easy mechanism to locate and manipulate the data (think of the traditional file approach as data storage on a VCR tape)
      - ◆ DB approach (1980s and 1990s) labels and organizes each piece of digitized data (usually into tables) and provides tools to locate and manipulate data quickly
  - Changed the kind of information collected and stored
    - » Ecommerce: on-line click stream data, on-line search query data
    - » Workplace: biometric characteristics (e.g., fingerprint scans), keystrokes, work habits, time logged in, email read and sent
    - » Elsewhere: physical location data
    - » This is information we never thought about collecting years ago, but IT now enables it

Has IT Created a Panopticon?

- IT has:
  - Changed the scale of information exchanged and distributed
    - » WWW, broadband (high-speed) Internet connections, peer-to-peer (P2P) networks vs. client-server architecture
    - » Easy and quick transmission of stored digital data over the private networks and the Internet
  - Magnified the effect of erroneous information
    - » Once you give up control of your data it is impossible to regain control
    - » Consider an example
      - A pregnant woman decides to register at a Babies-R-Us Web site to receive baby-related coupons, notices, free samples, and advertisements
      - What does Babies-R-Us do with that data? Sells it to 3rd parties (e.g., Gerber's)
      - Assume that the woman has a miscarriage – what is going to happen? She is likely to continue receiving painful reminders on a daily basis! Adverse psychological affects?
      - What is the woman notifies Babies-R-Us of the problem? The ads probably continue since her data has been sold to many marketers – it will be difficult to track down all the other lists that she has been added to

Has IT Created a Panopticon?

- IT has:
  - Enabled the combination (or recombination) and analysis of data
    - » We can now merge data from different DB (e.g., link financial records, work records, family record, and medical records) to develop much more detailed user profiles of our personal characteristics, activities, opinions, habits, etc.
      - Metromail is a data broker that aggregates and maintains a lot of data about over 100 million people in the U.S.
        - Specializes in tracking transitions in people's lives (e.g., moves)
        - When you move to a new house, Metromail figures it out and, for 25 cents/name, sells your name and address to junk mailers (furniture stores, cell phone companies, long distance telephone, hardware stores, appliance stores, local restaurants, etc.)
      - ChoicePoint is also a data broker
        - Maintains data on drug tests, insurance fraud, bankruptcies, public records
        - Government and business agencies use it to verify data and credentials for job applicants (i.e., background checks)
    - » Advances in algorithms (mathematical and statistical methods) and data mining tools have improved our ability to finds patterns in data that we could not see before

Privacy-Invasive Technologies
(Specific Technologies)

- IT has:
  - Made the invisible collection of personal data without user knowledge easier
    - » Cookies
      - Small text files (with ID number) written and stored on user's hard drive by a Web site when the user visits that site with a browser
      - Store information about a visitor's activities (e.g., passwords, a list of pages visited and for how long, dates last examined, what is in your shopping cart, what is in your wish list, the browser you used, IP address, etc.)
      - When the user visits again the stored cookie is sent back to the site with all the info
      - The cookie interaction can be anonymous (no personal info, only a unique cookie ID), but the anonymous info can be linked to personal info based on purchases or registration on the site
      - Help provide data for targeted marketing

Privacy-Invasive Technologies
(Specific Technologies)

- IT has:
  - Made the invisible collection of personal data without user knowledge easier
    - 3rd party cookies
      - Cookies placed on a network of related sites so that the user can be tracked not just within a single site but anywhere within the network
      - DoubleClick (now owned by Google) has deals with tens of thousands of Web sites and maintains cookies on over 100 million people (linked to lots of data on browsing behaviors)
      - ISPs are the ultimate 3rd party cookie (can access your entire navigation history)
    - Web beacons (or bugs)
      - Embedded as an invisible graphic (sometimes called "clear GIFs") on a Web site or an email in order to track visitors to that Web site or recipients of the email
      - Can count visitors (click rates to pay sites for ad space), track pages visited, get IP address of visitor, the browser used, count # times a banner was opened, etc.
      - Can use in email to trigger with an instruction to open an image – this tells the sender that the message was read and how many times it was forwarded (you can't do this with "snail mail")

Privacy-Invasive Technologies
(Specific Technologies)

- IT has:
  - Made the invisible collection of personal data without user knowledge easier
    - » Spyware
      - Much more intrusive methods for collecting online date
      - Small computer program installed on your hard drive (usually without your knowledge or consent) that tracks the user's habits (e.g., all Web surfing) and transmits that information to a third party
      - Can be malicious (e.g., steal credit card numbers, ID/passwords, or reformat search engine results to put a client's link at the top of a legitimate search results page)
    - » In 1999, Comet Systems offered a free software application that allowed users to change their Web browser's cursor into cartoon characters (~16 million people)
      - Without user knowledge or consent, the software tracked how many people used the software, their IP addresses, systems information (e.g., browser type), and the sites that they visited
    - » Article

Privacy-Invasive Technologies

(Specific Technologies)

Business

The Courier-Journal

4INFO Market news on your cell
Go to courier-journal.com/mobile for daily market news or stock quotes

SATURDAY SEPTEMBER 5, 2009 B8

Dan Blake, editor dblake@courier-journal.com | 582-4651 | Fax: 582-4360

Software gathers children's chat data

Information then sold to businesses

By Deborah Yao
Associated Press

Parents who install a leading brand of software to monitor their kids' online activities may be unwittingly allowing the company to read their children's chat messages — and sell the marketing data gathered.

Software sold under the Sentry and FamilySafe brands can read private chats conducted through Yahoo, MSN, AOL and other services, and send back data on what kids are saying about such things as movies, music or video games. The information is then offered to businesses seeking ways to tailor their marketing messages to kids.

