A Balancing Act: Fusing Spatial Privacy and Spatial Metadata for Responsible Participatory Geo-Governance

Usman IQBAL, David BRUCE, Ed GARVIN, Australia

Key words: Spatial Privacy, geographic metadata, privacy legislation, participatory governance, Risk management

SUMMARY

Public policy is undergoing significant change. Governments are now visibly proactive in facilitating public access to government information resources. Popular media channels such as YouTube, Twitter, flickr and Facebook are being used to engage with citizens. Among these initiatives spatial information plays an important enabler to support policy development across various facets of government operations. Governments are increasingly turning to electronic maps as vehicles for interaction with citizens in this new participatory governance model. Various governments across the globe have erected geo-portals to publish descriptions (geographic metadata: accuracy, timeliness, completeness, etc.) of their geographic information where citizens can search, locate and access the information they need. On the other hand, the availability of spatial data poses certain risks. Spatial technologies permit the synthesis and analysis of information for isolated pieces of data in a spatial repository, when drawn together, give a very detailed picture of a specific location and the people associated with that location. This poses threats to the ideals of democracies and rights of individuals, freedom, security, privacy, and open and free access to government. As we move toward international networked environments, there is an increasing need to reconcile competing social, economic, and political interests in geospatial data especially in an international arena. This paper highlights the opportunities and risks of spatial metadata and spatial privacy in the context of e-Governance. It further explores the fusion of spatial privacy and spatial metadata at a policy level to be the key to participatory governance in GIS. Finally, these fused aspects are engaged to reconceptualise a responsible geo-governance model capable of sustaining legal protection as well as empowering citizens in governance.

A Balancing Act: Fusing Spatial Privacy and Spatial Metadata for Responsible Participatory Geo-Governance

Usman IQBAL, David BRUCE, Ed GARVIN, Australia

1. INTRODUCTION

Geo-information has gained importance in societies over the past decades. The public sector has always been a major spatial data provider and user. Public policy development and public management have undergone major shifts because of government reform, decentralisation, market reform and information technologies. Governments have invested in digital registration systems, and many are active in developing service delivery to citizens via internet technology. At the same time, availability of public spatial registries and the engagement with citizens for participatory governance poses certain risks (Iqbal & Bruce; 2009). Spatial systems permit the synthesis and analysis of disparate sources of information in such a way that their interleaving provides a very detailed picture of the location and people associated with it. This poses threats to the ideals of democracies and rights of individuals, freedom, security, privacy, and open and free access to government. It is important to reconcile the need of competing interests open governance and protection of citizens' privacy. This paper briefly introduces the concepts of spatial metadata, geoportals and their role in participatory governance in Sections 2 and 3, followed by a primer in spatial privacy issues posed from the availability of spatial data in section 4 and 5. These issues are analysed and a framework for responsible participatory governance is introduced in Section 6.

2. SPATIAL METADATA

Until recently, geographic information, i.e. data with an explicit reference to geographical space, was produced and used by the geospatial community, such as experts in the specialised fields as geography, cartography, geodesy, photogrammetry, remote sensing, bathymetry, hydrography, geology, physical planning, architecture etc. Today, geo-referenced data starts to play an increasingly important role in many application areas, including marketing analysis, mobile and location-based services, and end user applications. As a result, the number of both users and providers of geo-referenced data increases. This implies a growing need for the development of infrastructures for access to and exchange of geo-referenced data.

From Greek geographers through to the Middle-Ages and until the mid 18th century, topographic maps and sea navigation charts carried descriptions and explanations to enable the reading of map information called marginalia. These marginalia captured dates, bounding coordinates, grids, scales, accuracy, author details etc. which essentially described the characteristics of the map (Moellering, 2005).

The word metadata, which has its origins in Greek and can be described as *'data about data'* was introduced in the late sixties with its first use in Computer Science literature (Moellering, 2005). Metadata answers 'who, what, where, when, why, and how' about every facet of data.

This includes detail about ownership, quality, time of collection, attribute information and how to access data. Metadata is a vital foundation for understanding, collaborating and sharing resources with others. In spatial contexts, geographic metadata defines spatial data that have an explicit or implicit geographic extent.

2.1 Metadata Standards

The growing appreciation of the value of geospatial metadata from 1980-1990 led to the development of a number of initiatives to collect metadata according to a variety of formats either within agencies, communities of practice, or countries. Efforts were also made to standardize metadata collection, storage and retrieval.

The Federal Geographic Data Committee (FGDC) in the United States develops geospatial data standards to enable sharing of data among producers and users. It developed its geospatial metadata standard over the period 1992-1994.

Similarly, Australia New Zealand Land Information Council (ANZLIC), a combined body representing spatial data interests in Australia and New Zealand, released version 1 of its 'metadata guidelines' in 1996.

The task of harmonizing the range of formal and de facto standards was undertaken by ISO/TC 211 over the approximate period 1999-2002, resulting in the release of ISO 19115 'Geographic Information - Metadata' in 2003. Individual countries, communities of practice and agencies are currently in the process of re-casting their previously-used metadata standards as 'profiles' or recommended subsets of ISO 19115, optionally with the inclusion of additional metadata elements as formal extensions to the ISO standard.

As the transition toward the implementation of the international metadata standard continues, so does the development of new applications capable of creating and managing ISO 19115 metadata. Geonetwork is an open-source metadata catalogue, and one of the most comprehensive implementations that support ISO 19115. It has been adapted by agencies in many jurisdictions, including ANZLIC, for creation, search and retrieval of geographic metadata.

