Maps are one of the oldest communication mediums for conveying spatial information, but... and as we’ll cover in the first section of this presentation...

- They are not value neutral;

- Nor are they objective representations of geographic phenomena;

- And often serve as instruments of either overt or subtle manipulation.
Maps as political tools

- Maps are one of the oldest communication mediums for conveying spatial information, but...

  - They are not value neutral;

  - Nor are they objective representations of geographic phenomena;

  - And often serve as instruments of either overt or subtle manipulation.
Critical cartography

- Common assumption is that there is a natural relationship between maps and territory
Maps depend on subjective views of space, and...

Maps are constructed based on culturally specific ideas and visual language (e.g. signs, symbols).

Objective appearance can hide cultural and social agendas.
Maps shape viewpoints

- Maps don’t merely reflect social relations... they also shape them as space can be delineated, identified, or claimed.

- For example, it is impossible without maps to develop and naturalize concept of property.
GIS and society

- Mapping involves **abstraction**
  - Subjective process.
  - What info is left in/out? What info is emphasized? De-emphasized?

- Colonial maps and planning maps have evidence of power relationships.
  - Military Applications
  - Surveillance
  - Privilege of access
  - Marginalization
  - Representation
Military applications

- 1970’s Tom Poiker (TIN) at SFU picketed by anti-war protesters (funding from US military interested in terrain modeling)
  - GoogleMapping Wars

- Should universities support GIS/military research?
Any new technology brings with it a set of previously unencountered ethical problems.

E.g. printing press; GIS.

New technologies force people to confront new rights and opportunities.

Technologies need to be integrated into the larger social fabric.
Issues

- Privacy and geo-demographics
- Privacy and digital technologies
- Privacy and the law
Erosion of privacy?

- Geodemographic databases have proliferated over the past ten years.
- Data collection at point of sale.
- When data-intensive GIS of any kind are connected to GPS and/or satellite imagery, you create a system of great power.
- John Pickles, a noted GIS critic has referred to such systems as *cybernetic grids of control*.
- Geodemographics associated with “an erosion of traditional forms of the private and the public” (Curry, 1998, 100).
Responses to privacy issues

- Various reactions to this loss of privacy.
- In the US, prevalent sense that this loss of privacy will create a greater morality.
- Use of video cameras on street cameras, at ATMs, and in airports.
- Some people walk to work and spend all day under surveillance.
- Less obvious is the continual gathering of remotely sensed imagery.
- Most homes are subject to remote sensors several times during the course of each 24-hour period.
Response 2

- Night of living dead.
- Is “normal behaviour” clearly defined?
- Increasing social transparency leads to complex questions about what is acceptable behavior.
Response 3

- Change in public/private division through history (Curry).
- Erving Goffman and the two stages.
Response by country

- US
- Canada
- Europe: more public discussion about privacy.
- Changes in regulations since the 1970s; tighter regulation of the use of personal data.
Europe today

- Series of regulations that very strictly regulate the flow of personal data.
- It is illegal to conduct telemarketing in Europe.
- Telemarketing rarer in Canada than the US.
- Trade dispute between the US and the EU over the buying and selling of personal data.
Buying and selling digital data

- On Oct 26, 1998, the EU passed a law prohibiting American-style data selling.
- Goal is to prohibit Eur companies from using or selling information about their customers in a way that the customers never intended.
- Law affects everything from credit card data to magazine subscriptions to electronic footprints that we leave when we visit web sites (cookies).
Anti-telemarketing

- Law prevents any company from doing business with any company in the world that does not respect the same guidelines.
- American companies argue they should be able to *self-regulate*; *laissez faire* economics.
- EU argues that we need to build a society based on trust and privacy.
The Canadian case

- In Canada, Bill C-6 went before the House and the Senate in November, 1999.
- “Personal Information Privacy and Electronic Documents Act” entails many of the provisos to ensure privacy of individual data as Europe has.
- Risk losing European business.
Privacy and the law

- 19th Century: home includes curtilage.
- For the purposes of the law, this area was a person’s private sanctuary.
- This area of privacy extended to the automobile, the workplace and the telephone through a series of legal rulings.
Privacy extended outside the home

- General trend through the 20th century of extending area of privacy.
- Example of car shooting as self-defense.
Technology as an aid in law enforcement

- Courts have allowed increasingly powerful technologies to enforce the law.
- In 1986, in a California court case, the police flew over a backyard at a height of 1,000 feet and identified marijuana plants.
- Courts protected the flying public.
- In a 1989 Florida case, police flew over a house using a helicopter at a height of 400 feet to see through a greenhouse in which marijuana plants were growing.
In Hawaii, police in a helicopter used an infrared camera to detect heat emitting from a garage where a heat lamp was being used to grow marijuana.

Police gained a search warrant.

Vision-enhancing techniques to make visible what was previously imperceptible.
Power to the government (US case)

- Individual privacy loses at expense of police enhancement.
- While the circumference of what is legally defined as private has grown to include the car and telephone, police have at the same time, increased their use of technology to observe.
- These trend has extend to the net (e.g. clipper chip debate; AT&T phones)
The Canadian case

- *Globe & Mail, Winter, 2003:* “Your home is your castle – right down to the heat that leaks out of it.

