online at http://www.innovativegis.com/basis/Misc/Geoslavery_event/ (*download .pdf*)

Notes from…

Geoslavery or Cyber-Liberation: Freedom and Privacy in the Information Age

Bridges to the Future 2005-2006 Event
Wednesday, September 14, 2005, 7:00-9:00 pm
University Of Denver Campus

…prepared by Joseph K. Berry for follow-up discussion group, Thursday, September 22, 2005

This Forum was part of the University of Denver's "Science, Technology and Values" program—what is the difference between "science" and "technology"? Is the distinction relevant to the issue of freedom and privacy?—and what is the difference between these concepts?

Dobson made several points in his opening remarks—

- Geosalvery and Cyber-Liberation are not mutually exclusive
- "Electronic Fence" and "Human Tracking"; imagine Ann Frank with a geo-positioning device locked to her body
- Governmental, Corporate and Private as different levels of "watchers"; citizens, employees, shoppers, children, spouse, animals and things as different levels of "watched"
- Positive tracking as Alzheimer's patients, backcountry hikers/skiers, goods shipped, onboard emergency tracking, stolen car, other?
- Tradeoff between privacy and freedom; what conditions modify the balance?

Haag made several points in his opening remarks—

- Cyber-Liberations contribute to a culture free independence; freely express opinions, level playing field for dialog (blogs)
- GPS enabled golf cart identifies distance to hole, obstacles, club recommendation, etc.; cart shutdown if off course;
- GPS enabled shopping carts provide wheel lock outside of parking lot; data for spatial data mining of in-store purchases
- E470 electronic toll devices provide ease of travel/convenience but records date/time/place of travel
- Must balance Benefits (Liberate) with Costs (Enslave)
- Geotechnology is like accepted previous technology; telephone, automobile, airplane, etc.

Keating made several points in his opening remarks—

- Personal Privacy versus Public Security; call police (security violated) if there was house break-in not the ACLU (privacy was violated)
- Police surveillance cameras require private citizen give up some privacy for some security
- "Mice and Elephants" in my life; depends on the importance of the issue and the amount of privacy or security that is involve; don't fret over "mice"

Zimmermann made several points in his opening remarks—

- Moore's Law of technology evolution (computing power for the same price doubles every 18 months) combined with improving and more prevalent surveillance means that the ability to track with more detail is increasing at an exponential rate (Capacity)

- The ability to fuse and interpret disparate information is increasing at a exponential rate; geographic position and time are very powerful “universal codes” that can link databases; WHAT is WHERE and WHEN can couple previously disparate databases (Capability)
- Rapidly developing technology is not guided by policy; opposite is the case (technology drives policy (forces a reaction from)
- After 911 it appears that policy is actively utilizing technology; Patriot Act as long sought set of procedures underwriting increased surveillance (librarians’ objection of privacy rights lost for gain in security); 911 was the catalyst for civil liberty “turn-back” that had long been sought by law enforcement
- Technology can be “used for things we did not intend”
- Analogy of submarine (civil liberties) constantly exposed to the relentless pressure of the sea (erosion of privacy/freedom); mentioned Seinfeld episode of and overdue library book from 1971 (technology and ability to merge datasets)

Moderator Sterett saw several threads in the opening remarks for follow-up—

- What are some “practical” things that can be done to protect privacy and strike an appropriate balance between Privacy/Cyber-Liberation and Security/Surveillance (subclass Geoslavery issue was lost)
- How do we maintain an appropriate amount of “Wiggle Room”; “right to do the wrong thing” without harming others (e.g., Stanley vs. Georgia concerned with illegal pornography in a teenager’s bedroom)
- Internet (and other electronic mediums) makes it much easier for surveillance of citizens ; loss of wiggle room

Zimmermann response—

- Most countries have a privacy commission (Europe, Canada) but corporate opposition in US
- Put a limit on the retention of privacy sensitive records (e.g., phone records destroyed after bill is paid)

Keating Response—

- Credit card companies simply pass through losses incurred by identity theft; no marketplace incentive to strengthen identify theft policies

Haag responses—

- Instilling core values in children (K-12); respect privacy and take responsibility
- Recognize that privacy is a dynamic process and must be thought of as relative so continually evolving (not an absolute); requires constant policy focus on identifying new threats created by technology and be in a position to have policy lead (instead of react) to advancing technological developments

Dobson response—

- Doesn’t hear a current groundswell of concern; Roberts hearing focused on “flash” issues (e.g., abortion) not endemic social issues (e.g., privacy); a public debate needs to be initiated and be energized enough to get on the public’s and policy maker’s radar

Zimmermann response—

- Robert's thought there was a right to privacy in the constitution; legal question if it is an implicit or explicit 'right"

Dobson response—

- Difference between privacy in a private place and privacy in a public place; is there a right to privacy in a public space …how much?