2.2 Spatial Data Infrastructures

While the metadata standardisation efforts continued in the last two decades, national surveying and mapping agencies felt motivated to initiate projects that would provide greater access to these standardized metadata and the data associated to them. A new term Spatial Data Infrastructure (SDI) was coined to define the technology, policies, standards, human resources and related activities required to acquire, process, distribute, use and maintain spatial data along various levels of government and private sector (Maguire, 2005).

A key component of any SDI is a catalogue of metadata that can be queried to search for data and resources using space, time and thematic attributes. Several SDI projects were initiated in the early nineties, including the NDSI in the US, the EU-wide INSPIRE (Infrastructure for Spatial Information in Europe) project and the Australian and Indian initiatives. These

projects have achieved their principal goals of spreading awareness, creating community involvement, building capacity, and establishing standards for accessing geospatial information.

3. PARTICIPATORY GOVERNANCE AND GEOPORTALS

3.1 Citizen Engagement

Public policy, both nationally and internationally seems to be undergoing significant change. Initiatives such as Inforoute in the UK and Government Information Locator Services (GILS) in the US facilitate access to publicly available government information resources. On the home turf, similar initiatives such as community cabinets aim to engage citizenry into governance. Governments are now visibly proactive in making documents and metadata available to public on a range of diverse topics. Popular media channels such as *YouTube*, *Twitter*, *flickr* and *Facebook* are being used to engage with the public (Iqbal & Bruce; 2009).

3.2 Geoportals

Spatial technology plays a key role in these governance initiatives. This idea has so much traction that in Australia, a conference was organised on this theme last year in Canberra, *'spatial@gov'* to discuss the importance of location as an enabler to support policy development across various facets of government operations. Governments are now increasingly turning to electronic maps as vehicles for social information and citizen interaction.

The US government promotes the use of geographic information as an essential part of e-Governance. The *geodata.gov* portal is a one-stop access for maps, data and other geospatial services to simplify access to geospatial data by all levels of government and citizens.

More recently, there has been a proliferation of geoportals for sharing of geographic information based on region or theme. Examples include the EU's prototype *INSPIRE* geoportal which allows discovery and viewing of spatial data sets and services. Other examples include the *NatCarb* geoportal, which provides geographic information concerning carbon sequestration in the United States, and the *UNSDI*, the United Nations Spatial Data Infrastructure. Similar local, regional, state and national portals have been deployed, including *Geoportail* in France, *GeoNorge* in Norway, *Go-Geo!* in the UK, and the *AD-SDI* in Abu Dhabi.

3.3 Participatory Geoportals

The advent of Web 2.0, coupled with the foundation of user-friendly online tools have enabled collaborative spatial decision making. Participatory governance frameworks take the Geoportals, discussed in Section 3.2, to the next level by directly creating channels for consultation with citizens and sharing spatial information at the grassroots level. Applications of participatory governance include program evaluation, assessment of local or neighbourhood needs, urban planning, counter-mapping and representation of local knowledge. These applications can utilise citizen input and benefit from local knowledge and

perception by empowering communities and under-privileged groups in solving development problems.

4. PRIVACY CONCEPTS

We have briefly reviewed the trends in spatial metadata management and participatory geo-governance concepts in Sections 2 & 3. Before delving deeper into analysing the relationship between spatial privacy and spatial metadata in the context of participatory governance in Section 5, it would be judicious to introduce some of the underlying concepts of privacy and spatial privacy first.

4.1 Privacy

It has been said that privacy is 'notoriously, even impossibly difficult' to define (Foord, 2002). Obtaining a definition for privacy, rather than producing abstracted generalisations has been recognised as difficult (Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd, 2001). Even though privacy is ill-defined, it is apparently a well-understood concept in the sense that most people use this term believing that others share their particular definition (Waldo, Lin, & Millett, 2007).

Early privacy researchers termed it *'the right to be let alone'* (Warren & Brandeis, 1890). Other researchers defined it as a *'claim of individuals ... to determine for themselves when, how, and to what extent information about them is communicated to others"* (Westin, 1967). Clarke argues that a right implies an intrinsic and absolute standard, something not always applicable to privacy. He defines privacy as '*the interest that individuals have in sustaining a `personal space', free from interference by other people and organisations'* (Clarke, 1988).

4.2 Personal Information

According to The Privacy Act 1988 (2009) personal information means information or an opinion, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information. This means information that can be related to a specific individual such as date of birth, gender, address**.**

4.3 Spatial Privacy

The following is a classification of spatial information in terms of privacy,

1. Spatial Information: Geographically referenced data with no personal information.
2. Personal Spatial Information: Geographic component along with personal information, such as land titles.
3. Personally-sensitive Spatial Information: Geographic component revealing sensitive personal information such as ethnicity and sexual orientation.

Figure 1 illustrates the different types of spatial information with respect to privacy. There are blurred boundaries in this attempted classification, because at times location information, with no overt identification information, could be used to identify a living person. Residential

address may only be considered location information until it is used to identify an individual, for instance, an individual living at a property in an isolated area can be reasonably identified based on address alone.

