

Location and Tracking of Mobile Devices: Überveillance Stalks the Streets

Review Version of 7 October 2012

Katina Michael and Roger Clarke

Abstract

During the last decade, location-tracking and monitoring applications have proliferated, in mobile cellular and wireless data networks, and through self-reporting by applications running in smartphones that are equipped with onboard global positioning system (GPS) chipsets. It is now possible to locate a smartphone-user's location not merely to a cell, but to a small area within it. Innovators have been quick to capitalise on these location-based technologies for commercial purposes, and have gained access to a great deal of sensitive personal data in the process. In addition, law enforcement utilise these technologies, can do so inexpensively and hence can track many more people. Moreover, these agencies seek the power to conduct tracking covertly, and without a judicial warrant. This article investigates the dimensions of the problem of people-tracking through the devices that they carry. Location surveillance has very serious negative implications for individuals, yet there are very limited safeguards. It is incumbent on legislatures to address these problems, through both domestic laws and multilateral processes.

Keywords: location-based systems (LBS), cellular mobile, wireless LAN, GPS, mobile device signatures (MDS), privacy, surveillance

1. Introduction

Personal electronic devices travel with people, are worn by them, and are, or soon will be, inside them. Those devices are increasingly capable of being located, and, by recording the succession of locations, tracked. This creates a variety of opportunities for the people concerned. It also gives rise to a wide range of opportunities for organisations, at least some of which are detrimental to the person's interests.

Commonly, the focus of discussion of this topic falls on mobile phones and tablets. It is intrinsic to the network technologies on which those devices depend that the network operator has at least some knowledge of the location of each handset. In addition, many such devices have onboard global positioning system (GPS) chipsets, and self-report their coordinates to service-providers. The scope of this paper encompasses those already-well-known forms of location and tracking, but it extends beyond them.

The paper begins by outlining the various technologies that enable location and tracking, and identifies those technologies' key attributes. The many forms of surveillance are then reviewed, in order to establish a framework within which applications of location and tracking can be characterised. Applications are described, and their implications summarised. Controls are considered, whereby potential harm to the interests of individuals can be prevented or mitigated.

2. Relevant Technologies

The technologies considered here involve a device that has the following characteristics:

- it is conveniently portable by a human, and
- it emits signals that:
 - enable some other device to compute the location of the device (and hence of the person), and
 - are sufficiently distinctive that the device is reliably identifiable at least among those in the vicinity, and hence the device's (and hence the person's) successive locations can be detected, and combined into a trail

The primary form-factors for mobile devices are currently clam-shape (portable PCs), thin rectangles suitable for the hand (mobile phones), and flat forms (tablets). Many other form-factors are also relevant, however. Anklets imposed on dangerous prisoners, and even as conditions of bail, carry RFID tags. Chips are carried in cards of various sizes, particularly the size of credit-cards, and used for tickets for public transport and entertainment venues, aircraft boarding-passes, toll-road payments and in some countries to carry electronic cash. Chips may conduct transactions with other devices by contact-based means, or

contactless, using radio-frequency identification (RFID) or its shorter-range version near-field communication (NFC) technologies. These capabilities are in credit and debit cards in many countries. Transactions may occur with the cardholder's knowledge, with their express consent, and with an authentication step to achieve confidence that the person using the card is authorised to do so. In a variety of circumstances, however, some and even all of those safeguards are dispensed with. The electronic versions of passports that are commonly now being issued carry such a chip, and have an autonomous communications capability. The widespread issue of cards with capabilities uncontrolled by, and in many cases unknown to, the cardholder, is causing consternation among segments of the population that have become aware of the schemes.

Such chips can be readily carried in other forms, including jewellery such as finger-rings, and belt-buckles. Endo-prostheses such as replacement hips and knees and heart pacemakers can readily carry chips. A few people have voluntarily embedded chips directly into their bodies for such purposes as automated entry to premises (Michael & Michael 2009).

In order to locate and track such devices, any sufficiently distinctive signals may in principle suffice. See Raper et al. (2007a) and Mautz (2011). In practice, the signals involved are commonly those transmitted by a device in order to take advantage of wireless telecommunications networks. The scope of the relevant technologies therefore also encompasses the signals, devices that detect the signals, and the networks over which the data that the signals contain are transmitted.

In wireless networks, it is generally the case that the base station or router needs to be aware of the identities of devices that are currently within the cell. A key reason for this is to conserve limited transmission capacity by sending messages only when the targeted device is known to be in the cell. This applies to all of:

- cellular mobile originally designed for voice telephony and extended to data (in particular those using the '3G' standards GSM/GPRS, CDMA2000 and UMTS/HSPA and the '4G' standard LTE)
- wireless local area networks (WLANs, commonly Wifi / IEEE 802.11x – RE 2010a)
- wireless wide area networks (WWANs, commonly WiMAX / IEEE 802.16x – RE 2010b).

Devices in such networks are uniquely identified by various means (Clarke & Wigan 2011). In cellular networks, there is generally a clear distinction between the entity (the handset) and the identity it is adopting at any given time (which is determined by the module inserted in it). Depending on the particular standards used, what is commonly referred to as 'the SIM-card' is an R-UIM, a CSIM or a USIM. These modules store an International Mobile Subscriber Identity (IMSI), which constitutes the handset's identifier. Among other things, this enables network operators to determine whether or not to provide service, and what tariff to apply to the traffic. However, cellular network protocols may also

involve transmission of a code that distinguishes the handset itself, within which the module is currently inserted. A useful generic term for this is the device 'entifier' (Clarke 2009b). Under the various standards, it may be referred to as an International Mobile Equipment Identity (IMEI), ESN, or MEID.

In Wifi and WiMAX networks, the device entifier may be a processor-id or more commonly a network interface card identifier (NIC Id). In various circumstances, other device-identifiers may be used, such as a phone-number, or an IP-address may be used as a proxy. In addition, the human using the device may be directly identified, e.g. by means of a user-accountname.

A WWAN cell may cover a large area, indicatively of a 50km radius. Telephony cells may have a radius as large as 2-3 km or as little as a hundred metres. WLANs using Wifi technologies have a cell-size of less than 1 hectare, indicatively 50-100 metres radius, but in practice often constrained by environmental factors to only 10-30 metres.

The base-station or router knows the identities of devices that are within its cell, because this is a technically necessary feature of the cell's operation. Mobile devices auto-report their presence 10 times per second. Meanwhile, the locations of base-stations for cellular services are known with considerable accuracy by the telecommunications providers. And, in the case of most private Wifi services, the location of the router is mapped to c. 30-100 metre accuracy by services such as Skyhook and Google Locations, which perform what have been dubbed 'war drives' in order to maintain their databases – in Google's case in probable violation of the telecommunications interception and/or privacy laws of at least a dozen countries (EPIC 2012).

Knowing that a device is within a particular mobile phone, WiMAX or Wifi cell provides only a rough indication of location. In order to generate a more precise estimate, within a cell, several techniques are used (McGuire et al. 2005). These include the following (adapted from Clarke & Wigan 2011. See also Figueiras & Frattasi 2010):

- directional analysis. A single base-station may comprise multiple receivers at known locations and pointed in known directions, enabling the handset's location within the cell to be reduced to a sector within the cell, and possibly a narrow one, although without information about the distance along the sector;
- triangulation. This involves multiple base-stations serving a single cell, at known locations some distance apart, and each with directional analysis capabilities. Particularly with three or more stations, this enables an inference that the device's location is within a small area at the intersection of the multiple directional plots;
- signal analysis. This involves analysis of the characteristics of the signals exchanged between the handset and base-station, in order to infer the distance between them. Relevant signal characteristics include the apparent response-delay (Time Difference of Arrival – TDOA, also referred to as

multilateration), and strength (Received Signal Strength Indicator – RSSI),

The precision and reliability of these techniques varies greatly, depending on the circumstances prevailing at the time. The variability and unpredictability result in many mutually inconsistent statements by suppliers, in the general media, and even in the technical literature.