"This scares me more than anything I have seen using monitoring technology," said Parry Aftab, a child-safety advocate. "You don't put children's personal information at risk."

The company that sells the software insists it is not putting kids' information at risk, since the program does not record children's names or addresses. But the software knows how old they are because parents customize its features to be more or less permissive, depending on age.

Five other makers of parental-control software contacted by The Associated Press, including McAfee and Symantec, said they do not sell chat data to advertisers.

One competitor, CyberPatrol, said it would never consider such an arrangement. "That's pretty much confidential information," said Barbara Rose, the company's vice president of marketing. "As a parent, I would have a problem with them targeting youngsters."

The software brands in question are developed by EchoMetrix, based in Syosset, N.Y.

EchoMetrix Chief Executive Jeff Greene said it complies with U.S. privacy laws and does not collect any identifiable information.

One EchoMetrix service, Pulse, reveals how kids feel about upcoming movies, computer games or clothing trends. Such information can help advertisers craft their marketing messages as buzz builds about a product.

Parents who don't want the company to share their child's information to businesses can check a box to opt out.

But that option can be found only by visiting the company's Web site, accessible through a control panel that appears after the program has been installed. It was not in the agreement contained in the Sentry Total Home Protection program the AP downloaded and installed Friday.

Privacy-Invasive Technologies
(Specific Technologies)

- IT has:
  - Made the invisible collection of personal data without user knowledge easier
    - » Are you aware of Event Data Recorders (EDRs) in automobiles?
      - Installed in some cars to record information related to vehicle crashes / accidents (~ “black box” in airplanes)
      - May record impact speed, brake application, steering angle, sea belt use, airbag deployment, cruise control status, etc.
      - On April 12, 2007, N.J. Governor Jon Corzine was seriously injured in an automobile accident – an EDR recorded his SUV travelling at 91 mph (in a 65 mph speed limit zone) 5 seconds before the crash
      - How will this data be used in insurance claims and court cases?

Privacy-Invasive Technologies
(Specific Technologies)

- Did you know that search engines (e.g., Google.com, Ask.com) collect and store your search query data?
  - Search engines collect many terabytes of data daily (cheap to store) and maintain large databases of past user queries. What does Google collect? Search engine log data
    - » What search terms that you entered
    - » How many pages of search results that you looked at
    - » How many search results that you clicked on
    - » How you refined your search queries
    - » What spelling errors that you commonly make
    - » What browser you use
    - » What your IP address is
    - » What might this look like?
      - Assume you have never visited Google.com and now visit it and search for “cars”
      - Google will send a cookie and record something like (notice no personal data)

Inktomi1-Ing.server.ntl.com – 25/Mar/2009 10:15:32 – http://www.google.com/search?q=cars – MSIE 6.0; Windows XP – 740674ce2123e969

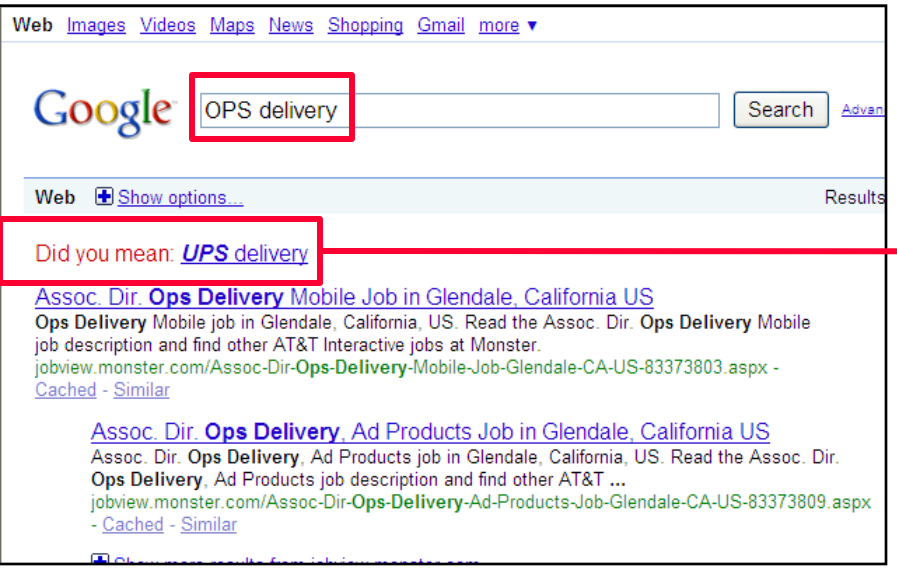
Privacy-Invasive Technologies
(Specific Technologies)