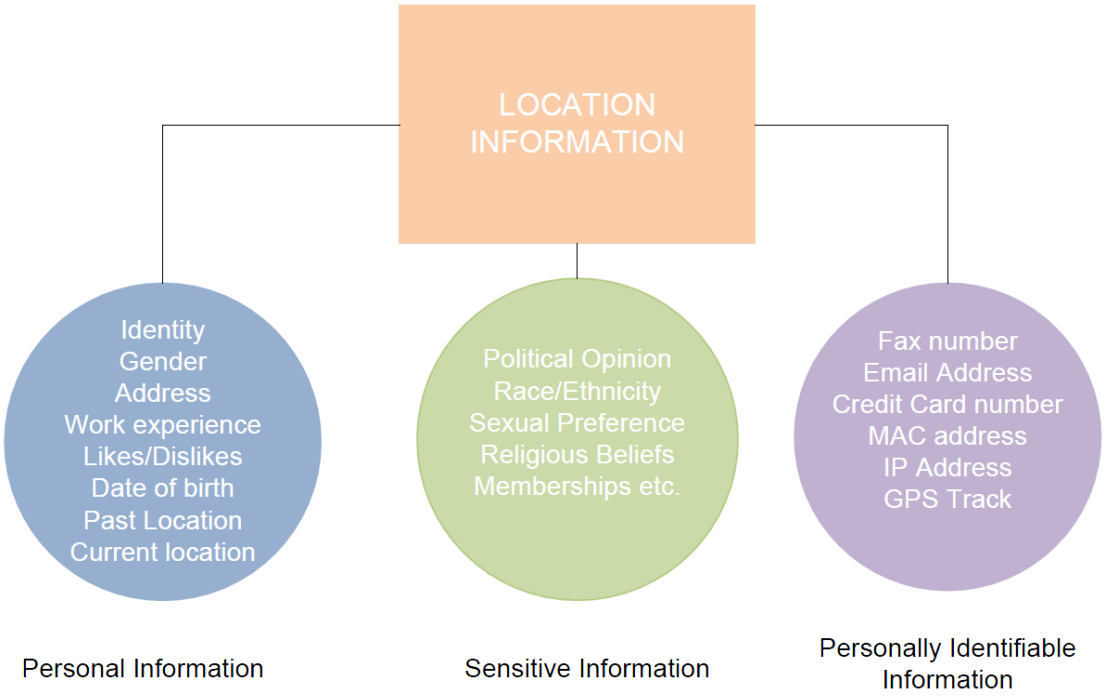

Figure 1: A privacy classification of spatial information

4.4 Sensitive Data

Sensitive information is a subset of private information that has additional protection under the Act under NPP 10, and generally requires consent without which an organisation is not allowed to collect this information. Sensitive information includes racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, sexual preferences or practices (National Privacy Principles, 2001).

Because of the inherent complexity of spatial data, it is difficult to identify the border where spatial information becomes personal sensitive spatial information. Research has proven that anonymous data of various spatial resolutions can be used to infer identities (Iqbal & Lim; 2007). Even using anonymous (de-identified) spatial data and disparate databases, it is possible to infer 'sensitive information' (as per the Privacy Act) about identifiable individuals. These intricacies mean that governments need to be very careful in identifying these blurring boundaries and in their release of spatial information.

5. PUBLIC SPATIAL DATA AND SPATIAL PRIVACY RISKS

Public authorities gather and hold substantial citizen-centric data from census, registries, electoral listings, land titles and other instruments. The GIS industry claims that 80% of enterprise data has a location or spatial component (Franklin & Hane; 1992). A major spatial component of public data concerning citizens is their physical address as has been discussed

in earlier sections. However, with the agenda of electronic enforcement, national security and process streamlining, a range of technologies are being employed including surveillance cameras, automatic number plate recognition systems (ANPR), electronic tolls, which are increasingly being used to collect spatial information about citizens (CrimTrac, 2008). The result is that one's past is always present. As an author noted,

"*No fact unrecorded, nothing forgotten nor lost, nothing forgiven"*(Stone & Warner;1969)