Techniques for cellular networks generally provide reasonably reliable estimates of location to within an indicative 50-100m in urban areas and some hundreds of metres elsewhere. Worse performance has been reported in some field-tests, however. For example, Dahunsi & Dwolatzky (2012) found the accuracy of GSM location in Johannesburg to be in the range 200-1400m, and highly variable, with "a huge difference between the predicted and provided accuracies by mobile location providers".

The web-site of the Skyhook Wifi-router positioning service claims 10-metre accuracy, 1-second time-to-first-fix and 99.8% reliability (SHW 2012). On the other hand, tests have resulted in far lower accuracy measures, including an average positional error of 63m in Sydney (Gallagher et al. 2009) and "median values for positional accuracy in [Las Vegas, Miami and San Diego, which] ranged from 43 to 92 metres ... [and] the replicability ... was relatively poor" (Zandbergen 2012, p. 35). Nonetheless, a recent research article suggested the feasibility of "uncooperatively and covertly detecting people 'through the wall' [by means of their WiFi transmissions]" (Chetty et al. 2012).

Another way in which a device's location may become known to other devices is through self-reporting of the device's position, most commonly by means of an inbuilt Global Positioning System (GPS) chip-set. This provides coordinates and altitude based on broadcast signals received from a network of satellites. In any particular instance, the user of the device may or may not be aware that location is being disclosed.

Despite widespread enthusiasm and a moderate level of use, GPS is subject to a number of important limitations. The signals are subject to interference from atmospheric conditions, buildings and trees, and the time to achieve a fix on enough satellites and deliver a location measure may be long. This results in variability in its practical usefulness in different circumstances, and in its accuracy and reliability. Civil-use GPS coordinates are claimed to provide accuracy within a theoretical 7.8m at a 95% confidence level (USGov 2012), but various reports suggest 15m, or 20m, or 30m, but sometimes 100m. It may be affected by radio interference and jamming. The original and still-dominant GPS service operated by the US Government was subject to intentional degradation in the US's national interests. This 'Selective Availability' feature still exists, although subject to a decade-long policy not to use it; and future generations of GPS satellites may no longer support it.

Hybrid schemes exist that use two or more sources in order to generate more accurate location-estimates, or to generate estimates more quickly. In particular, Assisted GPS (A-GPS) utilises data from terrestrial servers accessed over cellular networks in order to more efficiently process satellite-derived data (e.g. RE 2012).

Further categories of location and tracking technologies emerge from time to time. A current example uses means described by the present authors as 'mobile device signatures' (MDS). A device may monitor the signals emanating from a user's mobile device, without being part of the network that the user's device is communicating with. The eavesdropping device may detect particular signal characteristics that distinguish the user's mobile device from others in the vicinity. In addition, it may apply any of the various techniques mentioned above, in order to locate the device. If the signal characteristics are persistent, the eavesdropping device can track the user's mobile device, and hence the person carrying it. No formal literature on MDS has yet been located. The supplier's brief description is at PI (2010b).

The various technologies described in this section are capable of being applied to many purposes. The focus in this paper is on their application to surveillance.

3. Surveillance

The term surveillance refers to the systematic investigation or monitoring of the actions or communications of one or more persons (Clarke 2009c). Until recent times, surveillance was visual, and depended on physical proximity of an observer to the observed. The volume of surveillance conducted was kept in check by the costs involved. Surveillance aids and enhancements emerged, such as binoculars and, later, directional microphones. During the 19th century, the post was intercepted, and telephones were tapped. During the 20th century, cameras enabled transmission of image, video and sound to remote locations, and recording for future use (e.g. Parenti 2003).

With the surge in stored personal data that accompanied the application of computing to administration in the 1970s and 1980s, dataveillance emerged (Clarke 1988). Monitoring people through their digital personae rather than through physical observation of their behaviour is much more economical, and hence many more people can be subjected to it (Clarke 1994). The dataveillance epidemic made it more important than ever to clearly distinguish between personal surveillance – of an identified person who has previously come to attention – and mass surveillance – of many people, not necessarily previously identified, about some or all of whom suspicion could be generated.

Location data is of a very particular nature, and hence it has become necessary to distinguish location surveillance as a sub-set of the general category of dataveillance. There are several categories of location surveillance with different characteristics (Clarke & Wigan 2011):

- capture of an individual's location at a point in time. Depending on the context, this may support inferences being drawn about an individual's behaviour, purpose, intention and associates

- real-time monitoring of a succession of locations and hence of the person's direction of movement. This is far richer data, and supports much more confident inferences being drawn about an individual's behaviour, purpose, intention and associates
- predictive tracking, by extrapolation from the person's direction of movement, enabling inferences to be drawn about near-future behaviour, purpose, intention and associates
- retrospective tracking, on the basis of the data trail of the person's movements, enabling reconstruction of a person's behaviour, purpose, intention and associates at previous times

Information arising at different times, and from different forms of surveillance, can be combined, in order to offer a more complete picture of a person's activities, and enable yet more inferences to be drawn, and suspicions generated. This is the primary sense in which the term 'überveillance' is applied: "Überveillance has to do with the fundamental who (ID), where (location), and when (time) questions in an attempt to derive why (motivation), what (result), and even how (method/plan/thought). Überveillance can be a predictive mechanism for a person's expected behaviour, traits, likes, or dislikes; or it can be based on historical fact; or it can be something in between ... Überveillance is more than closed circuit television feeds, or cross-agency databases linked to national identity cards, or biometrics and ePassports used for international travel. Überveillance is the sum total of all these types of surveillance and the deliberate integration of an individual's personal data for the continuous tracking and monitoring of identity and location in real time" (Michael & Michael 2010. See also Michael & Michael 2007, Michael et al. 2008, Michael et al. 2010, Clarke 2010).

A comprehensive model of surveillance includes consideration of geographical scope, and of temporal scope. Such a model assists the analyst in answering key questions about surveillance: of what? for whom? by whom? why? how? where? and when? (Clarke 2009c). Distinctions are also needed based on the extent to which the subject has knowledge of surveillance activities. It may be overt or covert. If covert, it may be merely unnotified, or alternatively express measures may be undertaken in order to obfuscate, and achieve secrecy. A further element is the notion of 'sousveillance', whereby the tools of surveillance are applied, by those who are commonly watched, against those who are commonly the watchers (Mann et al. 2003).

These notions are applied in the following sections in order to establish the extent to which location and tracking of mobile devices is changing the game of surveillance, and to demonstrate that location surveillance is intruding more deeply into personal freedoms than previous forms of surveillance.

4. Applications

This section presents a typology of applications of mobile device location, as a means of narrowing down to the kinds of uses that have particularly serious privacy implications. These are commonly referred to as location-based services (LBS). One category of applications provide information services that are for the benefit of the mobile device's user, such as navigation aids, and search and discovery tools for the locations variously of particular, identified organisations, and of organisations that sell particular goods and services. Users of LBS of these kinds can be reasonably assumed to be aware that they are disclosing their location. Depending on the design, the disclosures may also be limited to specific service-providers and specific purposes, and the transmissions may be secured.

Another, very different category of application is use by law enforcement agencies (LEAs). The US E-911 mandate of 1999 was nominally a public safety measure, to enable people needing emergency assistance to be quickly and efficiently located. In practice, the facility also delivered LEAs means for locating and tracking people of interest, through their mobile devices. Personal surveillance may be justified by reasonable grounds for suspicion that the subject is involved in serious crime, and may be specifically authorised by judicial warrant. Many countries have always been very loose in their control over LEAs, however, and many others have drastically weakened their controls since 2001. Hence, in any given jurisdiction and context, each and all of the controls may be lacking.

