HERBERT SMITH FREEHILLS

DRIVERLESS CARS, DRONES AND DNA: HOW TO BUILD TRUST IN THE DATA AGE

16 May 2017 | Australia, Brisbane, Melbourne, Perth, Sydney
Legal Briefings – By **Matt O'Leary** and **Shadia Rahman**

'Trust and transparency' is the theme of this year's Privacy Awareness Week (15-19 May 2017). This is an annual event held since 2006 to raise awareness across the Asia-Pacific region of the importance of protecting personal information.

While 'trust' and 'transparency' may sound like fuzzy concepts, particularly in a legal context, they are increasingly underpinning privacy considerations in our data-driven society.

'Big data' – the processing and use of large scale, complex data – and the 'internet of things' have fundamentally transformed, and will continue to transform, how businesses operate. For example, they are enabling companies to know what consumers want before they do, predict business failures before they happen and monitor employee performance in real time. Big data is also enabling the development and use of highly-advanced technologies such as automated (driverless) vehicles, drones and biometric identification.

But, as the Productivity Commission has identified, a lack of trust in existing data processes is stalling the development of technologies and 'choking the use and value of Australia's data'.[1] One of the keys to addressing this issue is for the public and private sectors to develop more transparent and robust processes for dealing with and protecting data – particularly big data and the ever-expanding array of technologies that rely on it.

1. THE INTERNET OF THINGS

The internet of things (**IoT**) is already a major source of big data, and its influence is growing rapidly.

Put simply, IoT is a term that refers to devices – from simple sensors to smartphones – that are connected together or to the internet. IoT enables businesses to obtain real-time data from devices in people's homes, pockets and handbags, through to devices that are attached to machinery, vehicles and employees. Examples include the smart thermostat that automatically adjusts temperature based on your routines, and the smart refrigerator, which can order milk online before you run out.

To give some indication of the potential scale of IoT, it is estimated that by 2020 there will be up to 30 billion devices connected to the internet.[2]

IoT raises specific privacy concerns because many individuals are unaware that their information is being collected by their devices. Another concern is that the information from many different devices can be combined to provide more meaningful information about an individual. Basic information collected by one device may not be subject to legal protections, but once it is combined with other information, privacy issues may arise.

Research suggests that businesses have poor processes for dealing with their privacy obligations arising from IoT. In September 2016, the Office of the Australian Information Commissioner (**OAIC**) revealed results of its survey showing that 71 per cent of IoT devices did not provide a privacy policy that adequately explains how personal information is managed.[3]

Best practice recommendations from overseas include suggestions from the US Federal Trade Commission that businesses collecting information via IoT devices should:

- build data security into their practices by design;
- where possible, de-identify personal information so that it cannot re-identified;
- consider data minimisation – i.e. limit the amount of data collected; and
- provide individuals with clear and prominent privacy notices, so they have some choice in relation to the personal information they provide.

2. AUTOMATION AND ARTIFICIAL INTELLIGENCE

Automated IT systems, and other automated technologies like drones and driverless cars, are another major source of big data. It is estimated that a single automated vehicle can produce as much data as 3,000 people surfing the Internet, while a small fleet of drones could create 150 terabytes of data (enough to fill the hard drives of 300 laptops) per day.[4]
As well as generating big data, such automated systems rely heavily on big data to operate. If there are deficiencies with the underlying data, this can have significant unintended results. A recent example is the failures of the automated fraud detection system used by the Department of Human Services (Centrelink).[5] Without robust controls and checks, an automated system can generate information about individuals that is not correct – which can have serious consequences for those individuals and for the businesses which rely on the accuracy of the information. It could also breach the Australian privacy principle that requires businesses to take reasonable steps to only handle high-quality information.

In order to build consumer confidence in automated systems, businesses should think carefully about how to deal with the data which is generated and used by such systems. To give some examples of the consumer concerns that have been (and will continue to be) raised in this regard:

- Systems can collect and analyse data about people’s tone, emotion and expression. This type of information is intensely personal, but would probably not be considered ‘sensitive information’ under Australia's privacy laws. Will consumers be concerned if this information is treated with no greater sensitivity than their name or email address?

- IT vendors are increasingly combining the information of several businesses in a particular industry to produce artificial intelligence systems that can better understand individual preferences. Will consumers feel comfortable if data they provide to one business is combined in this way and shared across a broader industry?

- Automated vehicles continuously broadcast messages to other vehicles or to transport systems. This provides detailed information about a person’s movements to many different organisations. With no oversight body for the management of such data, will consumers be comfortable with what the movement of their vehicles is telling the wider world about them?

Road and traffic authorities are already working on some of the privacy issues with autonomous vehicles. As a part of this, Austroads has some suggestions to better protect privacy, including:

- the use of rotating pseudonyms to limit the identification of individual vehicles;

- requiring in-vehicle mechanisms (or alternative processes) that enable a short privacy collection notice to be provided to (and acknowledged by) the driver; and

- the adoption of an industry code of practice for autonomous vehicle manufacturers.[6]

3. BIOMETRICS

Biometrics – such as fingerprints, retina and facial recognition – are used primarily for identification and authentication. Smartphones, for example, have used fingerprint recognition in place of passcodes as a security measure for many years. But this technology will become more important as transactions are increasingly automated and businesses move away from traditional, and simplistic, username-password security measures.

Businesses who use, or are planning to use, biometrics for identification and authentication should be aware that biometric information is subject to a higher level of privacy protection than more traditional forms of identification. This is because biometric identifiers are considered to be 'sensitive information', which means that they:

- may only be collected with consent, except in specified circumstances (this is not required for other types of personal information);

- must not be used or disclosed for a secondary purpose unless the secondary purpose is directly related to the primary purpose for collection and within the individual's reasonable expectations;

- cannot be used for the secondary purpose of direct marketing; and

- cannot be shared by related entities in the same way that they may share other personal information.

While these measures will provide some additional protection to biometric data, many people still express serious concerns about the collection of such data. Biometric data can protect against identity fraud, but the potential for misuse is clear. A stolen card can be replaced, but if the digital file of an iris pattern is swiped, the victim may be subjected to continuing fraud. There are also fears that such information may be misused – for example, facial recognition technology makes surveillance and tracking much easier, and DNA information could be used to influence medical insurance premiums.

Meeting the higher standards afforded under privacy laws to ‘sensitive information’ may not be sufficient to allay these concerns, particularly given that privacy laws do not always keep up with the ways that new technologies deal with personal data or community expectations in response to these developments.

ENDNOTES:

1. Productivity Commission, ‘Data Availability and Use: Overview and Recommendations’, 2017.

2. Forbes, ‘Roundup of Internet of Things Forecasts’, 2016.

3. OAIC, ‘Privacy shortcomings of Internet of Things businesses revealed’, 2016.

4. FTC Staff Report, ‘Internet of things: Privacy & Security in a Connected World’, 2015

5. Bloomberg, ‘Here Comes the War for Commercial Drone Dominance’, 2017.

6. ABC News, ‘We're all talking about the Centrelink debt controversy, but what is 'robodebt' anyway?’, 2017.

7. Austroads, ‘Privacy Impact Assessment (PIA) for Cooperative Intelligent Transport System (C-ITS) data messages’, 2017.

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

TONY JOYNER
LEAD PARTNER –
TMT, PERTH
+61 8 9211 7582
Tony.Joyner@hsf.com

LEGAL NOTICE

The contents of this publication are for reference purposes only and may not be current as at the date of accessing this publication. They do not constitute legal advice and should not be relied upon as such. Specific legal advice about your specific circumstances should always be sought separately before taking any action based on this publication.