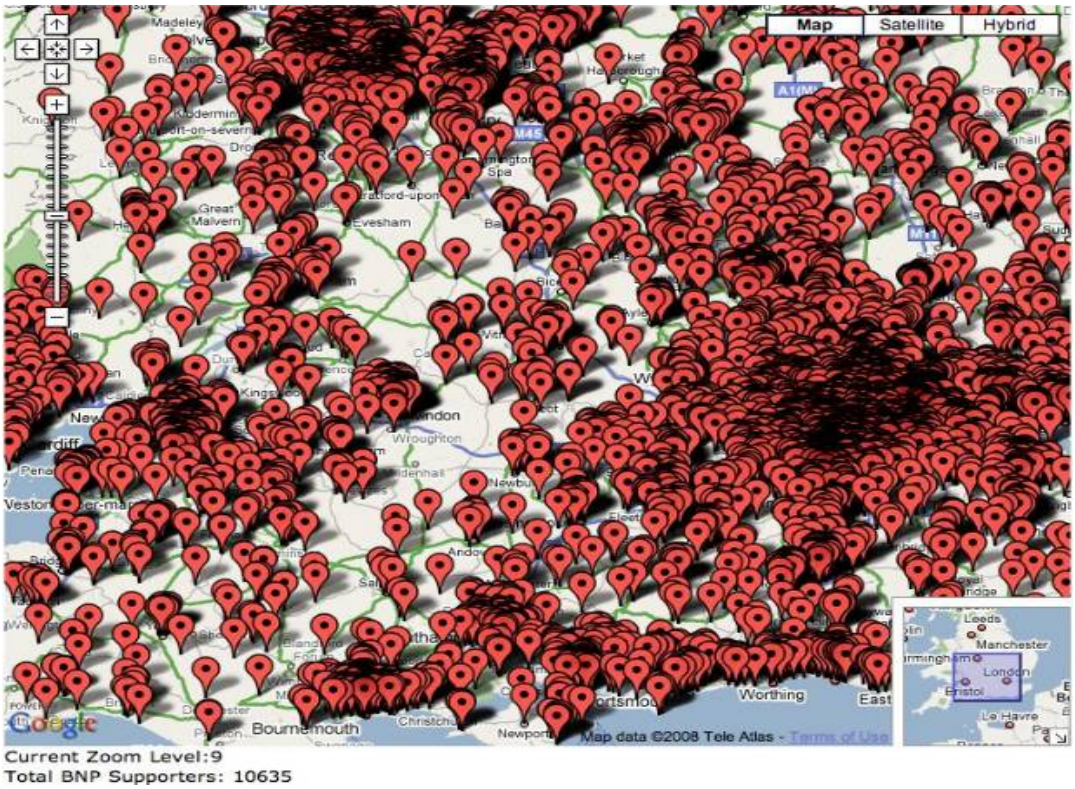

Figure 2: Push pins indicating the addresses of BNP members (Source: Butcher, 2008)

5.1 Data Breaches

A related aspect is that information now walks out of government offices via every conceivable avenue, from DVDs, to data downloaded to USB drives, to Blackberries. It is not comforting to find through media outlets the frequent data breaches in particular by government. In the UK, for instance, 62 out of 100 data breaches occurred in the public sector ranging from hard drives containing personal information of armed forces personnel being lost to un-encrypted CDs with personal information of child care benefits recipients disappearing in transit (Ranger, 2008).

Imagine this data getting into the hands of a technology savvy individual with malicious intent who geo-codes this information and performs spatial analysis to use this information for unscrupulous purposes. This is what happened when a list of all the members of the right-wing British National Party was leaked on *WikiLeaks* and then circulated via *BitTorrent* (Butcher, 2008). Although a court injunction prevents the publishing of names, many

neogeographers had mashed this information up with web mapping software and made them available online, as represented in Figure 2, which exposed the addresses to possible vigilante attacks.

Australia doesn't have mandatory data breach disclosure laws, so a statistic is not available about how many breaches took place. However, the Australian Law Reform Commission (ALRC), in its recent report outlining the amendments to the Privacy act, recommended that a data breach reporting framework be introduced to notify affected individuals and the Privacy Commissioner of the breach (ALRC, 2008).

Data breaches can also occur within the organisation so it is equally important to protect data internally, which most information security professionals consider to be the highest risk to an organisation. Governments amassing data about citizens should think about how best to protect sensitive spatial information from the enemy within.

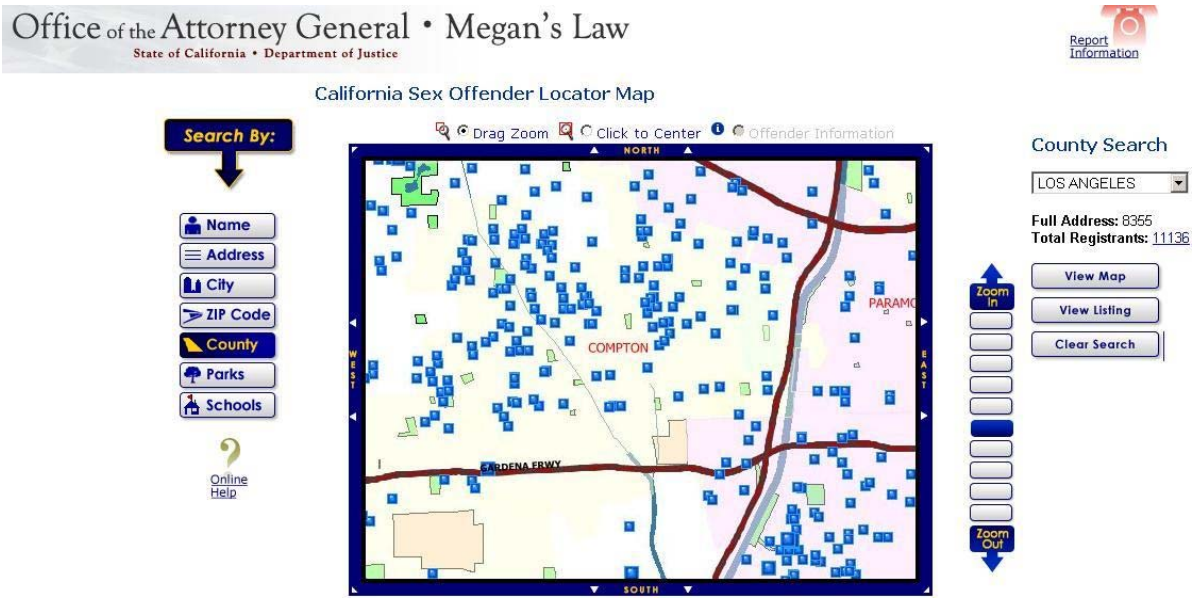

Figure 3: Snapshot of Sex Offender locator map (Source: Megan's Law, 2010)

5.2 Inadvertent Oversharing

While the community has a right to information held by the government, and the best possible outcome for an open, accountable and participatory government is the proactive release of information, careful consideration should be given as to how much information released is appropriate. Government services provide map-based search facility to locate specific offenders, along-with photos, with 'no guarantees of accuracy, completeness, or timeliness of the information' (Megan's Law, 2010). The issue here is that a community vigilante may try and take matters in their own hands (as shown in a contemporary movie, *'Little Children'*) and attack offenders or innocent people being mistaken for offenders. Luckily Australia has not taken that path and this information is available to law enforcement agencies only.