Yet worse, LEAs use mobile location and tracking for mass surveillance, without any specific grounds for suspicion about any of the many people caught up in what is essentially a dragnet-fishing operation (e.g. Mery 2009). Examples might include monitoring the area adjacent to a meeting-venue watching out for a blacklist of device-identifiers known to have been associated with activists in the past, or collecting device-identifiers for use on future occasions. In addition to netting the kinds of individuals who are of legitimate interest, the 'by-catch' inevitably includes threatened species. There are already extraordinarily wide-ranging (and to a considerable extent uncontrolled) data retention requirements in many countries.

Of further concern is the use of Automated Number Plate Recognition (ANPR) for mass surveillance purposes. This has been out of control in the UK since 2006, and has been proposed or attempted in various other countries as well (Clarke 2009a). Traffic surveillance is expressly used not only for retrospective analysis of the movements of individuals of interest to LEAs, but also as a means of generating suspicions about other people (Lewis 2008).

Beyond LEAs, many government agencies perform social control functions, and may be tempted to conduct location and tracking surveillance. Examples would include benefits-paying organisations tracking the movements of benefits-recipients about whom suspicions have arisen. It is not too far-fetched to anticipate zealous public servants concerned about fraud control imposing

location surveillance on all recipients of some particularly valuable benefit, or as a security precaution on every person visiting a sensitive area (e.g. a prison, a power plant, a national park).

Various forms of social control are also exercised by private sector organisations. Some of these organisations, such as placement services for the unemployed, may be performing outsourced public sector functions. Others, such as workers' compensation providers, may be seeking to control personal insurance claimants, and similarly car-hire companies and insurance providers may wish to monitor motor vehicles' distance driven and roads used (Economist 2012).

A further privacy-invasive practice that is already common is the acquisition of location and tracking data by marketing corporations, as a by-product of the provision of location-based services, but with the data then applied to further purposes other than that for which it was intended. Some uses rely on statistical analysis of large holdings ('data mining'). Many uses are, on the other hand, very specific to the individual, and are for such purposes as direct or indirect targeting of advertisements and the sale of goods and services. Some of these applications combine location data with data from other sources, such as consumer profiling agencies, in order to build up such a substantial digital persona that the individual's behaviour is readily influenced. This takes the activity into the realms of überveillance.

All such services raise serious privacy concerns, because the data is intensive and sensitive, and attractive to organisations. Companies may gain rights in relation to the data through market power, or by trickery – such as exploitation of a self-granted right to change the Terms of Service (Clarke 2011). Once captured, the data may be re-purposed by any organisation that gains access to it, because the value is high enough that they may judge the trivial penalties that generally apply to breaches of privacy laws to be well worth the risk.

A recently-emerged, privacy-invasive practice is the application of the mobile device signature (MDS) form of tracking, in such locations as supermarkets. This is claimed by its providers to offer deep observational insights into the behaviour of customers, including dwell-times in front of displays, possibly linked with the purchaser's behaviour. This raises concerns a little different from other categories of location and tracking technologies, and is accordingly considered in greater depth in the following section.

It is noteworthy that an early review identified a wide range of LBS, which the authors classified into mobile guides, transport, gaming, assistive technology and location-based health (Raper et al. 2007b). Yet that work completely failed to notice that a vast array of applications were emergent in surveillance, law enforcement and national security, despite the existence of relevant literature from at least 1999 onwards (Clarke 2001, Michael & Masters 2006).

5. Implications

The previous sections have introduced many examples of risks to citizens and consumers arising from location surveillance. This section presents an analysis of the categories and of the degree of seriousness with which they should be viewed. The first topic addressed is the privacy of personal location data. Other dimensions of privacy are then considered, and then the specific case of MDS is examined. The treatment here is complementary to earlier articles that have looked more generally at particular applications such as location-based mobile advertising, e.g. Cleff (2007, 2010) and King & Jessen (2010). See also Art. 29 (2011).

5.1 Locational Privacy

Knowing where someone has been, knowing what they are doing right now, and being able to predict where they might go next is a powerful tool for social control and for chilling behaviour (Abbas 2011). Humans do not move around in a random manner (Song et al. 2010).

One interpretation of 'locational 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" (Blumberg & Eckersley 2009). A more concise definition is "the ability to control the extent to which personal location information is ... [accessible and] used by others" (van Loenen et al. 2009). Hence 'tracking privacy' is the interest an individual has in controlling information about their sequence of locations.

Location surveillance is deeply intrusive into data privacy, because it is very rich, and enables a great many inferences to be drawn (Clarke 2001, Dobson & Fisher 2003, Michael et al. 2006a, Clarke & Wigan 2011). As demonstrated by Raper et al. (2007a, pp. 32-33), most of the technical literature that considers privacy is merely concerned about it as an impediment to deployment and adoption, and how to overcome the barrier rather than how to solve the problem. Few authors adopt a positive approach to privacy-protective location technologies. The same authors' review of applications (Raper et al. 2007b) includes a single mention of privacy, and that is in relation to just one of the scores of sub-categories of application that they catalogue.

Most service-providers are cavalier in their handling of personal data, and extravagant in their claims. For example, Skyhook claims that it "respects the privacy of all users, customers, employees and partners"; but, significantly, it makes no mention of the privacy of the people whose locations, through the locations of their Wifi routers, it collects and stores (Skyhook 2012).

Consent is critical in such LBS as personal location chronicle systems, people-followers and footpath route-tracker systems that systematically collect personal location information from a device they are carrying (Collier 2011c). The data handled by such applications is highly sensitive because it can be used to conduct behavioural profiling of individuals in particular settings. The sensitivity exists

even if the individuals remain 'nameless', i.e. if each identifier is a temporary or pseudo-identifier and is not linked to other records. Service-providers, and any other organisations that gain access to the data, achieve the capacity to make judgements on individuals based on their choices of, for example, which retail 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 reasonably made that they are in some way affiliated to that religion (Samuel 2008).

It is frequently asserted that individuals cannot have a reasonable expectation of privacy in a public space. Contrary to those assertions, however, privacy expectations always have existed in public places, and continue to exist (VLRC 2010). Tracking the movements of people as they go about their business is a breach of a fundamental expectation that people will 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 specific, prior approval in the form of a warrant. This principle has, however, been compromised in many countries since 2001. Warrantless tracking using a mobile device generally results in the evidence, which has been obtained without the proper authority, being inadmissible in a court of law (Samuel 2008). Some law enforcement agencies have argued for the abolition of the warrant process because the bureaucracy involved may mean that the suspect cannot be prosecuted for a crime they have likely committed (Ganz 2005). These issues are not new; but far from eliminating a warrant process, the appropriate response is to invest the energy in streamlining this process (Bronitt 2010).

Privacy risks arise not only from locational data of high integrity, but also from data that is or becomes associated with a person and that is inaccurate, misleading, or wrongly attributed to that individual. High levels of inaccuracy and unreliability were noted above in respect of all forms of location and tracking technologies. In the case of MDS services, claims have been made of one-to-two metre locational accuracy. This has yet to be supported by experimental test cases, however, and hence there is uncertainty about the reliability of inferences that the service-provider 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'.

5.2 Privacy More Broadly

Privacy has multiple dimensions. One analysis, in Clarke (2006a), identifies four distinct aspects. Privacy of Personal Data, variously also 'data privacy' and 'information privacy', is the most widely-discussed dimension of the four. Individuals claim that data about themselves should not be automatically available to other individuals and organisations, and that, even where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use. The last five decades have seen the

application of information technologies to a vast array of abuses of data privacy. The degree of privacy-intrusiveness is a function of both the intensity and the richness of the data. Where multiple sources are combined, the impact is particularly likely to chill behaviour. An example is the correlation of video-feeds with mobile device tracking. The previous sub-section addressed that dimension.

