LOCATION PRIVACY UNDER DIRE THREAT AS UBERVEILLANCE STALKS THE STREETS

By Katina Michael and Roger Clarke

Abstract

Location tracking and monitoring applications have proliferated with the arrival of smart phones that are equipped with onboard global positioning system (GPS) chipsets. It is now possible to locate a smart phone user down to 10 metres of accuracy on average. Innovators have been quick to capitalise on this emerging market by introducing novel pedestrian tracking technologies which can denote the geographic path of a mobile user. At the same time there is contention by law enforcement personnel over the need for a warrant process to track an individual in a public space. This paper considers the future of location based people tracking in Australia and emphasises the importance of citizen consent.

COVERT PEOPLE TRACKING AND MONITORING

Knowing where someone has been,[1] what they are doing right now, and being able to predict where they might go next using historical or near real-time data is incredibly powerful.[2] Humans do not move around in a random manner.[3] The implementation of such tracking and monitoring location services are very important in the emergency sector but we are now witnessing the seemingly "legal" deployment of new applications that allow for real-time people tracking in closed campus-based zones like shopping malls, airports and transport hubs, as well as neighbouring locations. This kind of covert tracking can only be described as a type of secret surveillance. Not only is it secret but it is also atypical and indiscriminate. Secret surveillance differs from covert surveillance because the subject never finds out that they have been watched. In covert surveillance, the subject does not know they are being watched at the time the surveillance is occurring but will likely find out after-the-fact.

When one visits a shopping mall they find themselves surrounded by CCTV cameras. From the parking lot to the shopping mall walkways, and from the cafeterias to the stores they visit, customers are always under surveillance. At least notices like "you are now being watched" or "smile you are being recorded" let consumers explicitly know that they are under observation. But the tracking of a mobile phone throughout a complex has a look-and-feel to it that essentially goes above and beyond CCTV- it is an all-encompassing, all-pervading view of the citizen. It is in other words an "uber" view, providing a set of uber analytics to shopping complex owners and their constituents. Despite uberveillance[4] having become synonymous with planetary scale systems in a global theatre, uberveillance can be equally detrimental within a limited geographic space.[5] Uberveillance has to do with the ability to obtain identification, near real-time location tracking and condition monitoring of the subject. It answers the fundamental who, where and when questions in an attempt to derive why, what and how. It is more than traditional forms of visual surveillance like CCTV and the linking together of personal information with consumer credit transaction data- it is the sum total of various types of surveillance.[6]

Obscure Commercial Location-Based Services

In almost every case citizens are oblivious to the fact that the temporary mobile subscriber identity is being transmitted from their mobile phone, allowing for multilateration of their exact location in the shopping mall.[7] The other issue is that they have not formally consented to providing such mobile phone data to a third party, in this case a location service provider (LSP) whom they have never had contact with, and whom it is very likely their mobile telephone operator has never had contact with. Private organisations developing these mobile tracking solutions, state that they are not gaining access to any personal information such as a name, mobile telephone number or contents of a short message service (SMS). They stress they are simply using "complex algorithms" to denote the geographic position of a mobile, using strategically located "proprietary equipment" in a campus setting.[8]

Up until now, citizens have been subjected to "legitimate" surveillance of various degrees and orders of granularity by the government in the name of national security. We are now conceivably opening the floodgates for anyone who has the relevant technology to join the ranks. The Australian Parliament has unquestioningly granted powers to national security agencies to use location technology to track citizens under the Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Act 2003 and to intercept telecommunications. Similarly, parliamentarians have failed the public by permitting a warrant to be signed by the Attorney General to temporarily allow special investigative powers to track a suspect or their vehicle for a period of time.[9] But are these already-gross breaches of the principle of a free society to be extended to the authorisation of a private organisation to track mobiles of ordinary citizens because it may lead to better services planning or more efficient advertising and marketing?[10]

INVADING THE LOCATION PRIVACY OF A CONSUMER

Whether or not providers of new services are breaching the applicable statutory Privacy Principles, they are invading the locational privacy of each user. One interpretation of location privacy is that it "is the ability of an individual to move in public space with the expectation that under normal circumstances their location will not be systematically and secretly recorded for later use".[11] A more concise definition of location privacy is the interest an individual has in controlling information about their location. Tracking privacy follows as the interest an individual has in controlling information about their sequence of locations. Contrary to the assertions of consumer-marketing corporations, privacy expectations always have existed in public spaces, and continue to exist.[12]