Zimmermann response—

- There is an expectation of privacy; telephone clip[per-chip as backdoor for wire taps …if implemented then there shouldn't be an expectation for phone conversation privacy
- Triangulation on gunfire (sound) for positioning and surveillance cameras seem to be encroaching on the expectation of privacy in a public place
- As technology advances it erodes implicit privacy expectations; giving ground with each unintended (or overt) use of technology for surveillance

Moderator Sterett additional question of "How do you think the Internet will be used?" (with respect to the balance between privacy and security)—

Zimmermann response—noted Guatemala genocide trial used encryption chips to protect witness identity; globalization and outsource of jobs; geography barriers are coming down (Thomas book The Flat Earth)

Keating response—China's response to the Privacy/Security balance is the "Great Firewall of China"; we are one of many nations all striking a different balance (concern for intellectual property rights radically different in US versus China); complicates striking a balance in any country

Haag response—education economic, digital, monetary, health divides are recognized …beginning the Information Divide; you know about what you know; information is power …rich vs. poor relative advantages aggravates the divides

Dobson response—not an "Us vs. Them" issue; top GIS applicants are often foreign; maybe something more than just technology …education (is the US slipping?)

Moderator Sterett closing question of ""Is technology Opening or Closing Privacy?" …is it possible it is opening?—

Zimmermann response—encryption technology used in e-commerce can indirectly be used to increase privacy in computer dialog; voice over Internet as secure phone conversations (allows encryption)

Keating response—if everything is known then there is need for privacy

Zimmermann response—we now have ability to "see" inside the police station (Rodney King situation); if encryption is employed then lose ability to track criminal activity for convictions; is there good/bad privacy flavors? …or is privacy always good?

Hag response—privacy and Security are not mutually exclusive …comes in a package that balances them as reflected by social values

Dobson response—to be geoslavery it must beyond surveillance; involve coercion and control

---

GEOEurope

Technology Trends

Brave new world?

JONATHAN RAPER conjures up Orwellian visions but admits to a professional interest in their realisation

'They are always watching you. Use cash. Do not give your phone number, social security number or address. Do not fill in questionnaires. Demand that credit firms remove you from marketing lists. Check your medical records often. Keep your telephone number unlisted. Never leave your mobile phone on. Do not use credit or discount cards. If you must use the Internet, use someone else's computer. Assume that all calls, voice mail, email and computer use are monitored.'

*- **The Economist, 1 May 1999***

Like all good parody, this invitation to paranoia contains an essential truth: privacy is not what it was. In the information society, we have created a vast new capacity to store personal details, log transactions, intercept digital communications and engage in video surveillance. In many cases, the information thus obtained is intended to facilitate new freedoms, such as online credit purchasing, or to tackle social problems such as crime.

Faustian pact

While governments regulate this process through provisions such as data protection legislation, perhaps collectively we have made a Faustian pact with this information bazaar in the belief that privacy resides in anonymity. There is a sense that many people regard the information held on them as reflecting a public ***persona*** without prejudice to their private one - at least, until credit refusals or junk mail overload spoil the illusion.

Another dimension to this debate will shortly emerge, this one focussed on the geolocation capabilities of the mobile phone. Many people already subscribe to cellular tariffs that offer roving 'local' call rates dependent on one's current location. Mobile phones on this tariff can be made to display location information (or 'cell info') and which, in many countries, is the telephone dialing code for the area in which they are physically located.

Jonathan Raper

Cellular network operators can achieve a higher level of locational precision by identifying the nearest transmitter mast to the phone according to signal strength. Generally, these transmitter cells are several kilometres in area, but shrink to hundreds of metres in city centres. Locating phones according to their dialling code area is easy but imprecise. Only

occasionally are cellular operators required to forensically analyse their records to pin-point a mobile 'phone to assist criminal investigations. However, all this is about to change.

No hiding place

With the arrival of technologies that allow operators to locate cellular subscribers to within an accuracy of 10-25m has come the promise of 'location-based services'. It will become possible to deliver information to you through your phone based on where you are at any point in time. The 'where' will, in future, place you in a particular building or on a specific street. With the arrival of larger screens in 'smartphones' and personal digital assistants (PDA's), and with the delivery of 'always-on' mobile Internet connectivity, a number of attractive new services will be offered. A moving map on screen wherever you go; the ability to find nearby cash machines or petrol stations (that are open and hopefully stocked with fuel ;and the delivery of alerts based on your location- a weather warning if walking in the mountains, for example. You may, indeed, find the new information services attractive, but you might also have some concern over 'locational' privacy.