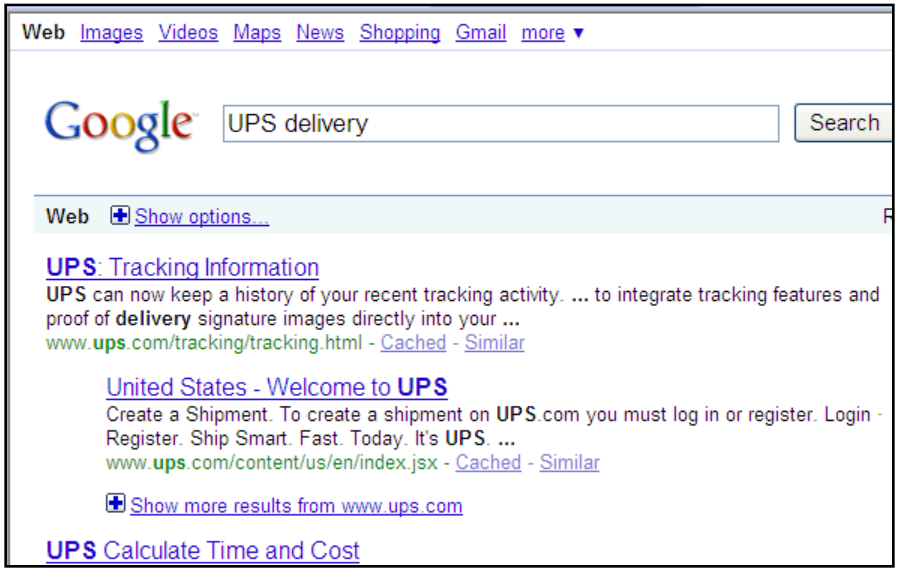
- Did you know that search engines (e.g., Google.com, Ask.com) collect and store your search query data?
  - How is this information used? (see Google Privacy FAQ)
    - » Google analyzes this data to improve search engine services (better quality result rankings), better targeted advertising, and develop new products/services (e.g., Google Spell Checker)
      - DB of queries serves as inputs for testing and evaluating modifications in search engine algorithms used to select and rank search results
      - Analysis of query data leads to new services such as "Google Spell Checker"
        - Automatically looks at a user's query and checks to see if the user is using the most common version of the word's spelling. If Google "calculates" that the user is likely to get more relevant search results with an alternative spelling it will ask "Did you mean: (more common spelling)?"
      - The cookie also records the user's search setting preferences (e.g., settings to see 100 results/page instead of 10 results/page)

Privacy-Invasive Technologies

(Specific Technologies)

- Did you know that search engines (e.g., Google.com, Ask.com) collect and store your search query data?
  - "Google Spell Checker"





Privacy-Invasive Technologies
(Specific Technologies)

- Did you know that search engines (e.g., Google.com, Ask.com) collect and store your search query data?
  - Is this data collect a threat to the users' privacy?
    - But you may still be concerned about maintaining privacy about searches that you make – for example, searches about: health and psychological problems, bankruptcy, alcoholism, erotica, illegal drugs, etc.
    - The data collection is basically invisible (i.e., covert) since most people do not know that every one of their searches is collected and stored

Privacy-Invasive Technologies
(Specific Technologies)

- Did you know that search engines (e.g., Google.com, Ask.com) collect and store your search query data?
  - Is this data collect a threat to the users' privacy?
    - » What type of data is not collected with Google searches from the main search page (i.e., when a user is not registered for a Google service)?
      - Does not collect personal data (such as name, address, phone number)
        - Google just knows (based on a cookie) that a particular software browser on a particular computer made a search
        - Google does not know who was sitting at the computer performing searches
        - Google *claims* that your "account cookies" (which have personal data) are not linked with your "search cookies" (which do not have personal data)
        - Take note that by registering you do run a more significant privacy risk in the future (i.e., if Google decides to link and combine the cookies)

Privacy-Invasive Technologies
(Specific Technologies)

- Did you know that search engines (e.g., Google.com, Ask.com) collect and store your search query data?
  - Is this data collect a threat to the users' privacy?
    - » Who gets to see this huge mass of data and why should we care?
      - The federal government presented Google with a subpoena for 2 months of user search queries and all of the URLs that Google indexes
        - At the time the government wanted to respond to court challenges to the Children's Online Protection Act (COPA)
        - This generated lots of protests from users and privacy advocates
        - Courts reduced the scope to 50,000 URLs and no user query data
      - A few months later, Google posted a huge DB of user search query data for researchers to access
        - >20 million searches by ~650,000 people over a 3-month period
        - Data identified by coded ID #, not by name or IP address
        - Re-identification problem: The ability to deduce the identity of some people from "anonymous" data
        - Journalists and others were able to identify some people from small towns based on specific topics searched (e.g., personal names/addresses, vehicles, health)
        - Once identified, that person may be linked with all his other searches

Privacy-Invasive Technologies
(Specific Technologies)

- Did you know that search engines (e.g., Google.com, Ask.com) collect and store your search query data?
  - What are the lessons?
    - » Anything we do online is recorded and linked to our computer (and maybe our name)
    - » Huge amounts of data are stored with new storage devices
    - » Data collection is often covert (without your knowledge and consent)
    - » Leaks happen
    - » A collection of many small items of information can give a fairly detailed picture of what a person's like
    - » Direct association with a person's name is not essential for compromising privacy (i.e., re-identification)
    - » The government sometimes requests sensitive, personal data held by a company
    - » Data on the Internet and stored in DB seem to last forever
    - » It is extremely likely that data collected for one purpose will be used for another purpose (secondary uses)
    - » We cannot protect all data ourselves – we must depend on the company's that have it to protect it from thieves, accidental leaks, and a prying government

Privacy-Invasive Technologies
("Big Brother" is Watching)

- Basis of privacy rights → 4th Amendment of the Bill of Rights
  - Protects people from unreasonable search and seizure by the government
  - Requires probable cause to get a warrant for a search and a specification of the place to be search and what will be seized
- "Big Brother" = Government
  - George Orwell's 1984: The government could watch everyone via "telescreens" in all homes and public places
    - » Little crime, little political dissent, and little love or freedom
  - Minority Report (2002 movie with Tom Cruise)
    - » Similar idea except law enforcement used psychics (precogs - mutated humans with precognition abilities) to monitor people's thoughts and arrest people pre-crime (i.e., before they commit a crime!)
  - Eagle Eye (2008) technological thriller with lots of privacy implications