Users demand that services such as a personal location chronicle system, people follower or footpath route tracker system that systematically collects personal location information from a personal device they are carrying, can only be provided on the basis of consent, that is to say voluntary opt-in.[13] This data is highly sensitive because it can be used to conduct behavioural profiling of individuals (even if they remain "nameless") in particular social settings. They may even provide any organisation that gains access to the data the capacity to make judgements on individuals based on their choices of which stores they walk into and which they do not. For example, if a subscriber visits a

particular religious bookstore within a shopping mall on a weekly basis, the assumption can be made that they are in some way affiliated to that religion.[14]

While corporations and law enforcement agencies assert that individuals cannot have a reasonable expectation of privacy in a public space, tracking the movements of a person as they go about their business is in fact a breach of a fundamental expectation to be let alone. In policing for example, in most democratic countries, it is against the law to covertly track an individual or their vehicle without prior approval of a warrant. Tracking by any means has always required legal authority, although this principle has been compromised in many countries since 2001. Warrantless tracking[15] using a mobile phone (or any other electronic instrument such as a GPS strapped to a vehicle), generally results in evidence obtained without the proper authority and is inadmissible in a court of law. Some law enforcement agencies have argued for the abolition of the warrant process because the red tape often means that valuable information is lost and the suspect cannot be prosecuted for a crime they have likely committed.[16] These issues are not new but far from eliminating a warrant process the appropriate response it to invest the energy in streamlining this process.[17]

The Potential for Warrantless Tracking

Warrantless tracking is largely against the law even when undertaken by law enforcement personnel in Australia. How then can it be in any way acceptable for a form of warrantless tracking to be undertaken by or on behalf of corporations or mainstream government agencies, of shoppers in a mall, or travellers in an airport, or commuters in a transport hub? Why should an LSP have the right to do what a law enforcement agency cannot normally do? It is very disturbing that this kind of invasion of locational privacy involves no incentive, no value proposition for the individual whose mobile is being tracked, and of course and more importantly it is being done without their knowledge.[18] Companies specialising in these kinds of location intelligence applications are interested in how they might help shopping mall owners better value their floorspace in terms of rental revenues, and to identify points of on-foot traffic congestion to on-sell physical advertising and marketing floorspace.[19] In short, they are making a profit from devices possessed by the average citizen who has visited a shopping mall for the purchase of goods and services. In reality, an entity is covertly collecting data from the citizen that could be used in various ways to exploit the person in financial or other ways. Even if privacy were not a human right, this would demand statutory intervention on the public policy grounds of commercial unfairness.

Organisations specialising in these solutions may state in their disclaimer that they are not collecting, or are not disclosing personally identifiable information, and that they only ever provide aggregated data at varying zone levels to the shopping mall owners. There is no explicit definition of what constitutes a zone however, only that aggregated data at the smallest zone level that is at the highest geographic resolution, is more expensive to purchase. The information that can be captured among other details includes:

- dwell times in front of shop windows
- repeat visits by shoppers in varying frequency durations

- typical route/ circuit paths taken by shoppers as they go from shop to shop during a given shopping experience.[20]

More disturbing still is that some companies claim that their proprietary technology can acquire data that can derive the nationality of the cell phone owner.[21] This is despite the fact that this kind of action flies in the face of telephonic interception laws, and that mobile phones and SIM cards are transferable items.

In addition to the "transparency" that this process inflicts on the shopper is the disturbing potential to collect data about the interactions of a given shopper(s) at a given mall, and then to also follow them to a neighbouring area such as a nearby town centre.[22] This would mean that individuals were being tracked, potentially directly to their place of residence or place of employment, depending on the distance range of the network equipment element used to track the location of a shopper. Even if only aggregated data is sold to businesses, the individual records still reside on the LSP's database server, possibly even outside the local jurisdiction. There is also the potential of overlaying this data with other personal information, including visual surveillance footage and customer transaction histories.[23] The notion of dataveillance here is especially important "…the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons."[24] This is where traditional visual surveillance intersects with data surveillance giving breath to what is now being dubbed "smart" surveillance.[25]

WHAT REGULATORY PROTECTIONS FOR CONSUMERS?