As yet there are few explicit principles to govern locational privacy. I put a question on this issue to the UK Data Protection Registrar, Elisabeth France, at the Association for Geographic Information conference in September 2000. In her response, she said that personal location held in a computer system was 'personal information' within the meaning of the 1998 UK Data Protection Act, no matter what the spatial and temporal resolution.

Caught in the Act?

The gist of this would appear to mean that anyone merely recording the fact that I am in the UK at any given time on a computer needs to abide by the principles of the 1998 Act. If I were in another EU member state, similar provisions exist in EU Directive 95/46/EC. Clearly, therefore, high resolution geolocation will be governed by data protection legislation - provided there is consent, a contract, a legal obligation or a vital/legitimate interest, and you have right of access to the record. However, 'location' is not one of the categories of 'sensitive' information specified in the 1998 UK Act, i.e., those that govern the processing of data relating to racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sex life or criminal convictions.

Perhaps location should be added to this list, for while there are many potential social and economic benefits to be derived from location-based services, public support for them may be undermined if constraints are not seen to be placed on network operators to safeguard locational privacy. The design of these services and their supporting systems must give users a measure of control over their own locational profiles; allow them to delete or generalise those profiles, and set a minimum resolution or time delay.

Personally, I am hooked, not least as
developer of a location-based service in the
EU funded Hypergeo project (http://www.hypergeo.org/). Here, I have been carrying a prototype device with GPS positioning and street mapping for six months and the real-time information flow is compelling. Let my mobile phone operator record my movements and build up a locational profile. Who knows, they might even put something on my personal map that I'd like to know. The cost? Another brick in the wall of my public persona... unless, of course, I switch off my phone.

JONATHAN RAPER *is with the Department of Information Science, City University, London, England and can be contacted by email at raper@soi.city.ac.uk*

Will GPS tech lead to 'geoslavery'?

Tracking technology gives access to dangerous power

CNN, Tuesday, March 11, 2003 Posted: 10:10 AM EST (1510 GMT)

LAWRENCE, Kansas (AP) -- Jerome Dobson worries that 1984 may be just around the corner. Dobson, a University of Kansas research professor and president of the American Geographical Society, is concerned that technical advances carry the potential for bringing about George Orwell's nightmarish vision of a society that destroys privacy. This new threat, says Dobson -- a respected leader in the field of geographic information technologies -- is "geoslavery."

Devices currently on the market, for example, use satellites to locate and track people anywhere on the planet.

One company sells a device that can record a vehicle's location so employers can keep track of every move their drivers make.

Sounding an alarm

Another company makes implanted chips to keep track of livestock or pets, and a device that looks like a digital wristwatch that can pinpoint the wearer's location and sound an alarm.

Dobson knows the good these devices do, but he also worries that they may be abused. He hopes his fearful vision will create debate and perhaps legislation or safeguards around the technology that will keep it from being misused.

Already the technologies are sparking debates regarding privacy. Add a transponder to a locked device, he said, and the punitive possibilities are endless.

> "The phrase I like to use to bring this home is to ask, 'How long would Anne Frank's diary be if she were wearing one of these nifty devices?'"
>
> *-- Jerome Dobson, University of Kansas professor*

"What we are suggesting," Dobson said, "is that we are only one technological step from placing a transponder in there that burns or stings a person if they step off a prescribed path by a meter. Or if they stay too long in one place. Or cross the path of another person they are prohibited from seeing, or if they congregate with other people.

"I can confine you to a place. You can't go there. Or you must go there. And I can control it."

Avoiding abuses

In the hands of repressive governmental regimes, the devices could be devastating, Dobson said, just as they could be in people's personal lives.

Before going to Kansas less than two years ago, Dobson worked 26 years at Tennessee's Oak Ridge National Laboratory creating, for the government, the maps used in global tracking.

"We may avoid the most serious abuses of this technology in the U.S. because we have a tradition of personal freedom," he said. "But it will differ by country and by culture. Think of the countries where they already have ethnic cleansing."

---

http://www.ur.ku.edu/News/03N/MarchNews/March5/dobson.html

March 5, 2003

KU researcher warns against potential threat of 'geoslavery'

LAWRENCE -- Jerome Dobson wants to make sure his field of research doesn't aid the greatest threat to personal freedom.

As a pioneer of geographic information systems (GIS), Dobson, a researcher at the Kansas Applied Remote Sensing Program at the University of Kansas, helped develop the technology that now is commonplace in government, business and practically every aspect of modern life.

