

# Privacy

Consider supermarket affinity cards.

a) One of my students in 2005 received a call from her supermarket that there was a product recall on a particular brand of smoked salmon, and she had bought a package recently, and would she please return it for a refund (actually she had already eaten it without ill effects).

b) Somebody suing a California supermarket over an alleged parking-lot slip-and-fall injury was told that if he brought it to trial, the supermarket would bring forward the records of how much alcohol he had bought.

# Government programs

Most people are more worried about these, although you are well off ignoring any webpage that talks about black helicopters, the grassy knoll, or Waco.

Echelon: NSA eavesdropping on foreigners

Carnivore: FBI tracking messages to and from domestic computers.

Magic Lantern: alleged FBI keystroke logger

TIAS: total information awareness system

# Private snooping more common

September 2006: Hewlett-Packard scandal. This was pretty much old-fashioned fraud via “social engineering”: HP's private detectives, searching for the source of a leak in the HP board of directors, rang up phone companies pretending to be customers to gain access to their bills. The intent was to look through the phone calls made by the directors and by some news reporters to see who might have made the call.

The real policy question is that new crimes like this sometimes aren't clearly illegal. This one, however, seems to have already been dealt with under the various eavesdropping statutes.

# Collaborative filtering

Best known as the Amazon feature “other people who bought this book also bought...”

Was invented, I would claim, by Will Hill, Jim Hollan and George Furnas at Bellcore in the early 1990s.

It's now a standard way of marketing that is perceived valuable by many users.

It can be done somewhat without tracking individuals (by tracking sessions) but it will work better by tracking specific users.

# Gathering information

You can build better search engines by looking at what pages other people who typed the same query looked at. Every large search engine vendor has employees who do the most common searches and pick out good answers to be remembered. And they look at what other people who do searches find.

You can recommend movies or restaurants to people by gathering comments and web clicks.

Sometimes you can do this anonymously; but you can do better by remembering your choices from session to session.

# Other environments

It is difficult to talk to anyone without being seen. But it has been OK to walk into a store, look at prices, ask some questions, and walk out without giving a name and address.

Postal mail has return addresses as a matter of courtesy.

“caller-id” had many opponents when announced but now seems to be accepted

Newspapers will usually not print letters-to-the-editor if unsigned; they will frequently not print the name if there is a reason.

# What's known on the internet?

When you access a website, your IP address can be captured, and the exact time.

With the cooperation of the ISP, that information can be turned into your name and address.

Each website is at an IP address, and the “whois” registry will tell you who owns the website. There are registrars who at least tolerate people who give fleeting addresses.

When you access a website, it can fetch from your browser the “cookies” and the history.

# What does society want?

There are traditional national differences. For example, the US and UK have a history that there are no “national ID cards”; in most of continental Europe they are standard. Or, to exaggerate (and go back a few years):

In Britain everything is permitted except that which is prohibited.

In Germany everything is prohibited except that which is permitted.

In Russia everything is prohibited, including that which is permitted.

In Italy everything is permitted, including that which is prohibited.

# No real consistency

As a result of a Washington newspaper publishing Robert Bork's videotape rentals (A Day at the Races), we now have a law making videorental information private.

Gun purchases may be done anonymously (at gun shows) and Federal records of other purchases can be kept only 24 hours.

By contrast, airline passenger records are more carefully checked and kept indefinitely.

# Where it started

“The Right to Privacy,” by Samuel Warren and Louis Brandeis, 4 Harvard Law Review 193, (1890).

“...the right 'to be let alone.' 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." For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons;<sup>11</sup> and the evil of the invasion of privacy by the newspapers, long keenly felt, has been but recently discussed by an able writer.”

# Brandeis

Brandeis argued that that everyone has “the right to decide to what extent his thoughts shall be communicated to others” by extension of copyright law. He dealt with publication of unwanted statements about a private individual, making exception for matters relevant to a public office that a candidate might be seeking.