What are the rights of the consumer in a situation like this? And do users have control over their personal locational information? Clearly they do not. One need only ponder what rights employees might have if such a system was ever to be instituted in an organisational or employment setting, and what types of workplace surveillance laws might protect the employee from constant monitoring. This applies to commuters at an airport. In short, there has been no established social contract entered into between the parties, rendering the subscriber powerless. It is a blanket coverage application that monitors people on a large campus.

Some of the LSPs offering such services have not even stated clearly who has access to the data, where it is transferred for processing, and the length of time it will be retained.[26] The claim of 1-2 metre locational accuracy, which has yet to be supported by experimental test cases is also contestable, which raises questions about the reliability of inferences that the LSP or the shop-owner draw. If the data is the subject of a warrant or subpoena, the data's inaccuracy could result in false accusations and even a miscarriage of justice, with the "wrong" person finding themselves in the "right place" at the "right time".

Privacy laws are being continually eroded by exceptions built into subsequent legislation and by technological capabilities that were not contemplated when the laws were passed. Location privacy has yet to be specifically addressed in any Australian privacy legislation. The state of Victoria has responded generally to locational privacy, among other forms of privacy, by introducing a Victorian Charter of Human Rights and Responsibilities that

came into force on 1 January 2007.[27] The Telecommunications (Interception) Amendment Act 2006 and the Surveillance Devices Act 2004, however, do cover inappropriate interception and access, use, communication and publication of location information that is obtained from mobile device traffic.[28] On the other hand, when Google Inc. intercepted wi-fi signals and recorded the data they contained, the Privacy Commissioner absolved the company,[29] and the Australian Federal Police refused to prosecute despite a clear (although possibly "inadvertent") breach of the criminal law.[30]

Industry Guidelines

In 2010, the Australian Mobile Telecommunications Association (AMTA) released new industry guidelines to help promote the privacy of people using location-based services (LBS) on mobile devices. AMTA specifically called on location service providers to act in a manner befitting existing legislation in Australia. AMTA provided the following guidelines:

1. every LBS must be provided on an opt-in basis with a specific request from a user for the service;
2. every LBS must comply with all relevant privacy legislation;
3. every LBS must be designed to guard against consumers being located without their knowledge;
4. every LBS must allow consumers to maintain full control; and
5. every LBS must enable customers to control who uses their location information and when that is appropriate, and be able to stop or suspend a service easily should they wish.[31]

Point 2 is a matter for Parliaments, privacy oversight agencies and law enforcement agencies, not industry, and is not a matter for industry guidelines.

The real problem however is that industry guidelines are just not effective. Generally, if a code does contain provisions of value, then it is likely to be ignored by industry members. This has been the case with the Biometrics Code. In December 2010, the Biometrics Institute reported that it was "still struggling to get members to sign onto its voluntary biometric privacy code… Moeller said this is because businesses are reluctant to impose guidelines that may restrict their competitiveness against non-compliant rivals. It would also make it tougher to implement biometrics solutions." Ironically, industry still point to guidelines claiming self-regulatory schemes are in place, when in fact there is nothing that is enforceable by law. In short, self-regulatory codes for the greater part are a political tool to avoid regulation.

PROPOSED WAYS FORWARD

In the United States two senators recently proposed a Location Privacy Protection Act which is meant to empower mobile phone subscribers.[32] The bill provides that an organisation that collected location data from mobile or wireless data devices would have to explicitly state in their privacy policies what was being collected, in plain English. Essentially this is the recommendation of the Internet Engineering Task Force for Geographic Location/Privacy (IETF GEOPRIV) working group which finalised that technical systems include "Fair Information Practices to defend against harms associated with the use of location technologies."[33] These practices should be thought of as

"countermeasures" to technical systems that handle personal information such as location data. Another two United States senators acted similarly, in the same month the Location Privacy Protection bill was put forward, announcing the GPS Act meant to stamp down on warrantless tracking by law enforcement personnel. This bill is supposed to "balance the needs of Americans' privacy protections with the legitimate needs of law enforcement, and maintains emergency exceptions."[34] One downside is the narrowness of the definition- next will come the Wi-Fi Act, the A-GPS Act etc. That approach is obviously unviable in the longer term as new innovations emerge. Acts must strive for appropriate generality and avoid inappropriate technology-specificity, and should be based on semantics not syntax. But the much more serious problem is that the provision represents legal authorisation for grossly privacy-invasive location and tracking. IETF engineers, and now Congressmen, want to compromise human rights and increase the imbalance of power between business and consumers.

