EXTENDING ACCESS TO TELECOMMUNICATIONS DATA IN CIVIL PROCEEDINGS

Comment by Dr Peter Balint, Professor Clinton Fernandes and Professor Vijay Sivaraman (all from the University of New South Wales and the Australian Centre for Cyber Security) dated 27 January 2017.

This note dated 27 January 2017 addresses a call for submissions by the Attorney-General's Department on the subject of access to telecommunications data in civil proceedings. We have only just become aware of this call for submissions, the deadline for which is this afternoon. Our note is therefore brief, and we request the opportunity to make a more comprehensive submission before the relevant Parliamentary Committee.

We urge legislators to consider three conceptual issues that would result from an expansion of the current regime, and indeed from the current regime itself.

The Internet of Things and the coming data explosion

Legislators' interest has been overwhelmingly focused on communications data as an investigative tool. However, of arguably as much importance (or more) is the explosion of data generated by the so-called 'Internet-of-Things' (IoT). The term IoT refers to the network of physical objects or 'things' embedded with electronics, software, sensors and connectivity to enable objects to exchange data with the manufacturer, operator, and/or other connected devices. Such devices are finding increasing use in a wide range of applications: smart-homes and buildings (smoke-alarms, motion sensors, security cameras), health monitoring systems (wearable medical and fitness appliances), automobiles, industrial automation environments (fridges, climate-control, machine telemetry), and agriculture (soil monitoring, irrigation control). Forecasts by technology research firm Gartner Inc. estimate the number of IoT devices will reach 26 billion by 2020 (Middleton, Kjeldsen, Tully 2013). Interestingly, these devices will communicate among themselves and with the 'cloud' automatically, i.e. objects will exchange data without the knowledge of the user, revealing information on individuals: location, interests, health, habits and so on (Fernandes and Sivaraman 2015).

Legislators must make decisions about Australians' privacy with the coming data explosion in mind. Precedents set now will likely influence the legal-technological terrain for the human species for the foreseeable future.

Consent

The data under discussion is consumer data that has been collected by private companies. Consumers when entering contracts with companies sign consent forms formally allowing their data to be used in a variety of ways, including the sharing with law enforcement agencies. It may seem that this proposed new provision is covered by such contracts, even if some rewording may be required. Yet have Australians actually consented to this type of data collection, and could they even meaningfully be said to have consented? It might be argued that such consent is not required in criminal - especially national security - matters, since coercion goes to the heart of what is generally held to be the power of the state. However, since the call for submissions relates to civil proceedings, consent ought to weigh much more heavily in legislator's considerations.

For consent to be valid there must be: i) full knowledge of what you are consenting to; and ii) a low cost alternative (i.e. a 'your money or your life' situation does not involve free choice)

Precisely how do Australian consumers understand their consent when they 'tick the box' for Terms and Conditions? We submit that legislators must give weight to this issue in their considerations. Even if people do read the Terms and Conditions - and the vast majority do not (Ben-Shahar & Schneider 2011) - how many can actually understand them? Most people lack the background knowledge to make informed choices about their privacy, and do not understand how a series of individual actions can have cumulative and long-lasting future effects (Solove 2013).

Given that our lives will be enmeshed with the IoT forever, there is no possibility of a low cost alternative. No meaningful opt-out option will be possible; it will be analogous to telling people they do not need a bank account and can just put their pay cheque under the mattress: regardless of affluence, we can barely function in a modern society without utilising electronic banking. It is likely to be the same with IoT.

Privacy

The core elements of Privacy have not, we submit, received due attention from legislators. What precisely is its value?

Here there several possibilities. Innes (1992), for example, argues that privacy is essential for intimacy. Without being able to keep parts of ourselves private we cannot have intimate

relationships - something that is essential for a decent human life. This idea of privacy being essential for a decent human life is taken up by various other writers (e.g. Rachels 1975; Moore 2003).

Andrei Marmor (2015, p. 7), writes:

> The main interest in question here is the interest in having a reasonable measure of control over ways in which we present ourselves to others and the ability to present different aspects of ourselves, and what is ours, to different people.

This opacity allows us, for example, to 'take off the mask' that we may wear in public and allows us to show different aspects of ourselves to different people, and to try things out in one sphere before sharing them more widely.