Privacy-Invasive Technologies
("Big Brother" is Watching)

- Government DBs
  - Government agencies maintain 1000s of DB containing personal data
    - » Tax records, medical records (Medicare, Medicaid, military), marriage/divorce records, school records, property ownership, welfare (with family details), motor vehicle records, voter registration records, books checked out in public libraries, people with firearm permits, applications for government loans and grants, bankruptcy records, arrest records, and you get the idea!
    - » The government collects information (e.g., surveillance data related to the "war on terrorism"), requests it from businesses, gets court orders to collect data, buys personal information from resellers, etc.
    - » Helps government perform its functions
      - ◆ Determine eligibility for federal programs and government jobs and benefits, detect fraud in government programs, collect taxes, catch people who break the law, etc.
    - » So what is the problem?
      - ◆ Government has a ton of personal data and the power to arrest people and seize assets
      - ◆ The potential misuse of personal data by government poses a special threat to liberty and privacy

Privacy-Invasive Technologies
("Big Brother" is Watching)

- Government DBs
  - Government agencies maintain 1000s of DB containing personal data
    - » So what is the problem? Consider the IRS and taxpayer data!
      - Each year hundreds of IRS employees are investigated for snooping into people's tax files
        - Example: An IRS employee who was a KKK member read tax records for his KKK group to look for income information that would indicate a member was actually an undercover agent
      - IRS employees dispose of discs with sensitive tax data without erasing files
      - Tax data is at risk from hackers and disgruntled employees because many of the 250 + federal agencies to which the IRS provides taxpayer info do not have adequate data protections
    - » So what is the problem? Consider the expansion of government DB over time
      - CODIS = FBI DNA DB
        - Originally only contained DNA of convicted sex offenders
        - Now contains data collected from crimes scenes, other classes of criminals (e.g., murders, misdemeanors), people arrested for a crime

Privacy-Invasive Technologies
("Big Brother" is Watching)

- Government DBs
  - Government agencies maintain 1000s of DB containing personal data
    - So what is the problem? Consider the proposal for a government DB to track college students
      - Department of Education proposed establishing a DB to contain records of every student enrolled in a college or university in the U.S.
      - Universities would be required to provide and regularly update records including student's name, gender, SSN, major, degrees, loans, scholarships, courses taken, courses passed, etc.
      - Benefits
        - Good way to track success of govt student loan/scholarship programs
        - More accurate information on graduation rates and college costs
        - Better able to track the # of future nurses, engineers, etc. to improve the effectiveness of immigration policy and business planning
      - Privacy risks?
    - What about Social Security Numbers used for identification purposes?

Privacy-Invasive Technologies
("Big Brother" is Watching)

- Automated toll collection systems
  - Used at many bridges, tunnels, and toll roads
  - Sensors read devices in the car as it goes by without stopping and the owner's credit card or bank account is billed for the toll
  - Benefits
    - » Saves time and lowers collection costs (i.e., fewer human toll operators)
  - Privacy Risks?
    - » Toll DB now contains a record of when/where a person travelled (and sometimes how fast)
    - » Can marketers and government agencies use this information to track people?
      - NY judge ruled that police can access toll records without a court order because traffic movement is in public view and drivers should not have the expectation of privacy regarding their travel (not protected by 4th Amendment)
        - But without these detailed systems travel is basically anonymous
      - Does this mean that law enforcement should also be able to access a list of books that you buy at Barnes & Noble without a court order since your purchase is in public view?

Privacy-Invasive Technologies
("Big Brother" is Watching)

- Satellite imaging
  - Use of technology to take detailed photographs of earth
    - » Often shows homes, vehicles and even backyards
    - » Google Earth
  - State governments may use this technology to
    - » Catch people who are growing illegal drugs
    - » Detect buildings or property improvements that may lead to higher property taxes
    - » Catch people who have built backyard porches without the required building permits
  - Are such "noninvasive but deeply revealing" searches a privacy invasion that the 4th Amendment should prohibit?

Privacy-Invasive Technologies
("Big Brother" is Watching)

- Backscatter technology
  - Transportation Security Administration (TSA) uses new type of imaging technology at some U.S. airports that displays a (sometimes revealing) computer image of a person's body and any weapons or drug packets hidden under the clothes or a wig (no need for physical contact)
    - » First implemented in Phoenix Airport in 2007 with new tests now going on at Houston's George Bush International Airport and Greater Rochester Int'l Airport
    - » ACLU has call this a virtual strip search
  - What are the usage policies for this technology so far?
    - » TSA "blurs out" certain body parts (and use of cloakers)
    - » TSA claims that the technology cannot save, print, or transmit images
    - » Usage is voluntary → the person has the choice of using the backscatter technology or undergoing a pat-down search (which is slower, less thorough, and more physically intrusive)
    - » The security officer who assists the passenger through the screening process never sees the image the technology produces. Instead, the image is viewed by a remotely located security officer who never sees the traveler

Privacy-Invasive Technologies
("Big Brother" is Watching)

- Video surveillance
  - Security cameras at banks, convenience stores, casinos, and prisons
  - 2001 Super Bowl (aka Snooper Bowl) in Tampa, FL
    - » Used technology to scan the faces of all 100,000 fans and employees who entered
    - » The system used facial-recognition software to compare the facial geometry of each person with a DB of known criminals – trying to find matches
  - Tampa, FL installed a similar facial-recognition video surveillance system in a neighborhood with lots of restaurants and nightclubs
    - » Police in a control room would zoom in on faces and check for matches in their DB
    - » In 2 years the systems did not recognize any suspects but did occasionally identify an innocent person as a wanted suspect
    - » They stopped using it (accuracy was not good enough)
  - Traffic monitoring system in another city in FL
    - » Removed after engineers were found zooming in on individual pedestrians unrelated to traffic flow
  - More police patrols/increased lighting may better deter crime

Privacy-Invasive Technologies

("Big Brother" is Watching)

- Video surveillance

Security cameras blanket Lancaster, Pa.

