Invasive Technology & Privacy Implications

Rebecca Sharman discusses the boundary of recent amendments to privacy laws when applied to new technologies.

The Privacy Act 1988 (Cth) ("**Act**") regulates the collection and use of personal information. This is defined to include any information about an individual whose identity is apparent, or can reasonably be ascertained from the information. This article examines the concept of the "location" of a mobile phone user as personal information, the technology available for tracking mobile phone users and the benefits and risks involved with the use of this technology.

"LOCATION" AS PERSONAL INFORMATION?

Due to recent technological developments it is now possible to track the location of mobile phone users with reasonable accuracy. It is arguable that the location of a mobile phone user (whether past or present), when coupled with their name, falls within the definition of 'personal information' in the Act. Even if an organisation simply records and stores 'location' data without identifying the individual, it may still be possible for someone with the aid of other material, to identify the individual.

Given that under the Act personal information need not need to be in a material form or accurate or even correct, a rough calculation of a persons' whereabouts may amount to personal information.

If the concept of "location" as personal information is accepted, then organisations collecting and/or using this information will be subject to the requirements of the Act and either the National Privacy Principles ("**NPPs**") or the Information Privacy Principles ("**IPPs**"). This will be discussed further below.

TRACKING TECHNOLOGY

There are four types of tracking technology used to determine the location of a mobile phone telephone user. Firstly, the location of a mobile phone user may be determined by analysing the geographical position of the base station with which the mobile phone at that particular point of time is communicating. This method is universally available, however as it is dependant on the calculation of the distance between base stations; its accuracy ranging from 300m – 5km.

The second method is commonly known as 'triangulation'. At any one time, mobile phones send a signal, containing the phone's unique digital identity number known as "IMSI", to the surrounding network antennas. By comparing the strength of the signals and the time of arrival, mobile phone companies can triangulate the position of the user. These signals are sent regardless of whether the phone is switched on or whether the user is making or receiving a call. Using software, it is possible to generate the triangulation calculation automatically.

A more accurate method involves embedding a Global Positioning System (GPS) receiver into the mobile phone. The GPS receiver transmits location information to orbiting satellites. The GPS calculation enables the tracker to pin point the mobile phone user to within 10 metres.

The newest tracking technology is 3G broadwidth technology. It is alleged that this technology will enable mobile phone users to be tracked to the nearest metre.

WHO USES TRACKING TECHNOLOGY?

It is now the case that if you carry a mobile phone you can be tracked. Knowing this, the next question to ask is, who is analysing this data?

(a) Mobile Phone Companies

It is well known that mobile phone companies record, in real time, the signals transmitted by mobile phones to base stations. However, it is not known whether mobile phone companies link these signals in real time with the owner of the mobile phone. Mobile phone companies do make this link at a later stage for the purposes of billing.

While it may be necessary for mobile phone networks to know your location in order to communicate with your phone, the concern is that this information may be used for other purposes, or that someone may obtain unauthorised access to this information.

(b) Government

In June Senator Natasha Stott Despoja, then leader of the Australian Democrats raised concerns about the powers of the Government to access phone records under the *Telecommunications Interception Act*. There is a loophole in the Act that enables authorities to access phone records held by mobile phone companies, in particular the location of callers, without a warrant. In the past 12 months it is estimated that 750,000 disclosures of phone details were obtained by officials without a warrant. Stott Despoja states "no warrants, no privacy, no accountability". This denigration of individual privacy seems unnecessary. If access to records held by mobile phone companies is required for law enforcement purposes, then the authorities would be able to obtain a warrant.

The issue of accessing mobile phone user information by authorities is not new. In 1997, there was an outcry by privacy and civil liberty groups upon the revelation that NSW police where monitoring mobile phone users without their consent or knowledge. With the help of mobile phone companies, the police were tracking criminal suspects through the triangulation signals sent to the nearest base station. Police protocol required officers to obtain written approval from their superiors and a court warrant before tracking the position of individuals. Although a useful investigative tool, this activity is open to abuse and raises serious questions of breach of privacy laws.