Privacy of the Person, or 'bodily privacy', extends from freedom from torture and right to medical treatment, via compulsory immunisation and imposed treatments, to compulsory provision of samples of body fluids and body tissue, and obligations to submit to biometric measurement. Locational surveillance gives rise to concerns about personal safety. Physical privacy is directly threatened where a person who wishes to inflict harm is able to infer the present or near-future location of their target. Dramatic examples include assassins, kidnappers, 'standover merchants' and extortionists. But even people who are neither celebrities nor notorities are subject to stalking and harassment (Fusco et al. 2012).

Privacy of Personal Communications is concerned with the need of individuals for freedom to communicate among themselves, without routine monitoring of their communications by other persons or organisations. Issues include 'mail covers', the use of directional microphones, 'bugs' and telephonic interception, with or without recording apparatus, and third-party access to email-messages. Locational surveillance thereby creates new threats to communications privacy. For example, the equivalent of 'call records' can be generated by combining the locations of two device-identifiers in order to infer that a face-to-face conversation occurred.

Privacy of Personal Behaviour encompasses 'media privacy', but particular concern arises in relation to sensitive matters such as sexual preferences and habits, political activities and religious practices. Some privacy analyses, particularly in Europe, extend this discussion to personal autonomy, liberty and the right of self-determination (e.g. King & Jesson 2010). The notion of 'private space' is vital to economic and social aspects of behaviour, is relevant in 'private places' such as the home and toilet cubicles, but is also relevant and important in 'public places', where systematic observation and the recording of images and sounds are far more intrusive than casual observation by the few people in the vicinity.

Locational surveillance gives rise to rich sets of data about individuals' activities. The knowledge, or even suspicion, that such surveillance is undertaken, chills their behaviour. The chilling factor is vital in the case of political behaviour (Clarke 2008). It is also of consequence in economic behaviour, because the inventors and innovators on whom new developments depend are commonly 'different-thinkers' and even 'deviants', who are liable to come to come to attention in mass surveillance dragnets, with the tendency to chill their behaviour, their interactions and their creativity.

Surveillance that generates accurate data is one form of threat. Surveillance that generates inaccurate data, or wrongly associates data with a particular person, is dangerous as well. Many inferences that arise from inaccurate data will be wrong, of course, but that won't prevent those inferences being drawn, resulting in unjustified behavioural privacy invasiveness, including unjustified association with people who are, perhaps for perfectly good reasons, themselves under suspicion.

In short, all dimensions of privacy are seriously affected by location surveillance. For deeper treatments of the topic, see Michael et al. (2006b) and Clarke & Wigan (2011).

5.3 Locational Privacy and MDS

The recent innovation of tracking by means of mobile device signatures (MDS) gives rise to some issues additional to, or different from, mainstream device-location technologies. This section accordingly considers this particular technique's implications in greater depth. Limited reliable information is currently available, and the analysis is of necessity based on supplier-published sources (PI 2010a, 2010b) and media reports (Collier 2010a, 2010b, 2010c).

A company called Path Intelligence (PI) markets an MDS service to shopping mall-owners, to enable them to 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 (PI 2010a). The company claims to detect each phone (and hence person) that enters a zone, and to capture data, including:

- how long each device and person stay, including dwell times in front of shop windows;
- repeat visits by shoppers in varying frequency durations; and
- typical route and circuit paths taken by shoppers as they go from shop to shop during a given shopping experience.

For malls, PI is able to denote such things as whether or not shoppers who shop at one establishment will also shop at another in the same mall, and whether or not people will go out of their way to visit a particular retail outlet independent of its location. For retailers, PI says it is able to provide information on conversion rates by department or even product line, and even which areas of the store might require more attention by staff during specific times of the day or week (PI 2012).

PI says that it uses "complex algorithms" to denote the geographic position of a mobile, using strategically located "proprietary equipment" in a campus setting (PI 2010a). The company states that it is conducting "data-driven analysis", but is not collecting, or at least that it is not disclosing, any personal information such as a name, mobile telephone number or contents of a short message service (SMS). It states that it only ever provides aggregated data at varying zone levels to the shopping mall-owners. This is presumably justified on the basis that,

using MDS techniques, direct identifiers are unlikely to be available, and a pseudo-identifier needs to be assigned. There is no explicit definition of what constitutes a zone. It is clear, however, that minimally-aggregated data at the highest geographic resolution is available for purchase, and at a higher price than more highly-aggregated data.

Shoppers have no relationship with the company, and it appears unlikely that they would even be aware that data about them is being collected and used. The only disclosure appears to be that "at each of our installations our equipment is clearly visible and labelled with our logo and website address" (PI 2010a), but this is unlikely to be visible to many people, and in any case would not inform anyone who saw it.

In short, the company is generating revenue by monitoring signals from the mobile devices of people who visit a shopping mall for the purchase of goods and services. The data collection is performed without the knowledge of the person concerned (Renegar et al. 2008). The company is covertly collecting personal data and exploiting it for profit. There is no incentive or value proposition for the individual whose mobile is being tracked. No clear statement is provided about collection, storage, retention, use and disclosure of the data (Arnold 2008). Even if privacy were not a human right, this would demand statutory intervention on the public policy grounds of commercial unfairness. The company asserts that the "our privacy approach has been reviewed by the [US Federal Trade Commission] FTC, which determined that they are comfortable with our practices" (PI 2010a). It makes no claims of such 'approval' anywhere else in the world.

The service could be extended beyond a mall and the individual stores within it, to, for example, associated walkways and parking areas, and surrounding areas such as government offices, entertainment zones and shopping-strips. Applications can also be readily envisaged on hospital and university campuses, and in airports and other transport hubs. From prior research, this is likely to expose the individual's place of employment, and even their residence (Michael et al. 2006). Even if only aggregated data is sold to businesses, the individual records remain available to at least the service-provider.

The scope exists to combine this form of locational surveillance with video-surveillance such as in-store CCTV, and indeed this is claimed to be already a feature of the company's offering to retail stores. To the extent that a commonly-used identifier can be established (e.g. through association with the person's payment or loyalty card at a point-of-sale), the full battery of local and externally-acquired customer transaction histories and consolidated 'public records' data can be linked to in-store behaviour (Michael & Michael 2007). Longstanding visual surveillance is intersecting with well-established data surveillance, and being augmented by locational surveillance, giving breath to dataveillance, or what is now being referred to by some as 'smart surveillance' (Wright et al. 2010, IBM 2011).

Surreptitious collection of personal data is (with exemptions and exceptions) largely against the law, even when undertaken by law enforcement personnel. The MDS mechanism also flies in the face of telephonic interception laws. 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 a service-provider have the right to do what a law enforcement agency cannot normally do?

6. Controls

The tenor of the discussion to date has been that location surveillance harbours enormous threats to location privacy, but also to personal safety, the freedom to communicate, freedom of movement, and freedom of behaviour. This section examines the extent to which protections exist, firstly in the form of natural or intrinsic controls, and secondly in the form of legal provisions. The existing safeguards are found to be seriously inadequate, and it is therefore necessary to also examine the prospects for major enhancements to law, in order to achieve essential protections.

6.1 Intrinsic Controls

A variety of forms of safeguard exist against harmful technologies and unreasonable applications of them. The intrinsic economic control has largely evaporated, partly because the tools use electronics and the components are produced in high volumes at low unit cost. Another reason is that the advertising and marketing sectors are highly sophisticated, already hold and exploit vast quantities of personal data, and are readily geared up to exploit yet more data.

Neither the oxymoronic notion of 'business ethics' nor the personal morality of executives in business and government act as any significant brake on the behaviours of corporations and governments, because they are very weak barriers, and they are readily rationalised away in the face of claims of enhanced efficiencies in, for example, marketing communications, fraud control, criminal justice and control over anti-social behaviour.