When one assesses the current climate of technological deployment, the observation is made that information risks are addressed only as they emerge. There is a reactive force at play rather than a proactive force to ensure avoidance or mitigation of potential privacy breaches in the uberveillance trajectory. In Australia at least, existing laws hardly address the locational privacy issues that are facing the public. The problem is that there are bits and pieces of statute that pertain to parts of the problem under separate legislative regimes and in separate jurisdictions. There is no overarching framework for or even consistency among the laws. This causes confusion and inevitably results in inadequate protections for citizens.[35]

One approach to the problem would be a Location Privacy Protection Act or a GPS Act, as has been proposed in the United States, although it would need to embody far stronger protections than mere notification of the privacy breaches that the technology entails. An alternative is amendment of the current privacy legislation and other anti-terrorism legislation in order to create appropriate regulatory provisions, and deny the gaps that LSPs are exploiting.[36] It is time that sensitive data like location information and DNA profile data be protected through improved legislation, with "guidelines" no longer being used as a substitute for actual protections but instead playing a supporting role. The social implications of not proceeding to protect citizen rights[37] where personal location information is concerned will inevitably lead to disproportionate covert surveillance being conducted by government and business, and even citizens.[38]

Dr Katina Michael is an associate professor at the University of Wollongong. She teaches in the School of Information Systems and Technology and the Centre for Transnational Crime Prevention. She is a co-editor of the *Social Implications of Covert Policing* (2010). Phone (02) 42213937 Email katina@uow.edu.au

Dr Roger Clarke is principal of Xamax Consultancy Pty Ltd, Canberra. He is also a visiting professor in the Cyberspace Law & Policy Centre at the UNSW and in Computer Science at ANU. He has been a Board-member of the Australian Privacy Foundation since 1987, and its Chair since 2006. Roger.Clarke@xamax.com.au

[1] R Clarke and M Wigan, 'You are where you've been: The privacy implications of location and tracking technologies', *Journal of Location Based Services*, 2012, in press.
[2] R Abbas, 'The social and behavioural implications of location-based services: An observational study of users', *Journal of Location Based Services*, 2011, in press.
[3] C Song, Z Qu, N Blumm and A-L Barabási1, 'Limits of predictability in human mobility', *Science*, 327(5968), 2010, pp1018-21.
[4] MG Michael and K Michael, 'Towards a state of uberveillance', *IEEE Technology and Society Magazine*, 29(2), 2010, pp9-16.
[5] K Michael, G Roussos, GQ Huang, R Gadh, A Chattopadhyay, S Prabhu, and P Chu, 'Planetary-scale RFID services in an age of uberveillance', *Proceedings of the IEEE*, 98(9), 2010, pp1663-71.
[6] MG Michael and K Michael, see note 4 above, p9.
[7] K Collier, 'Shopping centres' Big Brother plan to track customers', *Herald Sun*, 14 October 2011, http://www.heraldsun.com.au/news/more-news/shopping-centres-big-brother-plan-to-track-customers/story-fn7x8me2-1226166191503
[8] See for example: Path Intelligence, 'Our Commitment to Privacy', 2010, http://www.pathintelligence.com/en/products/footpath/privacy
[9] DM Jay, 'Use of covert surveillance obtained by search warrant', *Australian Law Journal*, 73(1), Jan 1999, pp34-6.
[10] K Collier, 'Stores spy on shoppers', *Herald* Sun, 12 October 2011, http://www.heraldsun.com.au/news/more-news/stores-spy-on-shoppers/story-fn7x8me2-1226164244739
[11] AJ Blumberg and P Eckersley, 'On locational privacy, and how to avoid losing it forever', *Electronic Frontier Foundation*, August 2009, https://www.eff.org/wp/locational-privacy
[12] Victorian Law Reform Commission, *Surveillance in Public Spaces*, Final Report 18, March 2010, http://www.lawreform.vic.gov.au/wps/wcm/connect/justlib/Law+Reform/resources/3/6/36418680438a4b4eacc0fd34222e6833/Surveillance_final_report.pdf
[13] K Collier, ''Creepy' Path Intelligence retail technology tracks shoppers', *news.com.au*, 14 October 2011. http://www.news.com.au/money/creepy-retail-technology-tracks-shoppers/story-e6frfmci-1226166413071
[14] AA Otterberg, 'Note: GPS tracking technology: The case for revisiting Knotts and shifting the Supreme Court's theory of the public space under the Fourth Amendment', *Boston College Law Review*, 46, 2005, pp661-704.
[15] IJ Samuel, 'Warrantless location tracking', *New York University Law Review*, 83, 2008, pp1324-52.
[16] JS Ganz, 'It's already public: why federal officers should not need warrants to use GPS vehicle tracking devices', *Journal of Criminal Law and Criminology*, 95(4), Summer 2005, pp1325-37.
[17] S Bronitt, 'Regulating covert policing methods: from reactive to proactive models of admissibility', In. S Bronitt, C. Harfield and K Michael, *The Social Implications of Covert Policing*, 2010, pp9-14.
[18] BD Renegar, K Michael and MG Michael, 'Privacy, value and control issues in four mobile business applications', *Seventh International Conference on Mobile Business*, 2008, pp30-40.
[19] See for example: FootPath Pricing, 2010, http://www.pathintelligence.com/en/products/footpath/footpath-pricing
[20] Path Intelligence, see note 8 above.
[21] Path Intelligence, see note 19 above.
[22] *Ibid.*
[23] K Michael and MG Michael, *From Dataveillance to Überveillance and the Realpolitik of the Transparent Society*, 2007.
[24] R Clarke, 'Information technology and dataveillance', *Communications of the ACM*, 31(5), May 1988, pp498-512.
[25] IBM, 'IBM Smart Surveillance System (Previous PeopleVision Project)', *IBM Research*, 30 October 2011, http://www.research.ibm.com/peoplevision/
[26] B Arnold, 'Privacy guide', *Caslon Analytics*, May 2008, http://www.caslon.com.au/privacyguide19.htm
[27] H Versey, Office of the Victorian Privacy Commissioner, *Speech*, 13 February 2009, http://www.privacy.vic.gov.au/privacy/web2.nsf/files/update-on-privacy-laws/$file/helen_versey_speech_13_02_09.pdf
[28] AG, 'What the Government is doing: Surveillance Device Act 2004', 25 May 2005, *Australian Government*,

