

Privacy and Location

By

Daniel Shannon

Engineering Manager, Telus Geomatics

Edmonton, Alberta

Privacy and location is a growing concern. Steve Swazee, Executive Director of Shared Geo noted a significant rise in the number of articles in the mainstream media about geospatial information and technology privacy issues. It's been widely reported that Google, for example, has faced legal action related to collection of data over public Wi-Fi networks in several countries. In the USA, several states' Attorneys General have sought clarification from Google regarding the data they collected and their intended treatment of that data.

Google has generally been quick to reply. However not all groups have been placated by Google's responses, including advocacy groups such as EPIC, the Electronic Privacy Information Center, that notes Google's Street View collection techniques violated national privacy laws in countries such as Switzerland, France, New Zealand and the United Kingdom.

Facebook also came under fire last year from the American Civil Liberties Union over concerns over the privacy issues arising from their Places feature.

In many ways, the Street View data collection issue is not a GIS issue at all. The same issues and challenges surfaced in civil courts around the world much earlier relative to the use of video to collect images of citizens in public areas, often by municipalities seeking to curb undesirable activities in public areas such as parks and transit terminals. Traffic radar and intersection cameras have also been challenged on the basis of privacy violation when images collected for the stated purpose of recording moving violations have inadvertently exposed citizens in compromising positions. Other than the fact that all of these activities take place somewhere, there is nothing uniquely geospatial about them or the related privacy issues.

Privacy issues such as this can be cast as a GIS issue, however, when one considers the potential sanctions and restrictions which could face practitioners in the industry resulting from the reaction to the potential uses and feared abuses of information presented in applications such as Street View and virtual globes.

It should be noted that this type of data is not new nor was it non-existent prior to the explosion in popularity of web maps and virtual globes in the mid 2000's. Aerial imagery has been publically available on municipal websites for years previous. So why has the privacy issue specifically related to this kind of data become such a prominent issue?

It would seem that it is the popularity of the delivery mechanisms rather than the data itself that has triggered a backlash. The ubiquitous nature and ease of access to the information has brought the issue to the fore. It has made privacy concerns that would have previously been more theoretical in nature more substantial. Images on specific, less trafficked web sites offered a version of ‘security through obscurity,’ or in this case ‘privacy through obscurity.’ In contrast to individual, geographically specific repositories of spatial information, the most heavily trafficked of today’s websites provide seamless worldwide coverage. They constitute, and perhaps epitomize, what Canadian Marshall McLuhan was referring to in 1960 when he coined the phrase ‘global village’. In this very public forum in which everyone is a constituent, any potential damages can more readily be seen to be tangible and perhaps even likely.

GPS Privacy

In the United States, rulings regarding the use of GPS data in Automated Vehicle Location (AVL) applications have been inconsistent with different jurisdictions allowing or disallowing different uses of GPS vehicle location information.

A landmark Canadian ruling in 2006 resulted from a complaint lodged by employees of a national telecommunications company whose field services employees complained that the use of GPS units installed in company vehicles was an invasion of their privacy. Federal Privacy Commissioner Janice Stoddard ruled that the company could continue to use the GPS vehicle tracking devices and applications, but cautioned that this did not give employers ‘carte blanche’ to engage in ubiquitous monitoring of employees with the technology. The key issue in Commissioner Stoddard’s ruling was that of transparency. Not only must employers clearly specify up front with employees what data will be collected and what it will be used for, she said, but in addition employers must ensure that the data is indeed used only for the stated purpose. The Privacy Commissioner explained in her ruling that use of GPS data could be used for purposes beyond safety and dispatch efficiency and could include purposes such as managing employee productivity. However it would have to be demonstrable that there were no equally effective alternate less obtrusive methods of gathering the necessary information.

Interagency Spatial Data Sharing

Privacy and control issues don’t disappear when we own the geospatial information, however. There are many challenges facing governments and utilities when they contemplate sharing geospatial information over which they wish to maintain control. Business activities are highly integrated, and an organization’s Geospatial Information System (GIS) is only as effective as its capability to integrate its information with the external environment which provides context.

GITA’s white paper “The Geospatial Dimensions of Critical Infrastructure and Emergency Response: Spatial Infrastructures” highlights the need to overcome the reluctance to share geospatial infrastructure data due to the stakes involved in Critical Infrastructure Protection (CIP) due to the complex interdependencies of various infrastructure. The paper explains that managing this risk depends largely on each stakeholder having a clear understanding of the

relationship between and interdependencies of each others' infrastructure, and that an SDI is the mechanism for enabling the sharing of spatial data required to provide that clarity of understanding.