A further category of intrinsic control is 'self-regulatory' arrangements within relevant industry sectors. In 2010, for example, the Australian Mobile Telecommunications Association (AMTA) released industry guidelines to promote the privacy of people using LBS on mobile devices (AMTA 2010). The guidelines were as follows:

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
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

The second point is a matter for parliaments, privacy oversight agencies and law enforcement agencies, and its inclusion in industry guidelines is for-information-only. The remainder, meanwhile, are at best 'aspirational', and at worst mere window-dressing. Codes of this nature are simply ignored by industry members. They are primarily a means to hold off the imposition of actual regulatory measures. Occasional short-term constraints may arise from flurries of media attention, but the 'responsible' organisations escape by suggesting that bad behaviour was limited to a few 'cowboy' organisations or was a one-time error that won't be repeated.

A case study of the industry self-regulation is provided by the Biometrics Code issued by the misleadingly-named Australian industry-and-users association, the Biometrics 'Institute' (BI 2004). During the period 2009-12, the privacy advocacy organisation, the Australian Privacy Foundation (APF), submitted to the Privacy Commissioner on multiple occasions that the Code failed to meet the stipulated requirements and under the Commissioner's own Rules had to be de-registered. The Code never had more than five subscribers (out of a base of well over 100 members – which was itself only a sub-set of organisations active in the area), and had no signatories among the major biometrics vendors or users, because all five subscribers were small organisations or consultants. In addition, none of the subscribers appear to have ever provided a link to the Code on their websites or in their Privacy Policy Statements (APF 2012).

The Commissioner finally ended the farce in April 2012, citing the "low numbers of subscribers", but avoided its responsibilities by permitting the 'Institute' to "request" revocation, over two years after the APF had made the same request (OAIC 2012). The case represents an object lesson in the vacuousness of self-regulation and the business-friendliness of a captive privacy oversight agency.

If economics, morality and industry-sector politics are inadequate, perhaps competition and organisational self-interest might work. On the other hand, repeated proposals that privacy is a strategic factor for corporations and government agencies have fallen on stony ground (Clarke 1996, 2006b).

The public can endeavour to exercise countervailing power against privacy-invasive practices. On the other hand, individuals acting alone are of little or no consequence to organisations that are intent on the application of location surveillance. Moreover, consumer organisations lack funding, professionalism and reach, and only occasionally attract sufficient media attention to force any meaningful responses from organisations deploying surveillance technologies.

Individuals may have direct surveillance countermeasures available to them, but relatively few people have the combination of motivation, technical competence and persistence to overcome lethargy and the natural human desire to believe that the institutions surrounding them are benign. In addition, some government agencies, corporations and (increasingly prevalent) public-private partnerships seek to deny anonymity, pseudonymity and multiple identities, and to impose so-called 'real name' policies, for example as a solution to the imagined epidemics of cyber-bullying, hate speech and child pornography. Individuals who use cryptography and other obfuscation techniques have to overcome the endeavours of business and government to stigmatise them as criminals with 'something to hide'.

6.2 Legal Controls

It is clear that natural or intrinsic controls have been utter failures in privacy matters generally, and will be in locational privacy matters as well. That leaves legal safeguards for personal freedoms as the sole protection. There are enormous differences among domestic laws relating to location surveillance. This section accordingly limits itself to generalities and examples.

Privacy laws are (with some qualifications, mainly in Europe) very weak instruments. Even where public servants and parliaments have an actual intention to protect privacy, rather than merely to overcome public concerns by passing placebo statutes, the draft Bills are countered by strong lobbying by government agencies and industry, to the extent that measures that were originally portrayed as being privacy-protective reach the statute books as authority for privacy breaches and surveillance (Clarke 2000).

Privacy laws, once passed, are continually eroded by exceptions built into subsequent legislation, and by technological capabilities that were not contemplated when the laws were passed. In most countries, location privacy has yet to be specifically addressed in legislation. Even where it is encompassed by human rights and privacy laws, the coverage is generally imprecise and ambiguous. More direct and specific regulation may exist, however. In Australia, for example, the Telecommunications (Interception and Access) Act and the Surveillance Devices Act define and criminalise inappropriate interception and access, use, communication and publication of location information that is obtained from mobile device traffic (AG 2005). On the other hand, when Google Inc. intercepted wi-fi signals and recorded the data that they contained, the Privacy Commissioner absolved the company (Riley 2010), and the Australian Federal Police refused to prosecute despite the action – whether it was intentional, 'inadvertent' or merely plausibly deniable – being a clear breach of the criminal law (Moses 2010).

The European Union determined a decade ago that location data that is identifiable to individuals is to some extent at least subject to existing data protection laws (EU 2002). However, the wording of that so-called 'e-Privacy Directive' countenances the collection of "location data which are more precise

than is necessary for the transmission of communications", without clear controls over the justification, proportionality and transparency of that collection (para. 35). In addition, the e-Privacy Directive only applies to telecommunications service providers, not to other organisations that acquire location and tracking data. King & Jessen (2010) discuss various gaps in the protective regimes in Europe.

The EU's Advisory Body (essentially a Committee of European Data Protection Commissioners) has issued an Opinion that mobile location data is generally capable of being associated with a person, and hence is personal data, and hence is subject to the EU Directive of 1995 and national laws that implement that Directive (Art. 29 2011). Consent is considered to be generally necessary, and that consent must be informed, and sufficiently granular (pp. 13-18).

It is unclear, however, to what extent this Opinion has actually caused, and will in the future cause, organisations that collect, store, use and disclose location data to change their practices. This uncertainty exists in respect of national security, law enforcement and social control agencies, which have, or which can arrange, legal authority that overrides data protection laws. It also applies to non-government organisations of all kinds, which can take advantage of exceptions, exemptions, loopholes, non-obviousness, obfuscation, unenforceability within each particular jurisdiction, and extra-jurisdictionality, to operate in ways that are in apparent breach of the Opinion.

Legal authorities for privacy-invasions are in a great many cases vague rather than precise, and in many jurisdictions power in relation to specific decisions is delegated to an LEA (in such forms as self-written 'warrants'), or even a social control agency (in the form of demand-powers), rather than requiring a decision by a judicial officer based on evidence provided by the applicant.

Citizens in many countries are subject to more or less legitimate surveillance of various degrees and orders of granularity, by their government, in the name of law enforcement and national security. However, many Parliaments have granted powers to national security agencies to use location technology to track citizens and to intercept telecommunications. Moreover, many Parliaments have failed the public by permitting a warrant to be signed by a Minister, or even a public servant, rather than a judicial officer (Jay 1999). Worse still, it appears that these already-gross breaches of the principle of a free society are in effect being 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 (Collier 2011a).

Data protection legislation in all countries evidences massive weaknesses. There are manifold exemptions and exceptions, and there are intentional and accidental exclusions, for example through limitations in the definitions of 'identified' and 'personal data'. Even the much-vaunted European laws fail to cope with extra-territoriality and are largely ignored by US-based service-providers. They are also focussed exclusively on data, leaving large gaps in safeguards for physical, communications and behavioural privacy.

Meanwhile, a vast amount of abuse of personal data is achieved through the freedom of corporations and government agencies to pretend that Terms imposed on consumers and citizens without the scope to reject them are somehow the subject of informed and freely-given consent. For example, petrol-stations, supermarkets and many government agencies pretend that walking past signs saying 'area subject to CCTV' represents consent to gather, transmit, record, store, use and disclose data. The same approach is being adopted in relation to highly-sensitive location data, and much-vaunted data protection laws are simply subverted by the mirage of consent.

At least notices such as 'you are now being watched' or 'smile, you are being recorded' inform customers that they are under observation. On the other hand, people are generally oblivious to the fact that their mobile subscriber identity is transmitted from their mobile phone and multilaterated to yield a reasonably precise location in a shopping mall (Collier 2011a, b, c). Further, there is no meaningful sense in which they can be claimed to have consented to providing location data to a third party, in this case a location service-provider with whom they have never had contact. And the emergent combination of MDS with CCTV sources becomes a pervasive view of the person, an 'über' view, providing a set of über-analytics to – at this stage – shopping complex owners and their constituents.