http://www.ag.gov.au/agd/www/nationalsecurity.nsf/AllDocs/9B1F97B59105AEE6CA25700C0014CAF5?OpenDocument

[29] Riley J., 'Gov't 'travesty' in Google privacy case', ITWire, Wednesday, 03 November 2010 20:44, at http://www.itwire.com/it-policy-news/regulation/42898-govt-travesty-in-google-privacy-case

[30] Moses A., 'Google escapes criminal charges for Wi-Fi snooping' The Sydney Morning Herald, 6 December 2010, at http://www.smh.com.au/technology/security/google-escapes-criminal-charges-for-wifi-snooping-20101206-18lot.html

[31] AMTA, New mobile telecommunications industry guidelines and consumer tips set benchmark for Location Based Services'
http://www.amta.org.au/articles/New.mobile.telecommunications.industry.guidelines.and.consumer.tips.set.benchmark.for.Location.Based.Services, 2010.

[32] J Cheng, 'Franken's location-privacy bill would close mobile-tracking 'loopholes'', Wired: Epicenter, 17 June 2011, http://www.wired.com/epicenter/2011/06/franken-location-loopholes/

[33] EPIC, 'Privacy and human rights report 2006', *WorldLII*, 2006,
http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Location.html

[34] N Anderson, 'Bipartisan bill would end government's warrantless GPS tracking', *Ars Technica: Law and Policy*,
http://arstechnica.com/tech-policy/news/2011/06/bipartisan-bill-would-end-governments-warrantless-gps-tracking.ars

[35] ALRC, 'For your information: Australian privacy law and practice (ALRC Report 108)', *Australian Government*, 2, pp.1409-10, http://www.alrc.gov.au/publications/report-108

[36] A Koppel, 'Warranting a warrant: Fourth Amendment concerns raised by law enforcement's warrantless use of GPS and cellular phone tracking', *University of Miami Law Review*, 64(3), April 2010, pp1061-89.

[37] AA Gillespie, 'Covert surveillance, human rights and the law', *Irish Criminal Law Journal*, 19(3), August 2009, pp71-9.

[38] R Abbas, K Michael, MG Michael and A Aloudat, 'Emerging forms of covert surveillance using GPS-enabled devices', *Journal of Cases on Information Technology*, 13(2), 2011, pp19-33.