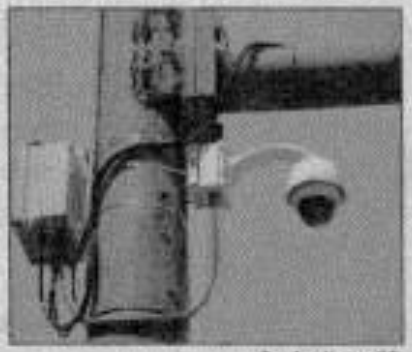
Surveillance system raises privacy issue

By Patrick Walters
Associated Press

LANCASTER, Pa. — Horses drawing buggies regularly clop down the roads approaching Lancaster, a peaceful city in the heart of Amish country that had only three murders last year and relatively low crime.

But if the community sounds reminiscent of the past, it also has some distinctly modern technology: 165 surveillance cameras that will keep watch over thousands of residents around the clock.

When it is complete, the surveillance system will be bigger than those in large cities such as Philadelphia, San Francisco and Boston. And the fact that it will be monitored by ordinary citizens has raised privacy concerns.



Carolyn Kastner/AP
One of 165 security cameras overlooks Penn Square in Lancaster, Pa.

"They are using fear to sell the cameras as much as possible," said Charlie Crystle, a member of a fledgling citizens group that opposes the cameras and is trying to raise public awareness about them. "There's just a huge potential for personal and political abuse."

Officials in the city of 54,000 say the cameras have deterred crimes and helped solve them.

The white, domed cameras sit atop utility poles in public spaces, business districts and some residential areas. They are monitored 18 to 24 hours a day by employees of the Lancaster Community Safety Coalition, a nonprofit board with workers who report suspected crimes to police.

The safety coalition, directed by City Councilman Joseph Morales, screens prospective monitors and provides training about racial profiling and how to spot trouble. The group has seven monitors, all paid. The coalition does not release their names.

"What they are typically seeing is people in their everyday life going through their business," Morales said. "They're looking for anything out of the ordinary."

Lancaster has seen some declines in property crimes since the cameras went up, but those numbers have fluctuated — along with the totals for violent crimes.

Crystle and others in Lancaster say they have done nothing to warrant being watched. The American Civil Liberties Union objects, especially since it covers the entire city — not just high-crime areas.

Privacy-Invasive Technologies
("Big Brother" is Watching)

- Location tracking systems
  - Computer and communications services that depend on knowing exactly where a person (or object) is located at a particular time
    - » Global Positioning Systems (GPS), cell phones
    - » Radio Frequency Identification (RFID) tags
      - Small devices that contain a computer chip and an antenna
      - Antenna transmits and receives radio signals for communicating with devices that read the tag
      - Inserted in many objects to track them through manufacturing and distribution
      - Government has proposals to embed RFID tags in various documents such as passports (although there are still a lot of security issues with RFID)
    - » Track pets, children, people with Alzheimer's disease
    - » Some schools have even proposed removable tracking devices for students
      - What do you think parents and students think of this idea?
    - » How do we protect ourselves from thieves, nosy neighbors, stalkers, divorce lawyers, people who object to our religion, politics, lifestyle, etc.?

How Can We Protect Our Privacy?

- How can we gain some semblance of control over this personal information?
  - Social norms-based solutions (privacy policies, consumer education)
    - » Allow the companies to self-regulate (may be likely to do so in order to avoid oppressive government intervention)
  - Technology-based solutions (encryption, cookies cutters, anonymizers)
  - Market-based solutions (privacy policies, consumer demands)
  - Legal protections (U.S. vs. Europe)

Fair Information Practices

(What Should Firm Privacy Policies Look Like?)

- Notice (awareness)
  - What data is being collected?
    - » Inform people when personally identifiable information about them is collected
    - » Only collect data that is needed to perform the task
  - How is the data collected?
    - » Cookies? Spyware? Web beacons? Surveys?
  - What is the data usage policy?
    - » Identify specifically what the data will be used for (e.g., completing a purchase, providing customized product offerings, secondary uses, etc.)?
    - » Develop policies to destroy records that are old or no longer needed
- Choice (informed consent)
  - Give users some control over secondary uses of their data
    - » Opt-out options
      - Consumer is notified upon collection that his personal information will be used for secondary purposes unless he disapproves and notifies the company
      - Offer people a way to opt out from mailing lists, advertising, transfer of data to other parties, and other uses of data (i.e., uses not specified during collection)
      - e.g., consumer can click a box on an agreement to request that their information not be used in a particular way

Fair Information Practices

(What Should Firm Privacy Policies Look Like?)

- Choice (informed consent)
  - Give users some control over secondary uses of their data
    - Opt-in options
      - Consumer must explicitly approve each secondary use (i.e., a use other than specified during collection or as required by a contract) of his personal information
        - e.g., with opt-in, if you fill out a bank loan application and provide credit data the bank cannot sell that data to a marketing company without your explicit permission
      - Provides stronger protection for sensitive data (e.g., disclosure of medical data)
- Integrity (security)
  - Provide protections and safeguard from data theft or modification, unauthorized access, accidental leaks, or other disclosures
- Access (participation)
  - Provide a way for people to review/access personal information, challenge its correctness, and have it changed
- Enforcement (redress)
  - Compliance verification, dispute resolution, and remedy

Fair Information Practices

(What Should Firm Privacy Policies Look Like?)