What rights do employees have if such a system were instituted in an employment setting? Are workplace surveillance laws in place that would protect employees from constant monitoring? A similar problem applies to people at airports, or on hospital, university, industrial or government campuses. No social contract has been entered into between the parties, rendering the subscriber powerless.

Since the collapse of the Technology Assessment movement, technological deployment proceeds unimpeded, and public risks are addressed only after they have emerged and the clamour of concern has risen to a crescendo. A reactive force is at play, rather than proactive measures being taken to ensure avoidance or mitigation of potential privacy breaches. In Australia, for example, safeguards for location surveillance exist at best incidentally, in provisions under separate legislative regimes and in separate jurisdictions, and at worst not at all. No overarching framework exists to provide consistency among the laws. This causes confusion and inevitably results in inadequate protections (ALRC 2008).

6.3 Prospective Legal Controls

Various learned studies have been conducted, but gather dust. In Australia, the three major law reform commissions have all reported, and all have been ignored by the legislatures (NSWLRC 2005, ALRC 2008, VLRC 2010).

One critical need is for the fundamental principle to be recovered, to the effect that the handling of personal data requires either consent or legal authority. Consent is meaningless as a control over unreasonable behaviour, however, unless it satisfies a number of key conditions. It must be informed, it must be

freely-given, and it must be sufficiently granular, not bundled (Clarke 2002). In a great many of the circumstances in which organisations are claiming to have consent to gather, store, use and disclose location data, the consumer does not appreciate what the scope of handling is that the service-provider is authorising themselves to perform; the Terms are imposed by the service-provider and may even be varied or completely re-written without consultation, a period of notice or even any notice at all; and consent is bundled rather than the individual being able to construct a pattern of consents and denials that suit their personal needs. Discussions all too frequently focus on the specifically-US notion of 'opt-out' (or 'presumed consent'), with consent debased to 'opt-in', and deprecated as inefficient and business-unfriendly.

Recently, some very weak proposals have been put forward, primarily in the USA. In 2011, for example, two US Senators proposed a Location Privacy Protection Bill (Cheng 2011). An organisation that collected location data from mobile or wireless data devices would have to state explicitly in their privacy policies what was being collected, in plain English. This would represent only a partial implementation of the already very weak 2006 recommendation of the Internet Engineering Task Force for Geographic Location/Privacy (IETF GEOPRIV) working group, which decided that technical systems should include 'Fair Information Practices' (FIPs) to defend against harms associated with the use of location technologies (EPIC 2006). FIPs, however, is itself only a highly cut-down version of effective privacy protections, and the Bill proposes only a small fraction of FIPs. It would be close to worthless to consumers, and close to legislative authorisation for highly privacy-invasive actions by organisations.

Two other US senators tabled a GPS Bill, nominally intended to "balance the needs of Americans' privacy protections with the legitimate needs of law enforcement, and maintains emergency exceptions" (Anderson 2011). The scope is very narrow – next would have to come the Wi-Fi Act, the A-GPS Act, etc. That approach is obviously unviable in the longer term as new innovations emerge. Effective legislation must have appropriate generality rather than excessive technology-specificity, and should be based on semantics not syntax. Yet worse, these Bills would provide 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.

7. Conclusions

Mobile device location technologies and their applications are enabling surveillance, and producing an enormous leap in intrusions into data privacy and into privacy of the person, privacy of personal communications, and privacy of personal behaviour.

Existing privacy laws are entirely incapable of protecting consumers and citizens against the onslaught. Even where consent is claimed, it generally fails the tests of being informed, freely-given and granular.

There is an urgent need for outcries from oversight agencies, and responses from legislatures. Individual countries can provide some degree of protection, but the extra-territorial nature of so much of the private sector, and the use of corporate havens, in particular the USA, mean that multilateral action is essential in order to overcome the excesses arising from the US *laissez faire* traditions.

One approach to the problem would be location privacy protection legislation, although it would need to embody the complete suite of protections rather than the mere notification that the technology breaches privacy. An alternative approach is amendment of the current privacy legislation and other anti-terrorism legislation in order to create appropriate regulatory provisions, and close the gaps that LBS providers are exploiting (Koppel 2010).

The chimeras of self-regulation, and the unenforceability of guidelines, are not safeguards. Sensitive data like location information must be subject to actual, enforced protections, with guidelines and codes no longer used as a substitute, but merely playing a supporting role. Unless substantial protections for personal location information are enacted and enforced, there will be an epidemic of unjustified, disproportionate and covert surveillance, conducted by government and business, and even by citizens (Gillespie 2009, Abbas et al. 2011).

References

Abbas R. (2011) 'The social and behavioural implications of location-based services: An observational study of users' *Journal of Location Based Services*, 5, 3-4 (December 2011)

Abbas R., Michael K., Michael m.g. & Aloudat A. (2011) 'Emerging forms of covert surveillance using GPS-enabled devices', *Journal of Cases on Information Technology*, 13, 2 (2011) 19-33

AG (2005) 'What the Government is doing: Surveillance Device Act 2004', 25 May 2005, Australian Government, at <http://www.ag.gov.au/agd/www/nationalsecurity.nsf/AllDocs/9B1F97B59105AEE6CA25700C0014CAF5?OpenDocument>

ALRC (2008) '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>

AMTA (2010) 'New mobile telecommunications industry guidelines and consumer tips set benchmark for Location Based Services', Australian Mobile Telecommunications Association, 2010, at

<http://www.amta.org.au/articles/New.mobile.telecommunications.industry.guidelines.and.consumer.tips.set.benchmark.for.Location.Based.Services>

Anderson N. (2011) 'Bipartisan bill would end government's warrantless GPS tracking', *Ars Technica*, June 2011, at <http://arstechnica.com/tech-policy/news/2011/06/bipartisan-bill-would-end-governments-warrantless-gps-tracking.ars>

APF (2012) 'Revocation of the Biometrics Industry Code' Australian Privacy Foundation, March 2012, at <http://www.privacy.org.au/Papers/OAIC-BiomCodeRevoc-120321.pdf>

Arnold B. (2008) 'Privacy guide', Caslon Analytics, May 2008, at <http://www.caslon.com.au/privacyguide19.htm>

Art. 29 (2011) 'Opinion 13/2011 on Geolocation services on smart mobile devices' Article 29 Data Protection Working Party , 881/11/EN WP 185, 16 May 2011, at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf

BI (2004) 'Privacy Code' Biometrics Institute, Sydney, April 2004, at <http://web.archive.org/web/20050424120627/http://www.biometricsinstitute.org/displaycommon.cfm?an=1&subarticlenbr=8>

Blumberg A.J. & Eckersley P. (2009) 'On locational privacy, and how to avoid losing it forever' Electronic Frontier Foundation, August 2009, at <https://www.eff.org/wp/locational-privacy>

Bronitt S. (2010) 'Regulating covert policing methods: from reactive to proactive models of admissibility', in S. Bronitt, C. Harfield and K. Michael (eds.), *The Social Implications of Covert Policing*, 2010, pp. 9-14

Cheng J. (2011) 'Franken's location-privacy bill would close mobile-tracking 'loopholes'', *Wired*, 17 June 2011, at <http://www.wired.com/epicenter/2011/06/franken-location-loopholes/>

Chetty K., Smith G.E. & Woodbridge K. (2012) 'Through-the-Wall Sensing of Personnel Using Passive Bistatic WiFi Radar at Standoff Distances' *IEEE Transactions on Geoscience and Remote Sensing* 50, 4 (April 2012) 1218 - 1226

Clarke R. (1988) 'Information technology and dataveillance', *Communications of the ACM*, 31(5), May 1988, pp498-512, at <http://www.rogerclarke.com/DV/CACM88.html>