Spotcrime (2010) is very similar in concept where crime statistics are georeferenced and mashed up on Google Maps. It has been claimed that Spotcrime obtains 90% of crime statistics from local police records and in cities where this information is not released, they obtain it from local news sources (Kincaid, 2008). While Spotcrime recognises the sensitivity associated with spatial information related to a particular crime by partially blurring the address details associated to pushpin in their ortho-photos, further zooming in and switching to the 360° panoramic imagery in StreetView can provide a strong hint (street number) about the address rendering this protection redundant.

5.3 Legal Issues

More recently, in the context of the Victorian bushfires, privacy legislation governing the use of the integrated public number database (IPND) prevented it to be used by emergency services which may have been an additional tool for preventing loss of life. There are reports, however, that amendments to the telecommunications legislation have been enacted providing access to data to state emergency services before the next bushfire season (DBCDE, 2009).

ANZLIC (2004) released its spatial privacy guidelines in 2004 which govern how to protect personal information when transferring spatial data amongst government agencies. While these guidelines acknowledge that spatial information, in some contexts, will also be personal information, they do not address situations where spatial information may be used to infer sensitive details about an identifiable individual, as discussed earlier. Sensitive information, as per the Privacy Act requires additional constraints on use and disclosure.

Additionally, Recommendation 12 of the guideline suggests that a licensee of spatial information is accountable for privacy breaches if the spatial information contains personal spatial information or if the licensee can conceivably combine with personal information or any other information to produce spatial information (ANZLIC, 2004). Perhaps future legislative amendments should include a level of responsibility for data creators and custodians instead of transferring the onus to comply with relevant laws to the licensee thus preventing the custodians to turn a blind eye to how others use their services. It would be worthwhile to review these guidelines in the light of recent initiatives such as participatory governance and the increased use of spatial technologies in many aspects of a citizen's life.

6. A FRAMEWORK FOR RESPONSIBLE PARTICIPATORY GEO-GOVERNANCE

6.1 A Privacy Management Framework

Based on the risks identified in Section 5 and discussions pertaining to Geoportals in Section 2 and 3, a framework can be designed to address these privacy challenges. It has been identified that a Geoportal has two essential components, the Catalogue or Search interface which helps in locating data and an application portal which allows interfacing with the data and gaining access to it. The proposed privacy framework is interleaved between these two components as displayed in Figure 4.

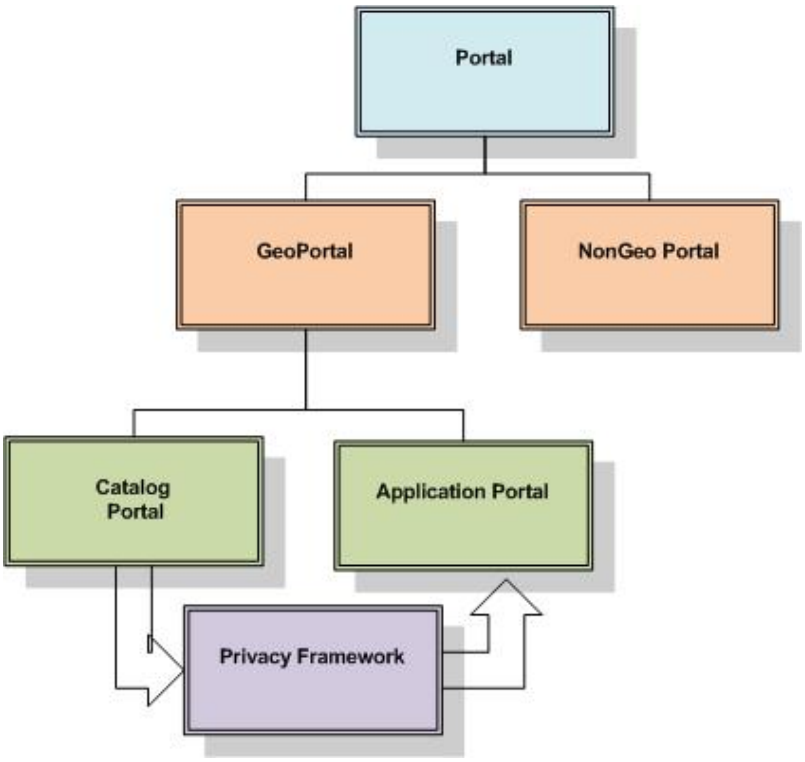

Figure 4: Privacy Framework interaction with the goeportal

This framework consists of privacy strategies to minimize privacy issues before the inception of a project via conducting privacy impact assessments and counter any privacy issues generated after deployment of a project via conducting audits.

Privacy enhancing technologies, on the other hand, provide support on a technological front by utilising capabilities built in the metadata structures and in addition providing tools to hide personal information usign spatial aggregation and minimising unsolicited disclosures.