- Develop policies for responding to law enforcement requests for data (announce it and follow it)
  - Some companies give up data to law enforcement and government agencies upon request
  - Some companies give up data when served with a subpoena or court order
  - Some challenge the court orders
  - Some inform consumers when they give personal data to law enforcement and government agencies
- Note the limitations of these Fair Information Practices
  - These principles primarily address privacy issues related to large DBs of businesses and government
  - These principles do not do much to address the use of public video surveillance or when individuals supply huge amounts of personal data about themselves to the public (e.g., via MySpace or Facebook)

Fair Information Practices
(What Should Firm Privacy Policies Look Like?)

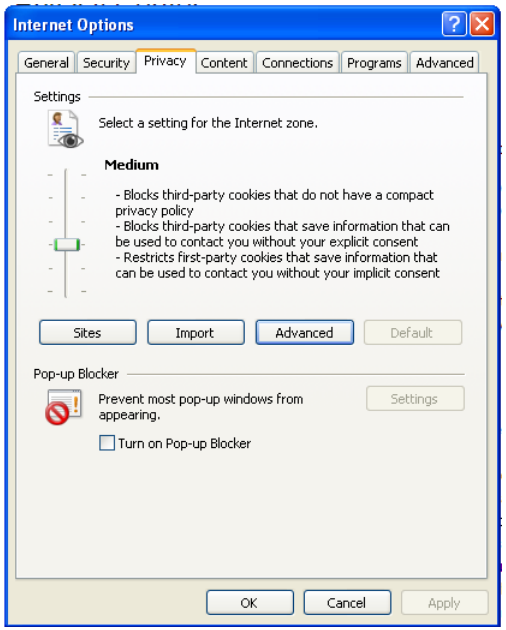
- Let's reconsider Google's Search Query DB again
  - Privacy advocates want to prevent collection and storage that allows identification or re-identification
  - If a user does not register or subscribe to some service of Google.com he has not viewed or accepted Google's privacy and information sharing policies (i.e., there is not informed consent)
  - People use Google.com and other search engines without registering
  - What should be done to be consistent with Fair Information Practices?
    - » Since there is no agreement and most people do not expect search query data to be collected and users may expect a privacy-protecting default that specifies that Google will not store or use the data beyond the purposes of the search in a way that can disclose a person's search data
    - » Or should the expectation that by using a free search tool you have given Google consent to collect and use the data for secondary purposes?
    - » No matter what, Google should provide a clear and visible link to its privacy policy regarding collection and use of search query data

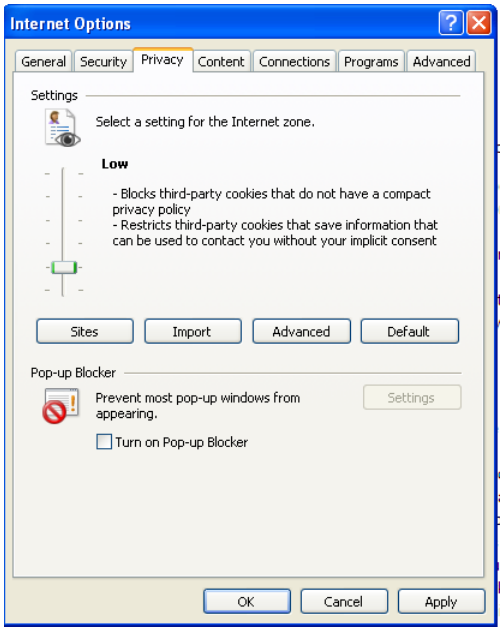
Fair Information Practices
(What Should Firm Privacy Policies Look Like?)

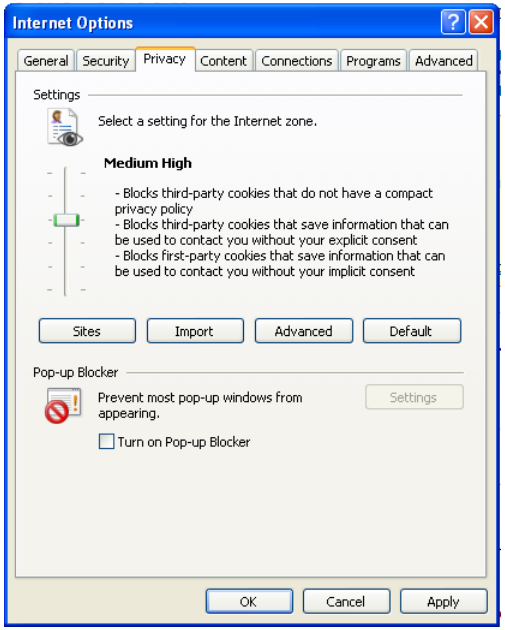
- Examples of Privacy Policies consistent with the Fair Info Practices
  - Google.com
    - » Google Privacy Center
    - » Google Privacy Policy
    - » Interesting note in Google's Privacy FAQs
      - Question: I have targeted ads on Gmail – is someone actually looking at what I write to match the ads with my emails?
      - Response: "Like most email services, Gmail uses software to scan emails for viruses and to filter out spam. Google uses this same kind of software to scan for keywords in users' emails which we can then use to match ads. When a user opens an email message, computers scan the text and then instantaneously display relevant information that is matched to the text of the message. Once the message is closed, ads are no longer displayed. The whole process is automated and involves no humans."
  - Amazon.com
    - » Amazon.com Privacy Notice
  - Walmart.com
    - » Walmart.com Privacy Policy