BENEFITS

Tracking technology does have utility for society and the user. One of the primary arguments in favour of the use of tracking technology is that it enables people to feel safe. There is some comfort to be derived from the knowledge that someone can locate you if the need arises. Undoubtedly, tracking technology is an enormous benefit to rescue workers and law enforcement officials. Mobile phone users can be located even if the individual is unsure or incapable of stating their whereabouts. This advantage was evident in the aftermath of the September 11, 2001 terrorist attacks on the World Trade Centre where rescue workers used mobile phone triangulation in the search for survivors. In Australia, Emergency Services often use triangulation as a tool to track injured and lost bushwalkers.

The United States Federal Communications Commission ("USFCC") have recognised the safety benefits of tracking technology. Late last year the USFCC ordered mobile-phone companies to incorporate tracking technology into mobile phones so as to enable law enforcement agents and emergency services to track the location of 911-mobile phone calls. By 2005, 95% of all mobile phones must have the 911-tracking technology installed.

However, the effectiveness of tracking technology in locating an injured or missing person is limited by its reliance on there being base stations/network antenna in close proximity to the person. Where there are long distances between base stations, such as in the Australian bush, it is near impossible to track the location of the person with any precision.

RISKS

(a) Loss of Privacy

'Privacy' and its counterpart 'surveillance' are key sociological issues. To an extent, enjoying a right to 'privacy' is fundamental to living in a free, democratic environment. The safety that comes in enabling people to find you when you are lost or hurt, means that people can also find you when you don't want to be found. It is possible that someone with criminal intent, such as a stalker could use tracking technology to locate their victim. Personal, but innocent activities such as attending mass on the weekend, or visiting someone in hospital may also be revealed. Similarly, the location of people who are on confidential government or corporate business may be disclosed with significant consequences. One must wonder whether the fundamental loss of privacy arising from this technology may be too high a price to pay.

(b) Corporate Marketing Power

The marketable nature of the information gathered by tracking technology, poses great risks to our privacy. When collated, this data will disclose such things as where we shop and at what time. Even on 'stand-buy' our mobile phones relay our location to mobile phone towers. This is vital information for businesses. Marketing can be directly tailored to individuals and advertisements sent to mobile phones when the user is in the general vicinity of the organisation. Once permitted, it would only be a matter of time before every business used tracking technology as part of their marketing campaign.

The combination of tracking technology and caller ID may impact on the quality and fairness of phone sales and consumer enquiry numbers. It has been revealed that in the US, some corporations use caller ID to prioritise callers according to the suburb they are calling from. This enables the corporation to speak to prima facie wealthy customers first, thus maximising sales. Not only may this conduct amount to a breach of privacy laws, but it is a form of discrimination.

In defence of corporations, it is argued that consumer data derived from information about the location of mobile phone users would help to ensure that customer demands and capacity are met. However, one must ask whom the collection of such personal information and consequently the denegation of privacy really benefits.

PRIVACY IMPLICATIONS

Given that this information, when coupled with the users name, may be considered 'personal information' organisations handling this information must comply with the Act and the NPPs or the IPPs.

Under the NPP 1 and IPP 1 information must only be collected if it is necessary for one or more of the organisation's functions and must be collected by lawful and fair means. As it stands, it is questionable whether the collection (particularly by an organisation other than a mobile phone company) of location data by way of tracking technology would be considered to be by 'fair' means. There is no evidence that mobile phone companies presently give collection statements to individuals as required under NPP1.3 or indeed that the individual is even aware that such information is collected, recorded and used.

In addition, an organisation must not use or disclose this information for a purpose other than the primary purpose of collection: NPP 2; IPP2. If mobile phone companies collect this information for the purposes of billing, they are prevented from selling this information for profit without consent from the individual. Such information may be disclosed where it is necessary to prevent or lessen an imminent threat to an individual's life, health or safety or for the prevention, investigation, prosecution or punishment of criminal offences.

Furthermore, organisations collecting personal information are required under NPP 4 and IPP 4 to ensure the security of this information. Given the prevalence of data mining and cybercrime, maintaining the security of such marketable information may be difficult.

CONCLUSION

The collection use and storage of information detailing the location of mobile phone users has significant privacy implications. There is no doubt that in Australia there is a myriad of privacy laws and principles in place to protect the use and misuse of personal information. However, given the global nature of technology today, and the marketable nature of this type of information, one must question whether such laws will be effective in controlling the handling of personal information gathered by tracking technology.

The views expressed in this article are those of the author and not necessarily those of the firm or its clients.

Rebecca Sharman is a Solicitor in the Information, Communications and Technology practice at the Sydney office of PricewaterhouseCoopers Legal.