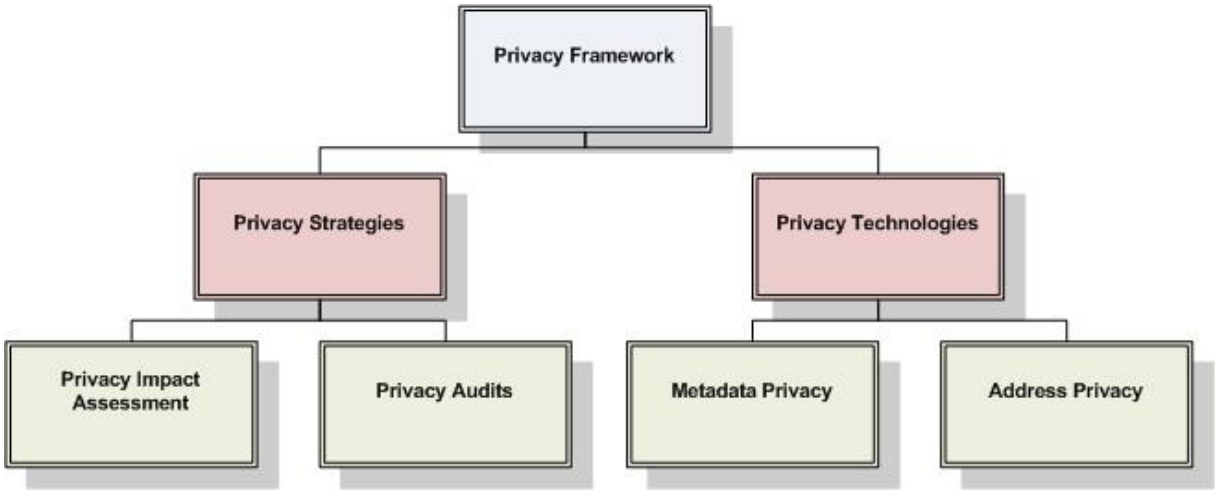

Figure 5: Components of the Privacy Framework

6.2 Privacy Strategies

6.2.1 Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is a risk mitigation tool to identify, manage, minimize and eradicate privacy impacts of new technologies, information systems, policies, programs and processes on privacy of data subjects.The Federal Privacy Commissioner has issued guidelines on how to conduct privacy impact assessments (OFPC, 2006). These statutory offices strongly encourage technology developers and implementers to conduct PIAs for large scale high privacy risk projects and it is expected that PIAs will become a mainstream practice soon.

Traditionally, PIAs of IT projects focus on informational privacy. However, the very nature of spatial data means that bodily and territorial privacy aspects may need to be considered too, thus creating a need for impact assessment of projects that revolve around personal spatial information

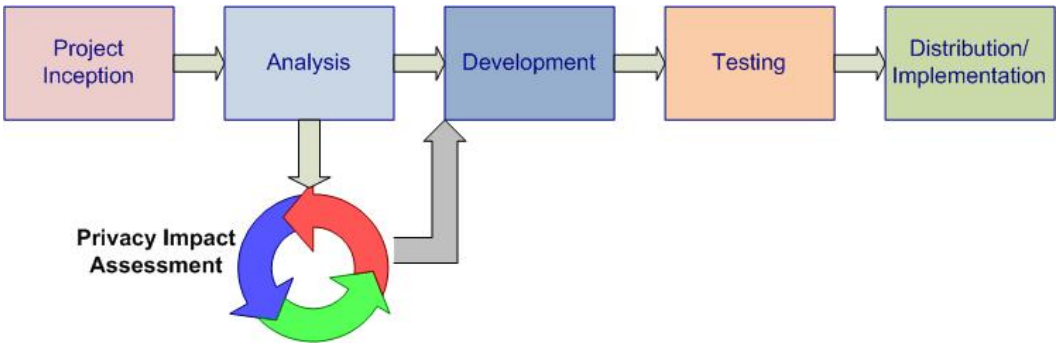

Figure 6: Participation of PIA in project lifecycle

If a proposed project significantly involves spatially driven personal information, then serious consideration should be given to conducting a PIA. As shown in Figure 6, ideally, a PIA is initiated at the early stages of a project to prevent unnecessary effort being expended on options incompatible with the legislative framework or stakeholder expectations. An impact assessment should synthesize the spatial informational inputs and critically analyse them, formulate alternative privacy-sensitive approaches and identify the strengths and weaknesses in the information management life-cycle.

6.2.2 Regular Privacy Audits

Privacy Audits can be a useful progression from the PIA process to measure the effectiveness of current privacy practices. The audit process also gauges compliance with existing legal environment as well as corporate privacy strategies.

Organisations should review their data practices on an on-going basis to ensure that they are appropriate, effective and responsive to current privacy expectations, legislation, and technology. Even though, spatial privacy can still be managed under current information privacy practices, the complex nature of spatial data may pose certain risks to the business that may warrant specific strategies targeted towards spatial privacy management.

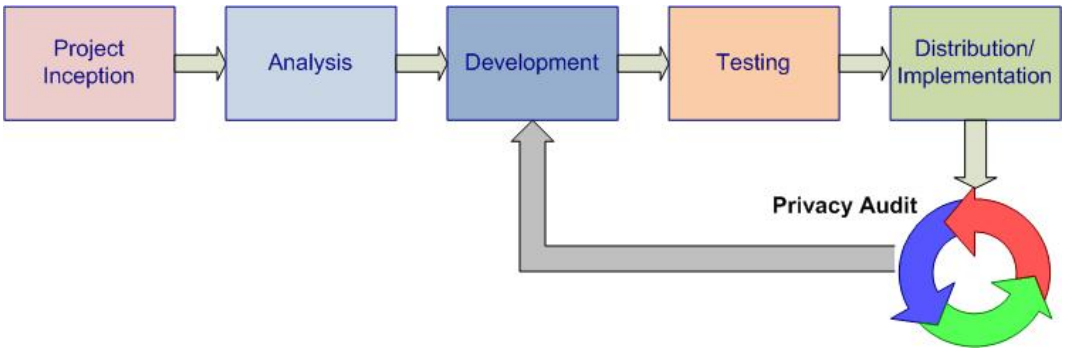

Figure 7: Participation of Audits in the project life cycle

The key deliverable of this process is an audit report which assesses regulatory compliance. The process is targeted at identifying and dealing with problems before they arise in complex technical projects involving spatial data

6.3 Privacy Enhancing Technologies

6.3.1 Restricting Spatial Metadata Visibility

The main issue, throughout the discussion, has not been whether spatial data and metadata should be collected and made accessible, but what restrictions should be applied to its usage and how to define this process. Public agencies now provide geoportals to facilitate access to spatial data by the citizens. The ANZLIC metadata profile, which is an extension of the international ISO 19139 Geographic metadata standard, has an attribute (Use Constraints) that can be used to restrict visibility of metadata (not the resource) for protecting intellectual property rights and privacy.