Technology-Based Solutions

- Data encryption
  - We will discuss this during “Computer Crimes and Security”
- Cookie cutters
  - Utility programs (usually free) that prevent Web browsers from exchanging cookies with Web sites
  - Web browsers have the capability to deal with cookies (uses P3P)

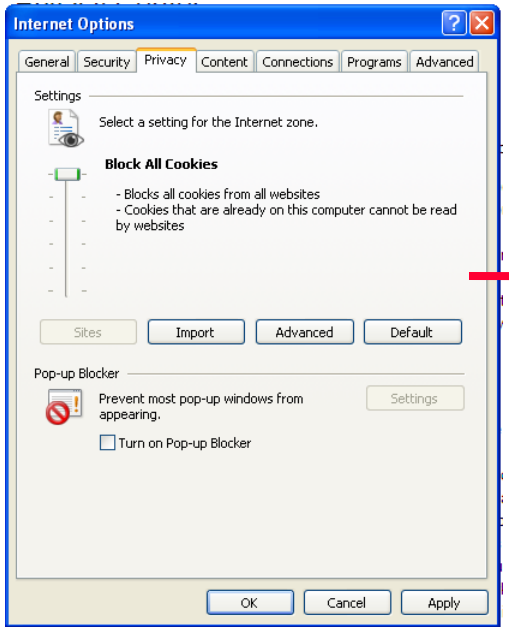


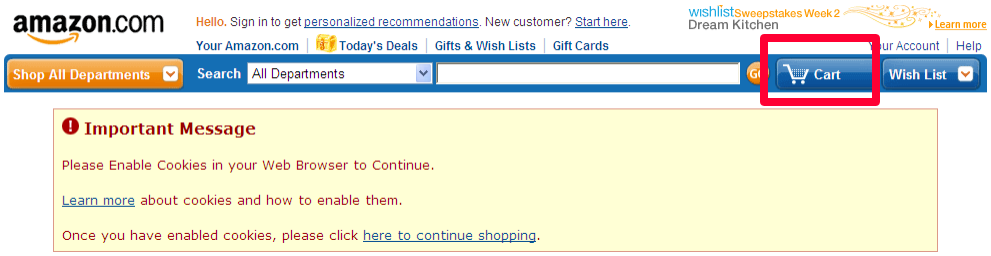




Technology-Based Solutions

- Cookie cutters





Technology-Based Solutions

- Anonymous remailers
  - Tools and services designed to help individuals surf the Web or send email anonymously (no link to IP address)
  - Some services rely on a series of trusted third-parties that strip off identifying information and forward requests on behalf of a user
  - Not much use if you need to do transactions that require personal info
  - Anonymizer (www.anonymizer.com)
    - » Anonymous Web browsing program that does not accept cookies and hides your IP address so that people cannot track your surfing or build profiles
    - » Redirects your Web surfing through their servers (128-bit SSL technology - like a bank)
    - » Latest version of Mozilla Firefox supports Private Browsing (under the Tools tab)
- P3P and identity managers
  - Platform for Privacy Preferences (P3P)
  - http://www.w3.org/TR/P3P/
- Automated privacy audits

Marketplace Solutions

- Pressure from customers and competitor
  - Privacy policies (firm-level)
  - Is this enough?
  - Are consumers sufficiently informed on the issue to take decisive action? Are they sufficient energized about the issue of privacy?
  - What about enforcement?
- What else can consumers do?
  - Stop putting so much personal data (e.g., contact information, pictures) on blogs and social-networking sites
    - » Especially data that may cause problems with parents, future employers, and law enforcement
    - » By sharing our data with outside companies and entities we put ourselves at risk
  - Be aware, find and read privacy policies, and make informed decisions
  - Is there a generational difference? Is it that young people do not care about privacy or is it that they do not sufficiently understand the risks?

Social Norms-Based Solutions

- Third party enforcement (or seal) programs
  - Online Privacy Alliance (http://www.privacyalliance.org/)
  - Network Advertising Initiative (http://www.networkadvertising.org/)
  - Direct Marketing Association (DMA) (http://www.the-dma.org/privacy/creating.shtml)
    - The DMA's Privacy Policy Generator
  - Privacy seal programs
    - TRUSTe (http://truste.org)
    - BBB Online (http://www.bbbonline.org)
  - How effective are these in the real world?

Law Solutions
(U.S. Approach)

- U.S. Constitution?
  - No explicit mention of “right to privacy”
  - Supreme Court has interpreted to imply a right
- State Constitutions?
  - Some offer better protection than others
- Federal/State Legislation
  - Piecemeal approach
- Common Law - Simple tort protections
  - Intrusion on solitude; public disclosure of private facts; publicity that places person in a false light; appropriation of a person’s likeness for commercial purposes

Law Solutions
(U.S. Approach)

- *Reactive, piecemeal* legislative acts in U.S.
  - Fair Credit Reporting Act (1970)
  - Family Educational Rights and Privacy Act (FERPA) (1974)
  - Right to Financial Privacy Act (1978)
  - Cable Communications Policy Act (1984)
  - Video Privacy Protection Act (1988)
  - Driver Privacy Protection Act (1994)
  - Children's Online Privacy Protection Act (1998)
    - » Examples of violations include BonziBuddy and UMG Recordings
  - Gramm-Leach-Bliley Act (1999)
  - Health Insurance Portability & Accountability Act (HIPAA) (2001)
  - Sarbanes-Oxley (SOX) Act (2002)
  - Genetic Information Nondiscrimination Act (GINA) (2008)

Law Solutions

(European Comprehensive Approach)

