

Data privacy in geographic information

Jonathan Raper, City University, London

Background

In the broadest sweep of IT history what we are seeing in 2009 is that location as an application feature is moving from a vertical market characterised by B2B geographic information (GI) processing to a horizontal market characterised by B2C personal location technologies (LT). The traditional GI sector, dominated by players such as ESRI and Intergraph, has been overtaken by the giants of the IT industry such as Google, Microsoft and Yahoo who have brought powerful LT consumer applications into the market. This has set the scene for massive changes to the GI sector over the next few years, in which privacy issues will play a big part.

One of the key differences between GI and LT is the relationship between the developer and the user. In GI applications the dominant paradigm is the representation of space, and people do not usually appear except through the proxy of addresses or properties. This has meant that few GIS have faced customers directly, reducing the scope for privacy questions to arise over GI. The most direct form of personal data collected and held by the traditional GI sector would be the Population Census, and this is aggressively anonymised to protect privacy.

Privacy has become an issue for GI when datasets have been linked using GIS e.g. when using geodemographics to link addresses and the electoral roll for direct marketing. A campaign against this by Brian Robertson of Wakefield in 2001 led to the division of the Electoral Roll into the Full and Edited versions in the 2002 Representation of the People Act, with the latter version being placed off limits for geodemographic analysis. However, when Barbra Streisland complained about intrusions into her privacy by the availability of aerial imagery of her Californian house on the Internet, courts in the US found that as the imagery was collected from the public domain and could not be used to identify individuals, then the California Coastal Records Project did not violate her privacy.

By contrast, in LT people and places are at the centre of the service concept and businesses have a direct relationship with the purchasers of the service: this means that that privacy has had to be actively managed. There are now services like location-based social networking e.g. Gypsii where location privacy is shared within social groups under user-controlled conditions. Google has also introduced a service called Google Latitude that allows individuals to 'publish' their location to selected people with Google accounts, using the best available positioning on the mobile device.

©Copyright 2010 belongs to the Author identified in this document.

The views expressed in this study are the personal opinions of the writer(s) and do not necessarily reflect the policies and view of the AGI or any of its individual or corporate members or the authors' employer.

The AGI Foresight Study - The UK Geospatial Industry in 2015

An Expert Paper



So far, privacy breaches in LT have been limited to unauthorised entry to poorly designed systems like the London Oyster card in 2006, which contains records of all journeys paid for by the card. The development of user generated content generator of photos, audio tracks and travel records also raises privacy concerns. However, privacy impacts may have been limited as yet since LT are still niche applications, though given the rate of growth of smartphone apps they will gain mass distribution within a few years on platforms like the Apple iPhone.

Current position

Generally, the position relating to privacy in the existing GI sector is stable with regulation having established a balance between data collection and its use e.g. Census privacy measures, Edited Electoral roll and aerial photography self-regulation to resolutions where individuals cannot be identified.

In LT privacy impacts are still evolving as they penetrate the mass market, but tracking concerns are currently mitigated by the limitations of current mobile positioning. Although GPS is capable of 5m accuracy and wifi positioning can snap to the location of hotspots, the power consumption for both these sensors is too high to be used continuously in mobile devices. Most tracking services use cell-ID (based on mobile phone base stations), which uses no extra power, but the resolution of this service is limited to c.100m at best in cities, and degrades to kilometres in rural areas. So the high resolution positioning services are too power-hungry to generate much tracking data, and the low resolution services cannot position accurately enough to breach privacy.

The biggest impacts on privacy in this area at present are being made by the collection of street imagery by CCTV, automated number plate recognition (ANPR) and Google StreetView. CCTV imaging is very pervasive in the UK with at least a million cameras installed, although many of them are monitoring private rather than public spaces. The Information Commissioner has a code of conduct for the use of CCTV as their use to monitor individuals is governed by the Data Protection Act. Most ANPR cameras are designed only to capture and read number plates at intervals along trunk roads as part of traffic speed monitoring schemes e.g. as conducted by TfL London Streets. These cameras are not able to look up car owner's details and cannot therefore be used in tracking. However, the police do maintain a network of 2000 cameras designed to check plates against car tax, insurance, MoT test and police watch lists. There is a scope here for massive privacy breaches if the police use this data to monitor the movement of protesters engaged in legitimate protests, or if the data leaks in some way.

The biggest current issue in LT privacy is the collection and publication of the street imagery in Google StreetView. The imagery contains pictures of people, places and car number plates, which generate all sorts of privacy implications, although the images are now historic and static and Google adopted a 'no questions' take-down policy for those with concerns. As soon as StreetView went live in the UK there were complaints to the Information Commissioner's Office (ICO) e.g. from Privacy International. These complaints were rejected on the grounds that face and number plate blurring were largely effective, but

©Copyright 2010 belongs to the Author identified in this document.

The views expressed in this study are the personal opinions of the writer(s) and do not necessarily reflect the policies and view of the AGI or any of its individual or corporate members or the authors' employer.

The AGI Foresight Study - The UK Geospatial Industry in 2015

An Expert Paper



the ICO required Google to do more to ensure that the anonymisation was completely effective. This kind of imagery when combined with other sources like user generated content and public CCTV does have the scope for privacy breaches.

Regulation

Ultimately, privacy is in the eye of the beholder as there is no law of privacy in the UK, only common law protection of confidences and trespass. Although the 1998 Human Rights Act transferred the provisions of the European Convention on Human Rights into UK law, this only guarantees 'respect for private and family life' and case law is still developing in location privacy.