It is important to understand that elements such as positional accuracy and geographic extents within metadata may reveal some information about spatial data, for instance, the mere knowledge of the existence of metadata on a particular topic with a geographic bounding box may provide indications of the existence of data for an area to somebody who should not have such knowledge. The 'use constraints' attribute would be an effective tool in minimising privacy risks of spatial data and metadata.

OMNILINK has extended the open source Geonetwork software and is currently working on a tighter correlation between use constraints and accessibility and visibility via groups and roles, as a solution to privacy of geographic information at the metadata level.

6.3.2 Cloaking Address Information

As discussed earlier, the spatial component of personal data that most large organisations maintain about their clients is 'Address Information'. Government organizations should collect, use, retain, and disclose data in an anonymised or aggregate format whenever possible in their GIS applications. While there are laws governing organisations' collection, retention and use of this spatial personal information, the risks of data breaches require looking at this problem from a privacy technology dimension as well.

For this we explore spatial blurring and spatial aggregation as two vital tools in achieving spatial privacy of addresses. Figure 8 illustrates the model identified to assign spatial access privileges to different roles within the organisation. This would provide role-based access within an organisation governing the granularity of access to spatial data for various needs such as providing services or erecting map-based reports. For instance, a contractor for a specific project may only need to access the postcode for the client addresses, so their visibility will be restricted using the role-based spatial views. Proper audit mechanisms and reporting would be embedded in the application to identify usage and abuse. This is an effort to protect citizen addresses from misuse without restraining various required reporting functionalities that could use aggregated address data.

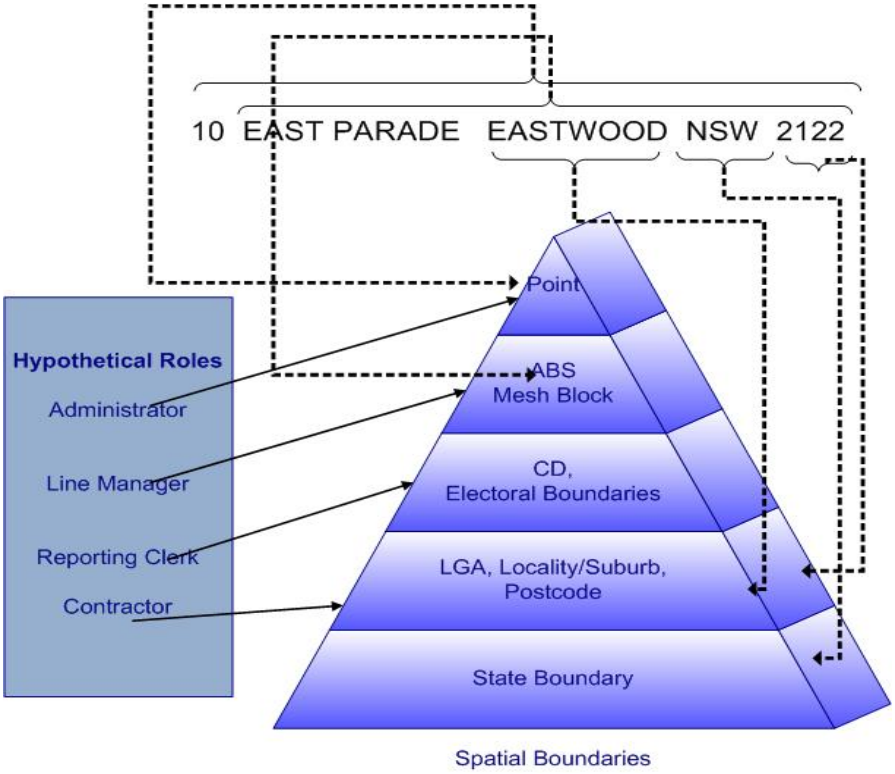

Figure 8: A role-based hierarchical spatial address scheme

7. CONCLUSION

Spatial Information is an enabling technology which holds out the promise of increased efficiency in various government services. It is also an enabler for the participatory governance model and the public-private decision making generally. However, spatial technologies permit the synthesis and analysis of spatial information where isolated pieces of information in a spatial repository when drawn together, give a very detailed picture of a specific location and the people associated with that location. This poses threats to the ideals of democracies and rights of individuals, freedom, security, privacy, and open and free access to government. As we continue to move toward global economies and international networked environments, the need to reconcile competing social, economic, and political interests in digital geographic data will greatly expand.

REFERENCES

Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd. (2001). High Court of Australia. 63.