Since 1975, Dobson has used GIS for a number of applications -- from conducting environmental analyses to identifying populations at risk of terrorism and natural disasters -- by combining data sets such as detailed population counts of every country in the world, terrain and nighttime lights interpreted from satellite images, road networks and elevations. Dobson, who is a professor of geography at KU, also is president of the American Geographical Society.

Unfortunately, the same technology that has so many beneficial uses also has the potential to create a highly sophisticated form of slavery, or "geoslavery," as Dobson calls it. What worries Dobson is that GIS technology easily could be used not only to spy on people but to control them as well.

"It concerns me that something I thought was wonderful has a downside that may lead to geoslavery -- the greatest threat to freedom we've ever experienced in human history," he said.

By combining GIS technology with a global positioning system (GPS) and a radio transmitter and receiver, someone easily can monitor your movements with or without your knowledge. Add to that a transponder -- either implanted into a person or in the form of a bracelet -- that sends an electric shock any time you step out of line, and that person actually can control your movements from a distance.

Sound like something from a bad sci-fi movie? Actually, several products currently on the market make this scenario possible.

"In many ways that's what we're doing with prisoners right now, but they've been through a legal process," he said.

In fact, many of the existing products are marketed to parents as a way to protect their children from kidnappers. Dobson, however, said parents should think twice before using such products.

"A lot of people think this is a way to protect their children," he said. "But most kidnappers won't have any compunction about cutting the child to remove an implant or bracelet."

Furthermore, these products rely on wireless networks, which are notoriously easy for hackers to break into, potentially turning the very products meant to protect children into fodder for tech-savvy child predators.

Dobson outlined the dangers of geoslavery in an article that appears in the most recent issue of the Institute of Electrical and Electronics Engineers' Technology and Society magazine. Peter F. Fisher, editor of the International Journal of Geographic Information Science, co-wrote the paper with Dobson. More than 375,000 scientists read the IEEE magazine.

One of the greatest dangers of geoslavery is that it doesn't apply just to governments. For example, individuals could use the technology to perpetuate various forms of slavery, from child laborers to sex slaves to a simple case of someone controlling the whereabouts of his or her spouse, Dobson said.

"Many people have concerns today about privacy but they haven't put all the pieces together and realized this means someone can actually control them -- not just know about them, but control them," Dobson said.

As the price of these products gets cheaper and cheaper, the likelihood rises that the technology will be abused, he said. To prevent this, Dobson's paper outlines a number of actions that should be taken, including revising national and international laws on incarceration, slavery, stalking and branding, and developing encryption systems that prevent criminals or countries with bad human rights records from accessing GPS signals.

Still, the first step is making people aware of the very real threat that geoslavery poses. The potential for harm is even greater in less developed nations without strong traditions of personal freedom, he said.

"We need a national dialogue on this if we're going to go into something so different from our traditional values of privacy and freedom," Dobson said. "We need to think about it very carefully and decide if this is a direction we as a society want to go."
Dobson said he doesn't consider himself a crusader. Instead, he is a scientist who is working diligently to ensure that people really understand the good and bad sides of the technology he helped create.

"There certainly are many, many good uses for the technology -- that's not the issue -- the issue is that it can be so easily misused," he said. "My role as a university professor is to alert people and make sure there is an informed debate."

Posted on Fri, Mar. 07, 2003

KU professor has nightmare vision of global positioning technology

By ERIC ADLER, The Kansas **City Star**

The first thing to know: Jerome Dobson is not joking.

The University of Kansas research professor, a respected leader in the field of geographic information technologies, thinks a terrible and unrealized threat looms about the globe.

This new threat, Dobson says, is "geoslavery" -- a form of technological human control that could make "George Orwell's `Big Brother' nightmare...look amateurish."

His vision would use the same manner of electronic devices some parents use to keep track of their children and police use to restrict the movement of criminals. He's talking about pimps electronically monitoring their prostitutes. He's talking about overlords electronically punishing errant workers.

He's talking about the possibility of people hooked to, tracked by, and potentially shocked or burned using inexpensive electronic bracelets, manacles or implants under the eyes of global positioning satellites.

Weird? Perhaps. But it is this scenario that Dobson is scheduled to present this afternoon in New Orleans at the annual meeting of the American Association of Geographers.

What gives Dobson's speech heft is his background. Before going to KU less than two years ago, Dobson worked for 26 years at Tennessee's Oak Ridge National Laboratory creating, for the government, the maps used in global tracking. He is the president of the American Geographical Society. And he is not alone in his thoughts.