When dealing with personal data in LT applications data protection is the key consideration. The Data Protection Act 1998 requires anyone in the UK who is processing data that identifies an individual to register with the (ICO) as a data controller. The information must be fair, limited, adequate, accurate, up-to-date, legal, secure and kept within the EU. There are special provisions for handling certain categories of sensitive data including sexual orientation, racial origin, religious beliefs, trade union membership, alleged criminal offences and political affiliations, though note that location is not on this list. Location information is mentioned in the "Privacy and Electronic Communications Regulations 2003, Section 14" which states that "Location data relating to a user or subscriber of a public electronic communications network... may only be processed... where necessary for the provision of a value added service, with the consent of that user or subscriber".

To process personal location information as part of a service is entirely legal if you obtain informed consent from the user to do this, you are registered with ICO and you obey the principles above. The UK mobile phone industry recognised the special sensitivity of location by drawing up a code of practice "For the use of mobile phone technology to provide passive location services in the UK". This code covers the marketing of services, consent, starting and stopping services and identity verification with specific application to child tracking, friend finding, game play and corporate services. This Code was reviewed by the Mobile Data Association in 2006, but is now in urgent need of revision to deal with current technologies and applications.

Looking forward towards 2015

The overall picture of location privacy is one of ad hoc regulation addressing specific applications as they arise: there has so far been no comprehensive attempt to regulate from first principles. There is now a case for the ICO to update the Privacy and Electronic Communications Regulations 2003, and for the mobile operators to update their Code. However, it might be better to plan to include location in a revision of the Data Protection Act where some of the missing provisions can be addressed e.g. retention of location records, linkage on the basis of location, location obfuscation and location

©Copyright 2010 belongs to the Author identified in this document.

The views expressed in this study are the personal opinions of the writer(s) and do not necessarily reflect the policies and view of the AGI or any of its individual or corporate members or the authors' employer.

The AGI Foresight Study - The UK Geospatial Industry in 2015
An Expert Paper



spoofing. There should in particular be a debate on what resolution of location information is private on a spectrum from "is the in the country" to "is located here to a resolution of x metres".

There has also been a longstanding concern that LT could be used as part of a coercive relationship if individuals had the power to obtain false consent or to force individuals to give consent for their location to be processed for surveillance reasons. Dobson and Fisher (2003) argued that a new form of 'geoslavery' could be generated by LT for those without the power to resist demands for consent to track. This is a societal issue which is not unique to LT, but an updated Data Protection Act could introduce penalties for 'procuring location': it is probably appropriate for mobile operators and professional bodies such as the Association for AGI to call for this before campaigners, the press and the public are agitated by any future 'cause celebre'.

There is also another concern that society is developing institutions that will require pervasive locating by design. Raper (2008) argued that citizens should be able to choose to consume a service based on their assessment of the privacy protection, and critically, that if they chose to reject the transaction then they should suffer no disbenefit. If protection and transaction choice are cross plotted (see figure 1) there are four cases, three of which are catered for by legislation and law enforcement.

Figure 1 Digital privacy transaction protection

	Accept transaction	Reject transaction
Protection sufficient	'Privacy by Design' ideal	"Respect for private life"
Protection insufficient	Enforcement of the law	Dystopia where cannot reject transaction

The fourth case where the citizen cannot reject the transaction and the protection is insufficient is becoming unacceptably common including the following problems:

©Copyright 2010 belongs to the Author identified in this document.

The views expressed in this study are the personal opinions of the writer(s) and do not necessarily reflect the policies and view of the AGI or any of its individual or corporate members or the authors' employer.

The AGI Foresight Study - The UK Geospatial Industry in 2015

An Expert Paper



- when it costs more to have a truly private service e.g. cash price versus Oyster price on London Transport, and Oyster has been hacked;
- when the State creates compulsory registers e.g. Identity card use, and the Home Office has been hacked;
- when data linkage creates an unfavourable and unfair profile e.g. credit rating dependent in some part on geodemographic profiling based on out of date or inaccurate locations, and there is no 'right to reply';
- when it is necessary to give location information in order to get a service e.g. tracking services when there is no profile delete option.

Over the next 5 years there will be a number of changes to the environment and capability of LT that will combine to create 'location crises', unless action is taken to guard against these. These changes will include some stepped ones e.g. arrival of a second GNSS constellation such Galileo when positional accuracy will suddenly improve, and some progressive ones e.g. steadily increasing penetration of smartphones offering location processing. We can forecast that when the stepped changes cross the progressive ones then a regulatory deficit may become apparent. This is the point at which lobbying work by mobile operators and professional bodies can be used to bring pressure to bear on government. Failing to do this preparatory work may see the industry cast in the role of the villain, and public trust may be difficult to rebuild.

References

Dobson, J. & Fisher, P. (2003) Geoslavery. IEEE Technology and Society, 22, 47-52.

Raper (2008) You can run but you can't hide. A fine balance: privacy technologies in action. Knowledge Transfer Networks in Sensors and Instrumentation; Location and Timing; Cyber Security and Digital Communications. <http://www.petsfinebalance.com/index.php>

©Copyright 2010 belongs to the Author identified in this document.

The views expressed in this study are the personal opinions of the writer(s) and do not necessarily reflect the policies and view of the AGI or any of its individual or corporate members or the authors' employer.