Clarke R. (1994) 'The Digital Persona and its Application to Data Surveillance' *The Information Society* 10,2 (June 1994) 77-92, at <http://www.rogerclarke.com/DV/DigPersona.html>

Clarke R. (1996) 'Privacy and Dataveillance, and Organisational Strategy' *Proc. I.S. Audit & Control Association (EDPAC'96)*, Perth, Western Australia, May 1996, at <http://www.rogerclarke.com/DV/PStrat.html>

- Clarke R. (2000) 'Submission to the Commonwealth Attorney-General re: 'A privacy scheme for the private sector: Release of Key Provisions' of 14 December 1999' Xamax Consultancy Pty Ltd, January 2000, at <http://www.anu.edu.au/people/Roger.Clarke/DV/PAPSSub0001.html>
- Clarke R. (2001) 'Person-Location and Person-Tracking: Technologies, Risks and Policy Implications' *Information Technology & People* 14, 2 (Summer 2001) 206-231, at <http://www.rogerclarke.com/DV/PLT.html>
- Clarke R. (2002) 'e-Consent: A Critical Element of Trust in e-Business' Proc. 15th Bled Electronic Commerce Conference, Bled, Slovenia, June 2002, at <http://www.rogerclarke.com/EC/eConsent.html>
- Clarke R. (2006a) 'What's 'Privacy'? ' Xamax Consultancy Pty Ltd, August 2006, at <http://www.rogerclarke.com/DV/Privacy.html>
- Clarke R. (2006b) 'Make Privacy a Strategic Factor - The Why and the How' *Cutter IT Journal* 19, 11 (October 2006), at <http://www.rogerclarke.com/DV/APBD-0609.html>
- Clarke R. (2008) 'Dissidentity: The Political Dimension of Identity and Privacy' *Identity in the Information Society* 1, 1 (December, 2008) 221-228, at <http://www.rogerclarke.com/DV/Dissidentity.html>
- Clarke R. (2009a) 'The Covert Implementation of Mass Vehicle Surveillance in Australia' Proc 4th Workshop on the Social Implications of National Security: Covert Policing, April 2009, ANU, Canberra, at <http://www.rogerclarke.com/DV/ANPR-Surv.html>
- Clarke R. (2009b) 'A Sufficiently Rich Model of (Id)entity, Authentication and Authorisation' Proc. IDIS 2009 - The 2nd Multidisciplinary Workshop on Identity in the Information Society, LSE, 5 June 2009, at <http://www.rogerclarke.com/ID/IdModel-090605.html>
- Clarke R. (2009c) 'A Framework for Surveillance Analysis' Xamax Consultancy Pty Ltd, August 2009, at <http://www.rogerclarke.com/DV/FSA.html>
- Clarke R. (2010) 'What is Überveillance? (And What Should Be Done About It?)' *IEEE Technology and Society* 29, 2 (Summer 2010) 17-25, at <http://www.rogerclarke.com/DV/RNSA07.html>
- Clarke R. (2011) 'The Cloudy Future of Consumer Computing' Proc. 24th Bled eConference, June 2011, at <http://www.rogerclarke.com/EC/CCC.html>
- Clarke R. & Wigan M. (2011) 'You are where you've been: The privacy implications of location and tracking technologies' *Journal of Location Based Services* 5, 3-4 (December 2011) 138-155, PrePrint at <http://www.rogerclarke.com/DV/YAWYB-CWP.html>
- Cleff E.B. (2007) 'Implementing the legal criteria of meaningful consent in the concept of mobile advertising' *Computer Law & Security Review* 23,2 (2007) 262-269

- Cleff E.B. (2010) 'Effective approaches to regulate mobile advertising: Moving towards a coordinated legal, self-regulatory and technical response' *Computer Law & Security Review* 26, 2 (2010) 158-169
- Collier K. (2011a) 'Stores spy on shoppers', *Herald Sun*, 12 October 2011, at <http://www.heraldsun.com.au/news/more-news/stores-spy-on-shoppers/story-fn7x8me2-1226164244739>
- Collier K. (2011b) 'Shopping centres' Big Brother plan to track customers', *Herald Sun*, 14 October 2011, at <http://www.heraldsun.com.au/news/more-news/shopping-centres-big-brother-plan-to-track-customers/story-fn7x8me2-1226166191503>
- Collier K. (2011c) 'Creepy' Path Intelligence retail technology tracks shoppers', *news.com.au*, 14 October 2011, at <http://www.news.com.au/money/creepy-retail-technology-tracks-shoppers/story-e6frfmc1-1226166413071>
- Dahunsi F. & Dwolatzky B. (2012) 'An empirical investigation of the accuracy of location-based services in South Africa' *Journal of Location Based Services* 6, 1 (March 2012) 22-34
- Dobson J. & Fisher P. (2003) 'Geoslavery' *IEEE Technology and Society* 22 (2003) 47-52, cited in Raper et al. (2007)
- Economist* (2012) 'Vehicle data recorders - Watching your driving' *The Economist* 23 June 2012, at <http://www.economist.com/node/21557309>
- EPIC (2006) 'Privacy and human rights report 2006' *Electronic Privacy Information Center, WorldLII*, 2006, at <http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Location.html>
- EPIC (2012) 'Investigations of Google Street View' *Electronic Privacy Information Center*, 2012, at <http://epic.org/privacy/streetview/>
- EU (2002) 'Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)' *Official Journal L 201* , 31/07/2002 P. 0037 - 0047, *European Commission*, at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML>
- Figueiras J. & Frattasi S. (2010) 'Mobile Positioning and Tracking: From Conventional to Cooperative Techniques' *Wiley*, 2010
- Fusco S.J., Abbas R., Michael K. & Aloudat A. (2012) 'Location-Based Social Networking and its Impact on Trust in Relationships' *IEEE Technology and Society Magazine* 31,2 (Summer 2012) 39-50, at <http://works.bepress.com/cgi/viewcontent.cgi?article=1326&context=kmichael>
- Gallagher T. et al. (2009) 'Trials of commercial Wi-Fi positioning systems for indoor and urban canyons' *Proc. IGSS Symposium*, 1-3 December 2009, Queensland, cited in Zandbergen (2012)

- Ganz J.S. (2005) '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) 1325-37
- Gillespie A.A. (2009) 'Covert surveillance, human rights and the law', *Irish Criminal Law Journal*, 19, 3 (August 2009) 71-79
- IBM (2011) 'IBM Smart Surveillance System (Previous PeopleVision Project)', IBM Research, 30 October 2011, at <http://www.research.ibm.com/peoplevision/>
- Jay D.M. (1999) 'Use of covert surveillance obtained by search warrant', *Australian Law Journal*, 73, 1 (Jan 1999) 34-36
- King N.J. & Jessen P.W. (2010) 'Profiling the mobile customer – Privacy concerns when behavioural advertisers target mobile phones' *Computer Law & Security Review* 26, 5 (2010) 455-478 and 26, 6 (2010) 595-612
- Koppel A. (2010) '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) 1061-1089
- Lewis P. (2008) 'Fears over privacy as police expand surveillance project' *The Guardian*, 15 September 2008, at <http://www.guardian.co.uk/uk/2008/sep/15/civilliberties.police>
- McGuire M., Plataniotis K.N. & Venetsanopoulos A.N. (2005) 'Data fusion of power and time measurements for mobile terminal location' *IEEE Transaction on Mobile Computing* 4 (2005) 142–153, cited in Raper et al. (2007)
- Mann S., Nolan J. & Wellman B. (2003) 'Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments' *Surveillance & Society* 1, 3 (June 2003) 331-355, at [http://www.surveillance-and-society.org/articles1\(3\)/sousveillance.pdf](http://www.surveillance-and-society.org/articles1(3)/sousveillance.pdf)
- Mautz R. (2011) 'Overview of Indoor Positioning Technologies' Keynote, Proc. IPIN'2011, Guimaraes, September 2011, at http://www.geometh.ethz.ch/people/.../IPIN_Keynote_Mautz_2011.pdf
- Mery D. (2009) 'The mobile phone as self-inflicted surveillance – And if you don't have one, what have you got to hide?' *The Register*, 10 April 2009, at http://www.theregister.co.uk/2009/04/10/mobile_phone_tracking/
- Michael K. & Michael M.G. (2007) 'From Dataveillance to Überveillance and the Realpolitik of the Transparent Society' University of Wollongong, 2007, at <http://works.bepress.com/kmichael/51>
- Michael K. & Michael M.G. (2009) 'Innovative Automatic Identification and Location-Based Services: From Bar Codes to Chip Implants' IGI Global, 2009
- Michael M.G. & Michael K. (2010) 'Towards a state of uberveillance' *IEEE Technology and Society Magazine* 29, 2 (Summer 2010) 9-16, at <http://works.bepress.com/kmichael/187>