He didn't look into merely the collection of information about an individual or its use for commercial gain.

But he was the first to hold in law principles which had previously been rules of etiquette.

# “Weblining”

Nowadays if you call a customer service representative about something, they typically have your entire history on the screen; the treatment you get may well depend on whether you are rated a profitable or unprofitable customer.

Of course, this is not all that different from the notes you see in small stores at the cash register with lists of people whose checks are to be refused.

But people don't know it's happening.

# Why might “weblining” be good?

“consumer activists have expanded the concept of weblining to apply to virtually any selective use of individual data on risk characteristics. While we do not wish to call into question prohibitions on the use of some classification variables such as race or religion, the mantle of privacy is being increasingly used to justify cross-subsidies between all manner of interest groups. Continuation of this tactic promises to erode the many efficiency gains in the insurance market made possible by e-commerce.”

(Competitive Enterprise Institute).

# Storage is cheap

It is now practical to imagine saving vast quantities of data. Each year in the US some 60 billion phone calls are made and some 200 billion pieces of mail are delivered.

Suppose it took 100 bytes to save the originating and terminating addresses of each. At 50 cents per gigabyte, that would be \$3000 worth of disk space for the phone calls and \$10,000 for the mail. Google gets a billion queries a day; again, even if they were 100 bytes long (well, we want to write down the originating IP address, time of day, etc) that's \$20,000 or so. Not a problem to keep everything.

35 billion email messages per day at 2,000 bytes each would be \$35,000 per day to store. Don't think the ISP don't do that.

# Health data

There is a very strict law about privacy of medical data: HIPAA, or the Health Insurance Portability and Accountability Act. However, if you actually expect to both get medical care and get reimbursed by your insurance company, you pretty much have to sign all the releases.

At least, however, other entities (employers, lenders, etc) should not be able to get at your health data.

Shared health data can help you: for example, detecting drug interactions, letting you renew prescriptions while traveling. And it can help you indirectly by reducing fraud.

# Video cameras

There has been a recent explosion of video cameras in the US: there are now 26 million of them (2005, "Privacy.org"). You can assume that every intersection in a major city is watched. An NYCLU search as far back as 1998 found 2300 of these cameras in Manhattan.

90%, by the way, were private, not government.

The UK has had a high density of video surveillance for more than a decade and people seem to accept it.

# Data in marketing

Providing personal information, whether deliberately or through surreptitious observation, can have benefits:

- better recommendations
- faster online shopping
- tailored services (what kind of airline seat you like)

It can also have disadvantages

- price discrimination
- denial of service
- risk of identity theft

People seem more tolerant of this compared with government data gathering partly because they don't see how what the government does could possibly help them.

# Privacy policies

Many websites have privacy policies, but often they are completely useless; remember that “we can share your data with selected marketing partners” means “anyone we choose”.

There is also a problem that many sites update their policies and it is really difficult to keep track of the changes (nor, if you have become accustomed to a particular site, is it necessarily easy to move to an alternative).

# Service or Snooping?

It can be hard to decide whether, for example, somebody who offers you free email if they get to look at the words in your email and send you targeted advertising, is providing an attractive financial offer or merely invading your privacy.

The absence of a history of using data in ways you wouldn't want is not a promise that it won't be used that way in the future.

E-Z Pass records, for example, have been delivered on request to police doing crime investigations and lawyers involved in divorce suits. (On “Law and Order” the detectives constantly use Metrocard records to find out where people have been).

Cellphones can locate themselves; perhaps good for 911 and children, but adults may have a different feeling.

# Summary

How much data gathering should be allowed, and by whom? The EU has very strict data standards; only the minimal data needed can be kept, and people must have the opportunity to correct data about themselves.

We haven't yet decided, as a country, the relative importance of privacy and efficiency (let alone law enforcement).

Nor, to my view, has the importance of transparency (you should know what is going on) been recognized.

And I regret to suggest that the public attitude is largely going to be dependent on the specific examples that become news stories.