- Europe sees privacy as “data protection” and “basic human right”
- Data Protection Directive: Directive 95/46/EC
  - Sets forth Fair Information Principles the EU members must implement in their own laws
  - The protection of individuals with regard to:
    - » Processing of personal data and
    - » The free movement of such data (between companies)
  - Customers must be notified of the collection and use of data about them
  - Personal data may be collected and used only for the explicit purpose specified and must not be processed for incompatible uses (i.e., no secondary uses without explicit consent of the customer)
  - Data must be accurate, up-to-date, and not kept longer than necessary
  - Can only process data with customer consent (opt-in requirement) unless processing is necessary to fulfill contractual obligations (or if processing is necessary for tasks in the public interest)

Law Solutions

(European Comprehensive Approach)

- Data Protection Directive: Directive 95/46/EC
  - Companies cannot process sensitive data (racial/ethnic origins, political/religious beliefs, health and sex life issues) at all without explicit customer consent
    - » Processing of data about criminal convictions is severely restricted
  - Customers have the right to see the processes and to access and correct their data
  - Accountability (bureaucratic infrastructure to monitor compliance)
    - » Requires each firm to designate one or more employees as a data controller
      - ◆ Responsible for processing data, registering with government, and contacting
        - Purpose, description of data subjects, those who may receive the data, proposed transfer to other countries, and assurance of security
    - » Requires a dedicated government (national) privacy agency
      - ◆ Firms must register DB with the agency and may need to get prior approval before processing personal information
      - ◆ Investigates data processing activities and monitors application of Directive
      - ◆ Intervenes to ban processing of data or to destroy data
      - ◆ Authorized to hear and resolve complaints from data subjects
    - » Requires legal framework for courts to follow
  - Onward Transfer: European firms cannot give customer information to any firm in any country that does not have the same level of protection as set under the directive

Law Solutions
(European Comprehensive Approach)

- What are the downsides of such comprehensive regulations?
  - Costs to firms of compliance
  - Costs to firms and government of monitoring and enforcement
  - Legal costs
  - Who protects companies from the government invading its right to privacy? (Big Brother vs. Little Brother)
    - » There do not seem to be restrictions on the processing of data by government agencies
    - » European governments actually require ISPs and telephone companies to retain customer records for up to two years and to make them available to law enforcement agencies (says it is need to fight terrorism and organized crime)
    - » I guess "Big Brother" knows best!
  - May hinder e-commerce transactions between European and U.S companies (i.e., the onward transfer requirement)
  - Enforcement has been relatively weak to this point
    - » However, at least people have legal recourse to protect their privacy

Safe Harbor Program

- Provides way for U.S. companies to comply with the European Data Protection Directive
  - July 2000
  - List of participants (http://www.export.gov/safeharbor/)
  - Companies outside of the EU that agree to abide by a set of privacy requirements similar to the Data Protection Directive may receive personal data from the EU companies
- Principles
  - Notice, Choice, Sensitive information (opt-in requirement)
  - Onward Transfer
    - » can only give info to firms that have same level of privacy protection
  - Security, Data integrity, Access, Enforcement
  - *No requirement for national agency* or *data controller* for Safe Harbor participants
- Interesting observation
  - 2001 study by Consumers International found that only 20% of European Web sites did comply with the requirement that Web sites provide an opt-out option while 60% of the most popular U.S. Web sites offered an opt-out option

Privacy Protection
(European Comprehensive Laws)

- E-Privacy Directive: Directive 2002/58/EC
  - Specific data privacy rules for the e-communications sector
  - Controls on sending SPAM by email, fax, and automated calling machines
    - » Can only be sent to individuals if sender has received "prior consent" to use contact details to send electronic marketing communications (more relaxed if individual is existing customer)
    - » Must clearly identify message as SPAM and offer opt-out option
    - » Must respect opt-out registers
  - Rules on the use of cookies by Web site operators
    - » Can use without "prior consent" but must provide clear and comprehensive reasons and explanation of what information will be stored on user's computer
    - » Must give right to refuse cookies
  - General data retention rules
    - » Must be erased or anonymized when no longer needed for intended purpose

Rationale for Comprehensive Laws by Europe

- To remedy past injustices
- To promote electronic commerce
- To ensure laws are consistent with Pan-European laws

Europe vs. U.S.

- European prescription for privacy
  - Comprehensive laws
- U.S. prescription for privacy
  - Legislation for sensitive data
    - » e.g., HIPAA, Children's Online Privacy Protection Act, Gramm-Leach-Bliley Act
  - Industry self-regulation with technology support for click stream / purchase data
    - » P3P, audits, privacy seal programs, anonymous remailers, cookie cutters, etc.

Example

- Students who live in a dormitory on a college campus are given cards with a magnetic strip that opens the front door of the dorm. Students are not told that each card contains the individual student identifier and that a record of each use of the card is stored.
  - What are the possible good purposes of such record keeping?
  - Is it right?
  - Is it OK if students are told?
  - Give arguments and examples to support your answers

Example

- You are the CPO of a midsized manufacturing company, with sales of more than $250 million per year and almost $50 million from Internet-based sales. You have been challenged by the VP of sales to change the company's Web site data privacy policy from an opt in policy to an opt out policy and to allow the sale of customer data to other companies. The VP estimates that his change will bring in at least $5 million per year in added revenue with little additional expense. How would you respond to this request?

Summary

- We have a right to privacy
- IT invades that right
- How do we protect it?
  - Technology and education (consumer awareness and action)
  - Privacy policies (firm, marketplace)
  - Privacy norms (industry self-regulation)
  - Laws (government)