In the most recent issue of *IEEE*, the journal published by the Institute of Electrical and Electronics Engineers, a paper titled "Geoslavery" is co-written by Dobson and Peter F. Fisher, British editor of the *International Journal of Geographical Information Science.*

"Human tracking systems, currently sold commercially without restrictions, already empower those who would be masters, and safeguards have not yet evolved to protect those destined to be slaves," they wrote.

"I've spoken about this at academic conferences," Dobson said by phone from New Orleans. "I find that the first reaction people have is, maybe, disbelief. But if I talk for two minutes, suddenly they begin to turn somber and say, `This is the scariest thing I have ever seen.' "

Even those experts who view Dobson's vision as exaggerated concede that his notions are within the realm of reality.

"Technically, it is possible," said Glen Gibbons, editor of *GPS World* and *Geospatial Solutions,* Oregon-based trade magazines. "Yes, people with ill intent could turn these technologies to evil purposes. But it is also a matter of how much sociopathology you think you have in a culture."

To Dobson, the point is to address the threat before it is too late.

Numerous companies produce devices that, using satellites, are able to locate and track people anywhere on the planet:

• Advanced Tracking Technologies Inc. of Houston sells TravelEyes. Placed in a vehicle, the device records a driver's location every moment of the day. It records how long the driver has stopped, the path a vehicle has taken, the speed traveled. With a laptop computer, employers can keep track of their drivers' every move.

• Digital Angel Corp. of St. Paul, Minn., makes implanted chips to keep track of livestock or pets. It also sells a Personal Safety and Location System. The device looks like a digital wristwatch. When the wearer -- say an elderly person with Alzheimer's -- wanders, the device not only pinpoints the person's location, but also sounds an alarm. The devices have emergency buttons that call 911 if a person has fallen or has a drastic change in temperature.

• In Redwood Shores, Calif., a company called Whereify Wireless Inc. sells its GPS Kids Locator for $400. The device, which also looks like a watch, can be locked to a child's wrist. Parents can log on to an Internet site to track their child's movements on a map every couple of minutes for 24 hours.

Dobson said that in creating these products, none of the companies was thinking of anything nefarious. He absolutely knows the good they do.

Like all the electronic monitoring devices, Whereify comes with 911 alert and locator features that can be triggered in case of an emergency. It even can be triggered automatically if someone tries to remove the device from a child's wrist.

Based on lecture notes by Michael Goodchild, USSB, Geography
http://www.geog.ucsb.edu/~good/176b/n14.html

SOCIAL ISSUES Surrounding Geotechnology

Do we have a right to location privacy?
Who has the right to know where we are?
Do we have a right to sell our location privacy? …in return for store discounts?

US law: E911 calls from cell phones; Wireless Communication and Public Safety Act of 1999…

- ``(4) to provide call location information concerning the user of a commercial mobile service (as such term is defined in section 332(d))_
- ``(A) to a public safety answering point, emergency medical service provider or emergency dispatch provider, public safety, fire service, or law enforcement official, or hospital emergency or trauma care facility, in order to respond to the user's call for emergency services;
- ``(B) to inform the user's legal guardian or members of the user's immediate family of the user's location in an emergency situation that involves the risk of death or serious physical harm; or
- ``(C) to providers of information or database management services solely for purposes of assisting in the delivery of emergency services in response to an emergency.".

UK law: Telecommunications (Data Protection and Privacy) Regulations 1999 establishes limitations on the processing of traffic and billing data by carriers (no clear reference to location). Regulation of Investigatory Powers Act 2001 can require recovery of location known from mobile phones (when this is part of traffic data) for intelligence purposes.

Is there adequate regulatory protection for the use of location in traffic data?
Who has access to the location?
How long should it be kept?
What geographic resolution is available?
Do users have control over their location information?

What is privacy? …relates to individuals; guards against intrusion, appropriation, breach of confidence
Economist 1 May 1999—*"They are always watching you. Use cash. Do not give your phone number, social security number or address. Do not fill in questionnaires. Demand that credit firms remove you from marketing lists. Check your medical records often. Keep your telephone number unlisted. Never leave your mobile phone on. Do not use credit or discount cards. If you must use the Internet, use someone else's computer. Assume that all calls, voice mail, email and computer use are monitored."*

Location privacy:

- Protection of information about your current or home location in space or cyberspace; currently no explicit regulation of locational privacy
- Raper essay in January 2001 GeoEurope http://www.geoplace.com/ge/2001/0101/0101tt.asp
- Private persona - should be absolutely protected
- Public persona - tradable by consent, disconnected from the private persona