- Ontario Court of Appeal extended the right of privacy to intrusive technological advances by acquitting a man accused of growing marijuana hydroponically.

- The grow-op was detected by police as they flew overhead with infra-red equipment.
The judgement stated “The nature of the intrusiveness is subtle, but almost Orwellian in its theoretical capacity.”

The Court ruled 3-0.

Police must henceforth obtain a search warrant for a fly-over in Ontario.

Defense: “this is the essence of freedom... why should the police know whether someone is taking a sauna, firing a kiln, growing orchids, or growing marijuana?”

Technologies of this sort are called “off-the-wall” as inferences can be drawn without going near the home.
Accessibility of data

- Not only police and governments have access to geographical data.
- NYT article, Sept 22, 2002 “A Place to Find Out for Yourself About the War”
- Satellite imagery illustrating US and Iraqi build-up of troops and weaponry is freely available to anyone.
- Corona project protected imagery for US until 1972.
- First remotely sensed image showed huge forest fire burning in Alaska.
Data availability changed in mid-1980s when the French launched the first for sale satellite images.

Low quality, but great coverage.

In 1999, Space Imaging, a US company launched high-res Ikonos satellite.

US Dept. of Defense has tried to control imagery since the public release of LandSat in 1970s.
Foreign sales of imagery

- 1992 law allows the government to declare any part of the earth off-limits to American commercial satellites in order to “meet significant national security or significant foreign policy concerns.”

- US now considering “space blockades” against foreign companies they suspect of selling images to a terrorist group.

- Other countries that sell imagery include Canada, India, Russia, and France.

- Major Robert Fabian, former chief of space control strategy, suggests that a more lasting solution be invoked if foreign companies sell to suspected terrorists: “lethal enforcement” (physical destruction of the satellite).
On-line privacy

- In 1998, the EU created strong on-line privacy regulations.
- Rules prohibit EU companies from transmitting sensitive personal information to countries that lack strong privacy laws.
- EU threatens to cut data lines to the US.
- In order to continue doing business with Europe, Canada adopted a policy that meets the EU’s on-line privacy requirements in 2000.
The US holds out

- The US has, however, opted to promote “safe data harbors” or voluntary pledges to abide by privacy codes rather than impose federal regulations.
- Privacy advocates are suggesting a work-around in which companies get consent before collecting on-line personal information.
- Congress may have to act in order to continue to participate in world data trade.
Social networking and privacy

- What Would You Want a Friend of a Friend of a Friend to Know about You?
- Facebook changed its privacy criteria and options in 2009 in response to a ruling by the Canadian Privacy Commission.
- Identity theft is also prevalent on social networking sites.
Case example

- An individual created a false account on a social networking site with personal information and an image of a particular person (a Dad with 2 daughters).
- The impersonator used the account to “friend” the daughters. They accepted the friend request and the impersonator was able to view their accounts.
- The same day, the impersonator began to harass the daughters. He first posted a threatening message about the father on one daughter’s wall.
- The daughters quickly realized that this person was not their father.
- They notified their real father, and the site, and in response the site deleted the account in question. However, both father and daughters believed that the site lacked control mechanisms when accounts are created to prevent identity theft.
Geo-surveillance technologies

- Devices on the market use satellites to locate and track people anywhere in the world (digital angels).
- Companies make chips to keep track of livestock and pets.
- Threat of “geo-slavery”; alarm sounded by GIS researchers including Jerome Dobson.
An example: SmartLabels

- Smartlabels are new merchandise tags that contain inventory information so that large supermarkets can better control supplies and track buyers.
- Smartlabels retain their intelligence, however, after they pass through the till.
- Specific products are linked to the customers that buy them based on customer data associated with debit and credit cards (as well as loyalty cards).
- Products bought with Smartlabels can be traced to individual households - a spatial form of consumer intelligence gathering.
Resistance to SmartLabels

- Early opposition to Smartlabels has resulted in the development of a "kill" command which allows the customer to turn-off the Smartlabel at the till.
- Gillette Razor and Walmart supermarkets are early adopters
Disseminating geospatial information

- So far, we have focused on collection of geospatial data about individuals.
- There are a number of ways that geographic information can be disseminated in ways that threaten privacy.
- A classic example is the 1991 Lotus MarketPlace CD.
- Lotus corporation, developers of huge spreadsheets, compiled a CD with information about many of the US’ 7 million businesses and 120 million households.
Lotus CD

- They intended to first market the business CD, followed shortly by the household CD.
- But 30,000 consumers wrote or telephoned the corporation asking for their names to be removed from the disk.
- Lotus replied that it was too late for the first edition, that they could only comply in future editions.
- The public pressure, however, forced them to retract the CD and abandon the project.
- Would that happen today?
Implications of disseminated data

- The implications of such data circulation are profound.
- What if the information about you, including credit information, is wrong?
- E.g. hard to recall defective Ford Pintos let alone 1 millions CDs.
- Lotus’ defense was that that information was freely available anyway.
- And it was. That information could be collected, for a price, from a variety of data vendors.
- What Lotus did was round it up and package it.
- With that many entries, however, it was impossible to check for error.
- Problem of skeletal digital personae.