There is also, of course, the risk to liberty. Other agents having information about you, especially when they wield power, exposes you to liberty-restricting risks. This is, of course, the classical liberal concern with limiting state power, where the state was seen as the greatest threat to individual freedom (Balint 2017). So your state may appear to be benign now, but giving it too much power - and information about people is power - may either corrupt it, or provide the tools for future abuses of power and restrictions on liberty. And there is certainly a great deal of historical and sociological precedents to choose from here - even among so-called liberal democratic states.

Many of the issues involved in the IoT seem much less like the classic state/citizen concerns, and much more corporation/consumer in nature: It is not hard to see how the corporate collection and cross-matching of data could lead to important denied opportunities, such as health care discounts, car insurance premiums and so on. Nevertheless, the use of data in civil cases brings back these state/citizen concerns.

Privacy also seems to protect the fundamental value of individual autonomy; when our privacy is violated, we lose control over access to aspects of ourselves. We make plans and decisions based on reasonable background assumptions, one of which is that, at least in certain areas of life, we can control what we reveal to others. Losing this control undermines our autonomy.

Autonomy is undermined in two ways. In the first, the unexpected loss of predictability of our environment is the problem. We make plans and take actions according to certain conditions, but

the conditions change potentially undermining our plans. It may seem then that if we know that our IoT devices are surveilling us, then this first problem does not exist. If you know, for example, that using the internet or your mobile phone may involve other parties listening in or tracking your movements, then your autonomy may not be undermined - your landscape is still predictable, and we can still control our lives within narrower parameters (Marmor (2015) argues that mobile phone tracking and internet surveillance do not breach privacy because we know about them). But this does not mean 'known-about' surveillance is not autonomy undermining.

This is the second way that autonomy is undermined. To see why, imagine if you knew that your home and all communications were monitored, and that your movements were tracked. It seems odd in such a case - especially when compared to a life without surveillance - to say your autonomy and control over your life would not be reduced. Sure, you may be able to avoid doing or saying certain things, but your life plans would likely be severely curtailed. That is, the deliberate avoiding of saying certain things in the places/ways you know are not private reduces the options you have. Indeed, for your autonomy to be undermined in this way, only the possibility of access is required. This is most famously demonstrated in Jeremy Bentham's Panopticon. The possibility of loss of privacy is enough to change behaviour. We do things we would not have otherwise done because we no longer feel our privacy is secure.

We understand the need to protect the security of Australian citizens. But this security needs to be understood as a protection of their basic liberties - of course this includes bodily security, but also privacy. The use of data in civil cases further erodes the protection of privacy, and seemingly not in the service of protecting bodily security.

PETER BALINT
CLINTON FERNANDES
VIJAY SIVARAMAN

REFERENCES

Balint, Peter (2017), *Respecting Toleration: Traditional Liberalism and Contemporary Diversity*, Oxford: Oxford University Press.

Ben-Shahar, Omri, and Schneider, Carl E. (2011), 'The Failure of Mandated Disclosure', 159 U. PA. L. REV. 647: 665–78.

Fernandes, Clinton, and Sivaraman, Vijay (2015), 'It's only the beginning: Metadata Retention laws and the Internet of Things', *Australian Journal of Telecommunications and the Digital Economy*, (3) 3: 47-57.

Innes, Julie (1992), *Privacy, Intimacy, and Isolation*, Oxford: Oxford University Press.

Marmor, Andrei (2015), 'What is the Right to Privacy?', *Philosophy and Public Affairs* 43 (1): 3-26.

Middleton, P., Kjeldsen, P. and Tully, J. Forecast: The Internet of Things Worldwide. (Stamford, CT: Gartner, Inc.) https://www.gartner.com/doc/2625419/forecast-internet-things-worldwide-

Moore, Adam D., (2003), 'Privacy: Its Meaning and Value', *American Philosophical Quarterly*, 40: 215–227.

Rachels, James, 1975, "Why Privacy is Important", *Philosophy and Public Affairs*, 4: 323–33.

Solove, Daniel J. (2013), 'Privacy Self-Management and the Consent Dilemma', 126 Harv. L. Rev. 1880-1903.