ALRC (2008) Media Briefing Note 6, ALRC Privacy Enquiry. Accessed (15th January 2010) http://www.alrc.gov.au/media/2008/mbn6.pdf

ANZLIC (2004). Spatial Information Privacy best practice guideline. Accessed (1st January 2010) http://www.anzlic.org.au/policies_privacy.html

Butcher, M., (2008). Accessed (15th January 2010), Updated: BNP member list mashed with Google maps creates a sea of red dots, but dangerously. TechCrunch Europe inaccurate http://uk.techcrunch.com/2008/11/19/bnp-member-list-mashed-with-google-maps-creates-a-sea-of-red-dots

DBCDE (2009). Rudd Government implements COAG agreement on telephone-based emergency warning systems. Media Release. Accessed (8th January 2010) http://www.minister.dbcde.gov.au/media/media_releases/2009/rudd_government_implements_coag_agreement_on_telephon

Clarke, R. (1988). Information Technology and Dataveillance. Communications of the ACM, 31 (5), 498-512.

CRIMTRAC. (2008). Automatic Number Plate Recognition- CrimTrac Scoping Study. Accessed 11th September, 2008, http://www.crimtrac.gov.au/systems projects/AutomatedNumberPlateRecognitionANPR.html

Foord, K. (2002). Defining Privacy (Occasional Paper). Victorian Law Reform Commission.

Franklin, C., Hane, P., (1992). An introduction to GIS: linking maps to databases. Database. 15 (2), PP 17-22.

Iqbal, M.U., Lim, S., (2007). Privacy implications of automated GPS tracking and profiling. Second Workshop on Social Implications of National Security: From Dataveillance to Uberveillance , Wollongong, Australia, 29 October, 225-240.

Iqbal, M.U., Bruce, D., 2009. Perils of Participation- Spatial privacy and geographic metadata in participatory governance. Position Magazine, Issue 40 (Apr-May, 2009).

Kincaid, J., (2008). SpotCrime Keeps You On The Right Side of The Tracks. TechCrunch. Accessed (10th January 2010) http://www.techcrunch.com/2008/05/21/spotcrime-keeps-you-on-the-right-side-of-the-tracks/

Maguire, D.J., Longley, P.A., (2005). The emergence of geoportals and their role in spatial data infrastructures. Computers, Environment, and Urban Systems 29:3-15.

Megan's Law (2010). Search California RegisteredSex Offenders. California Dept. of Justice. Accessed (12th January 2010) http://www.meganslaw.ca.gov/Search.aspx

Moellering, H., H. Aalders and A. Crane (Eds.) (2005) World Spatial Metadata Standards. London: Elsevier Ltd. Pg 5.

National Privacy Principles. (2001). National Privacy Principles. In National Privacy Principles extracted from the Privacy Act, Office of Legislative Drafting, Attorney General's Office. Canberra, Australia.

OFPC (2006). Privacy Impact Assessment Guide. Accessed (2nd January 2010) http://www.privacy.gov.au/publications/pia06/index.html

Ranger, S., (2008). UK nears 100 data breaches in six months, ZDNet News, Accessed (15th January 2010), http://news.zdnet.co.uk/security/0,1000000189,39397458,00.htm

SpotCrime (2010). SpotCrime - Know your neighborhood Accessed (9th January 2010) http://spotcrime.com/

Stone, M.G., Warner, M., (1969). POLITICS, PRIVACY, AND COMPUTERS.The Political Quarterly, 40(3), pg 256-269.

The Privacy Act 1988. (2009). The Privacy Act 1988 - Act No. 119 of 1988 as amended. In Office of Legislative Drafting, Attorney General's Office (p. 35). Canberra, Australia.

Waldo, J., Lin, H. S., & Millett, L. I. (2007). Engaging privacy and information technology in a digital age. Washington, D.C. : The National Academies Press.

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. Harvard Law Review., 4 (5).

Westin, A. F. (1967). Privacy and Freedom. New York : Atheneum.

BIOGRAPHICAL NOTES

Dr. Usman Iqbal

Usman works as a Geospatial Consultant at OMNILINK Pty Ltd. Usman has received his PhD from the School of Surveying and Spatial Information Systems, The University of New South Wales in Spatial Privacy. He has 8 years of experience in the fields of IT and GIS. At OMNILINK, he provides consulting services for metadata management, spatial privacy, and web-based GIS development. He is a board member of the Australian Privacy Foundation.

Mr. David Bruce

David Bruce is a Director of OMNILINK and holds an Honours Degree in Suverying from The University of NSW. David has over 20 years experience in the spatial industry and has a keen interest in metadata standards and their applications to information access across all sectors of government, business and the community. David is an active member of the SSSI and held a position on the NSW Board of Surveying and Spatial Information from 2002 – 2009.

Mr. Ed Garvin

Ed Garvin is Managing Director of OMNILINK Pty Limited, and Partner of Garvin Morgan & Co. He holds tertiary qualifications in Surveying and Urban Studies, an MBA and he is a Registered Surveyor in NSW and ACT. His experience is 40 years in the Surveying, Spatial and Engineering professions and he has established and run 2 businesses in these disciplines for over 20 years. He is a Director of the Australian Spatial Information Business Association and a part-time lecturer at the University of NSW in Business Management.

CONTACTS

Dr. Usman Iqbal
OMNILINK Pty Ltd
Suite 1, 10 East Parade
Eastwood NSW 2122, Australia
Tel. +612 9804 8807
Fax + 612 9804 7901
Email: usmani@omnilink.com.au
Web site: http://www.omnilink.com.au

Mr. David Bruce
OMNILINK Pty Ltd
Suite 1, 10 East Parade
Eastwood NSW 2122, Australia
Email: davidb@omnilink.com.au

Mr. Ed Garvin
OMNILINK Pty Ltd
Suite 1, 10 East Parade
Eastwood NSW 2122, Australia
Email: edg@omnilink.com.au