Some of the key points discussed in this paper are the need to define and agree upon a technical and procedural model for collaboratively sharing spatial information, and to ensure that this SDI is in place and operational before an emergency situation arises.

The Integrated Cadastral Information Society (ICIS) in the province of British Columbia in Canada is an interesting example of what has become recognized as a model for effective geospatial data sharing, its effective use of Data Sharing and License Agreement, sharing data with competitors, building a relationship and essentially overcoming privacy concerns on how shared spatial information is being used.

Former ICIS General Manager, Pete Flagg, says key roadblocks the society faced in sharing spatial data were fear of misuse, liability and being able to strike a balance of benefit versus risk. Flagg makes the case that there are direct linkages between perceived risks and benefits and that there are few benefits that aren't associated with specific risks. He further suggests that any organization proposing to share spatial information should ensure they address, and communicate, the risk mitigation strategies that are to be undertaken. The risks should not be ignored but neither should they become a roadblock preventing sharing of spatial information such as cadastre.

In a 2008 white paper, Flagg provides an interesting comparison of risks and associated benefits of sharing spatial information:

Risk	Balancing / Related Benefit
Compromising Competitive Advantage	Discover of new business relationships and new competitive opportunities.
Exposure of competence & capability	Reduction of redundant effort Comparable efficiencies made available
Compromised Security	Enhanced public safety Enhance response times of emergency responders
Compromised Interpretation	Requirements for standardization and improved interpretation
Liability and Indemnity	Reduced cost of legal administration Clearly defined liability
Reliance on Data and Policy Control	Improved operational efficiency Greater access to more data Data quality improvement
Compromised Revenue Generation	Enhanced revenue from collected sources

	Enhanced business opportunities through VAR interest in larger data sets Enhanced revenue from greater “traffic”
Compromised Economic Development	Discovery of new relationships between business and demographic phenomena
Contravention of the Freedom Of Information & Privacy Act	Transparency and convenience of data access

Table 1. Benefits and Comparative Risks of Spatial Data Sharing (Flagg, 2008 p. 16)

Current ICIS Executive Director, Barry Logan, acknowledges the importance of developing rigorous data sharing and licensing agreements, and ICIS has done that. However he suggests that interagency data sharing will not overcome the concerns and inherent adversity toward risk that stifles most collaborative efforts without paying careful attention to two key factors.

First, Logan suggests, governments and utilities must have a clear and agreed upon business purpose for spatial data sharing. It is not enough to simply think that spatial data exchange is generally a good idea. Specificity will drive progress.

Second, be patient. Constituents must take time to listen to each other, and take time to develop a relationship. Much early hesitancy related to privacy and control issues between members has since become a non-issue as ICIS member firms have developed a better understanding and increased level of trust in each other.

This is consistent with the findings of GITA’s Geospatially Enabling Community Collaboration (GECCo) workshops held in various cities in the United States in the past several years. The Tampa GECCo stakeholders’ experience was typical. Of the 37 barriers to spatial data exchange that group identified, only 7 were in any manner technological. With modern spatial tools and software what stands in the way of integration doesn’t appear to be a lack of technology, but rather the lack of functioning frameworks for spatial data sharing.

Personal Privacy and Location

There is, however, a big difference between voluntary collaboration between governments and utilities to share spatial information under the protection of data sharing and license agreements, and the aggregation and re-purposing of location information gathered without informed consent from members of the public.

The core issue remains much the same as articulated by ICIS, that of “perceived risk”, particularly where there is a lack of control over that information. Much has been made recently, for example, of the ability to monitor the individual movements of members of the public based on the location information passively provided by their cellular

References

Flagg, P. (2008). *An ICIS White Paper: Risks & Benefits of Spatial Data Sharing*. Victoria, BC: Integrated Cadastral Information Society.

Bailey, E. Jr. (2010) *Google denies use of private data for mapping*. Associated Press Writer retrieved May 12, 2011 from www.physorg.com/news19155114.html

Geospatial Information & Technology Association (GITA). (2005). *Geospatially Enabling Community Collaboration: The GECCo Pilot Project Series*. Aurora, CO: GITA

Google, Privacy Principles (2011), retrieved May 10, 2011 from www.google.com/intl/en/corporate/privacy_principles.html

Patent OfficeUS (2010) retrieved May 3, 2011 from <http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1=%220100218111%22.PGNR.&OS=DN/20100218111&RS=DN/20100218111>

Jeffery, A. (2009), *New use for GPS*. *Western Review* retrieved May 10, 2011 from <http://www.draytonvalleywesternreview.com/ArticleDisplay.aspx?archive=true&e=1151913>

Wortha, J. (2010) *New Facebook Location Feature Sparks Privacy Concerns*. New York Times