- Michael K., McNamee A., Michael M.G. & Tootell H. (2006a) 'Location-Based Intelligence – Modeling Behavior in Humans using GPS' Proc. Int'l Symposium on Technology and Society, New York, 8-11 June 2006, at <http://ro.uow.edu.au/cgi/viewcontent.cgi?article=1384&context=infopapers>
- Michael K., McNamee A. & Michael M.G. (2006b) 'The Emerging Ethics of Humancentric GPS Tracking and Monitoring' Proc. Int'l Conf. on Mobile Business, Copenhagen, Denmark IEEE Computer Society, 2006, at <http://ro.uow.edu.au/cgi/viewcontent.cgi?article=1384&context=infopapers>
- Michael M.G., Fusco S.J. & Michael K (2008) 'A Research Note on Ethics in the Emerging Age of Überveillance (Überveillance)' Computer Communications, 31(6), 2008, 1192-119, at <http://works.bepress.com/kmichael/32/>
- Michael K. & Masters A. (2006) 'Realized Applications of Positioning Technologies in Defense Intelligence' in Hussein Abbass H. & Essam D. (eds.) 'Applications of Information Systems to Homeland Security and Defense' Idea Group Publishing, 2006, at <http://works.bepress.com/kmichael/2>
- Michael K., Roussos G., Huang G.Q., Gadh R., Chattopadhyay A., Prabhu S. & Chu P. (2010) 'Planetary-scale RFID services in an age of uberveillance' Proceedings of the IEEE 98, 9 (2010) 1663-1671
- Moses A. (2010) '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>
- NSWLRC (2005) 'Surveillance' Report 108 , NSW Law Reform Commission, 2005, at http://www.lawlink.nsw.gov.au/lawlink/lrc/ll_lrc.nsf/pages/LRC_r108toc
- OAIC (2012) " Office of the Australian Information Commissioner, April 2012, at <http://www.comlaw.gov.au/Details/F2012L00869/Explanatory%20Statement/Text>
- Otterberg A.A. (2005) '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) 661-704
- Parenti C. (2003) 'The Soft Cage: Surveillance in America From Slavery to the War on Terror' Basic Books, 2003
- PI (2010a) 'Our Commitment to Privacy', Path Intelligence, 2010, heading changed in late 2012 to 'Privacy by design', at <http://www.pathintelligence.com/en/products/footpath/privacy>
- PI (2010b) 'FootPath Technology', Path Intelligence, 2010, at <http://www.pathintelligence.com/en/products/footpath/footpath-technology>
- PI (2012) 'Retail' Path Intelligence, 2012, at <http://www.pathintelligence.com/en/industries/retail>

Raper J., Gartner G., Karimi H. & Rizos C. (2007a) 'A critical evaluation of location based services and their potential' *Journal of Location Based Services* 1, 1 (March 2007) 5-45

Raper J., Gartner G., Karimi H. & Rizos C. (2007b) 'Applications of location-based services: a selected review' *Journal of Location Based Services* 1, 2 (June 2007) 89-111

RE (2010a) 'IEEE 802.11 standards tutorial' Radio-Electronics.com, apparently of 2010, at <http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11-standards-tutorial.php>

RE (2010b) 'WiMAX IEEE 802.16 technology tutorial' Radio-Electronics.com, apparently of 2010, at <http://www.radio-electronics.com/info/wireless/wimax/wimax.php>

RE (2012) 'Assisted GPS, A-GPS' Radio-Electronics.com, apparently of 2012, at http://www.radio-electronics.com/info/cellulartelecomms/location_services/assisted_gps.php

Renegar B.D., Michael K. & Michael M.G. (2008) 'Privacy, value and control issues in four mobile business applications' *Proc. 7th Int'l Conf. on Mobile Business*, 2008, pp. 30-40

Riley J. (2010) 'Gov't 'travesty' in Google privacy case', *ITWire*, Wednesday 3 November 2010, 20:44, at <http://www.itwire.com/it-policy-news/regulation/42898-govt-travesty-in-google-privacy-case>

Samuel I.J. (2008) 'Warrantless location tracking', *New York University Law Review*, 83 (2008) 1324-1352

SHW (2012) 'Skyhook Location Performance', at <http://www.skyhookwireless.com/location-technology/performance.php>

Skyhook (2012) Website Entries, including 'Frequently Asked Questions' at <http://www.skyhookwireless.com/whoweare/faq.php>, 'Privacy Policy' at <http://www.skyhookwireless.com/whoweare/privacypolicy.php> and 'Location Privacy' at <http://www.skyhookwireless.com/whoweare/privacy.php>,

Song C., Qu Z., Blumm N. & Barabási A.-L. (2010) 'Limits of predictability in human mobility' *Science* 327, 5968 (2010) 1018-1021

USGov (2012) 'GPS Accuracy' National Coordination Office for Space-Based Positioning, Navigation, and Timing, February 2012, at <http://www.gps.gov/systems/gps/performance/accuracy/>

van Loenen B., Zevenbergen J. & de Jong J. (2009) 'Balancing Location Privacy with National Security: A Comparative Analysis of Three Countries through the Balancing Framework of the European Court Of Human Rights' Ch. 2 of Patten N.J. et al. 'National Security: Institutional Approaches', Nova Science Publishers, 2009

VLRC (2010) 'Surveillance in Public Spaces' Victorian Law Reform Commission, Final Report 18, March 2010, at http://www.lawreform.vic.gov.au/wps/wcm/connect/justlib/Law+Reform/resources/3/6/36418680438a4b4eacc0fd34222e6833/Surveillance_final_report.pdf

Wright D., Friedewald M., Gutwirth S., Langheinrich M., Mordini E., Bellanova R., De Hert P., Wadhwa K. & Bigo D. (2010) 'Sorting out smart surveillance' *Computer Law & Security Review* 26, 4 (2010) 343-354

Zandbergen P.A. (2012) 'Comparison of WiFi positioning on two mobile devices' *Journal of Location Based Services* 6, 1 (March 2012) 35-50

Acknowledgements

A preliminary version of the analysis presented in this paper appeared in the November 2011 edition of *Precedent*, the journal of the Lawyers Alliance. The article has been significantly upgraded as a result of comments provided by the referees and editor.

Author Affiliations

Katina Michael is an Associate Professor in the School of Information Systems and Technology at the University of Wollongong. She is the editor in chief of the *IEEE Technology and Society Magazine*, is on the editorial board of *Computers & Security*, and is a co-editor of 'Social Implications of Covert Policing' (2010). She is a Board member of the Australian Privacy Foundation and a representative of the Consumer Federation of Australia.

Roger Clarke is Principal of Xamax Consultancy Pty Ltd, Canberra. He is also a Visiting Professor in the Cyberspace Law & Policy Centre at the University of N.S.W., and a Visiting Professor in the Research School of Computer Science at the Australian National University. He is currently Chair of the Australian Privacy Foundation, and an Advisory Board member of Privacy International.
