Ethics, privacy and legal issues concerning GIS

This is lecture 12
New technologies; new laws

• 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.
- When data-intensive GIS of any kind are connected to GPS and/or satellite imagery, you create a system of great power.
- 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.
Response 2

• Increasing social transparency leads to complex questions about what is acceptable behavior.
Response 3

• Change in public/private division through history (Curry).
Response by country

- US
- Canada
- Europe
Europe today

- Series of regulations that very strictly regulate the flow of personal data.
- 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.
Anti-telemarketing

• 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.
Privacy extended outside the home

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

- Courts have allowed increasingly powerful technologies to enforce the law.
- Courts protected the *flying public*.
Technology 2

• Vision-enhancing techniques to make visible what was previously imperceptible.
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.
The judgement stated “The nature of the intrusiveness is subtle, but almost Orwellian in its theoretical capacity.”.

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.
SPOT

• 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.
• 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.
Geo-surveillance technologies

• Devices on the market use satellites to locate and track people anywhere in the world (digital angels).

• 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.
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.
• The public pressure, however, forced them to retract the CD and abandon the project.
Implications of disseminated data

• The implications of such data circulation are profound.
• What if the information about you, including credit information, is wrong?