Privacy in automation: An appraisal of the emerging Australian approach

Angela Daly *

Queensland University of Technology, Brisbane, Australia

A B S T R A C T

Keywords:
Australia
Facial recognition
Drones
Driverless cars
Data protection
Privacy

This article presents an initial appraisal of the emerging Australian approach to applying privacy and data protection laws to automated technologies. These laws and the general context in which they operate will be explained, with appropriate comparisons made to the European Union frameworks. In order to examine their specific application vis-à-vis automated technologies, three case studies – automated facial recognition technologies (AFRT), unmanned aerial vehicles (UAVs – better known as 'drones') and autonomous vehicles (or 'driverless cars') – are selected to examine the extent to which existing privacy and data protection laws, and their application, can be considered adequate to address privacy and data protection risks that these technologies bring. These case studies evidence existing deficiencies with privacy protection in Australia and the inadequacy of recent reform processes, demonstrating that Australian data privacy laws are not well placed to protect individuals' rights vis-à-vis automated technologies.

1. Introduction

Automated technologies are increasingly being applied in daily life in developed countries. The term 'automation' when combined with technology can encompass a wide variety of devices and services, which are also cross-fertilised by other technological developments such as in algorithms, materials, and the Internet of Things.

Automation may bring various benefits for certain individuals and society at large. Automation may produce profit and efficiency, and facilitate the operation of highly complex systems.[1] However, dangers or disadvantages of automation have also been identified including the automation of jobs, dangers to individuals' health and wellbeing (including death) and even the possible eventual redundancy of humans.[2] These concerns are all, at heart, related to the ability for decisions to be made, and actions taken, by automated technologies directly or by humans on the basis of automated processes without further deliberation.[3] Among these concerns is the negative effect automation may have on individual data privacy and data protection, given many automated technologies rely on data,

---

* QUT Faculty of Law, Queensland University of Technology, GPO Box 2434, Brisbane, QLD 4001, Australia.
E-mail address: Angela.daly@qut.edu.au.
http://staff.qut.edu.au/staff/dalya2/.

[1] Peter Hancock, 'Automation: How Much is Too Much?' (2014) 57 (3) *Ergonomics* 449.

[2] Devdatt Dubashi and Shalom Lappin, 'AI Dangers: Imagined and Real' (2017) 60(2) *Communications of the ACM* 43; Robert Sparrow, 'Killer Robots' (2007) 24(1) *Journal of Applied Philosophy* 62; Stephen Mason, 'The presumption that computers are "reliable"', in Stephen Mason and Daniel Seng (eds), *Electronic Evidence* (4th ed, Institute for Advanced Legal Studies, 2017), at p. 124.

[3] Although in the European Union, Article 15 of the Data Protection Directive provides, subject to some exceptions, that a person should not be subject to a decision which produces legal effects concerning them or significantly affects them based solely on automated data processing intended to evaluate certain personal characteristics, such as that individual's performance at work, creditworthiness, reliability, conduct, etc. An updated version of this provision can be found in Article 22 of the General Data Protection Regulation.

which they may also create about human beings, or data which is created by humans and used by these technologies.[4]

The adequacy of existing laws to address automated technologies has been called into question in various jurisdictions. Autonomous vehicles alone are currently generating a large amount of scholarship about whether a variety of laws, from traffic regulations to the laws of war to tort liability, are appropriate for the characteristics and affordances of this new technology.[5] Among the relevant areas of law is also privacy: Current privacy and data protection measures when faced with automation have been called into question in a number of jurisdictions. In the US, where the Fourth Amendment provides some privacy protection against government interferences, automated systems so far have been implicitly treated by courts as equivalent to human beings for the purposes of the Third Party Doctrine whereby Fourth Amendment protection does not apply to information an individual voluntary discloses to a third party.[6] In the EU, robots may challenge the categories of data controller and data processor on which data protection law is based and render concepts such as privacy-by-design uncertain in their application.[7]

Indeed, the challenges for privacy from automation may be so profound that it has been argued in the context of autonomous vehicles that 'a default lack of privacy for personal travel may become the norm'.[8] Yet automation sounding the death knell for personal privacy may be a flawed technologically deterministic approach. A straightforward solution to the privacy risks – or at least a means of limiting them – in the context of robots and automation may be 'air gaps' i.e. a general policy of disconnecting robots and autonomous machines from the Internet and the cloud as a form of 'privacy before design'.[9]

In an attempt to begin to address some of the legal issues surrounding robots, the European Parliament has been proactive with a Resolution from February 2017 on Civil Law Rules on Robotics.[10] Among the topics covered in this Resolution is privacy and data protection. The European Parliament has requested clarification as regards the rules and criteria for using cameras and sensors in robots within the GDPR's implementation framework, and has also requested that the European Commission ensures data protection principles, control mechanisms for data subjects and appropriate remedies are followed as regards robots; and that the European Commission ensures appropriate recommendations and standards are fostered and integrated into policy.

This European Parliament Resolution is the most prominent attempt by a legislature or government to engage with the privacy and data protection implications of automation and robotics globally, which perhaps is not surprising given EU data protection and privacy laws are the most advanced internationally and represent a high level of protection. Yet automation and robotics are not bound by jurisdiction, and so how other countries' legislatures and governments encounter these technologies is also of great importance for the relationship between privacy and automation. To that end, this article examines the Australian experience with automation and privacy to provide an insight into how this particular jurisdiction is encountering the topic. Australia represents an important point of international comparison, particularly for EU privacy and data protection laws. Australian data privacy laws are based on a similar model to the EU's Data Protection Directive, but the legal system diverges sharply from its European counterparts with the absence of constitutional or enforceable fundamental rights to privacy (or data protection).

This paper takes three emerging 'automated technologies' as case studies in which to understand better the extent to which existing laws – in this case, in the Australian jurisdiction – are fit for purpose. The case studies comprise automated facial recognition technology (AFRT); unmanned aerial vehicles (drones); and driverless cars. These three applications of automated technologies have been selected since they are examples of automation which are currently being rolled out among the general population in Australia, as opposed to remaining under experimental use in research conditions. They are also all technologies which pose problems and risks for the privacy and data protection of individuals, and so represent lenses through which the adequacy of existing laws – and proposals for their reform – can be tested.

This article will proceed by providing some context on the Australian legal system's approach to privacy and data protection laws before exploring how the system has encountered the three aforementioned automated technologies. The article's main findings are that privacy concerns have been acknowledged in the deployment of all three technologies, which include the resurfacing of pre-existing deficiencies in the Australian legal framework to protect privacy, but that no

---

[4] Ryan Calo, 'Robots and Privacy', in Patrick Lin, George Bekey and Keith Abney (eds), *Robot Ethics: The Ethical and Social Implications of Robotics* (MIT Press 2011); Ian Kerr and Marcus Bornfreund, 'Buddy Bots: How Turing's Fast Friends are Under-Mining Consumer Privacy' (2005) 14(6) *Presence: Teleoperators and Virtual Environments* 647.

[5] See e.g. Bryant W. Smith, 'Automated Vehicles Are Probably Legal in the United States' (2014) 1 *Texas A&M Law Review* 411; Maurice Schellekens, 'Self-driving cars and the chilling effect of liability law' (2015) 31(4) *Computer Law and Security Review*; Gary Marchant, Braden Allenby, Ronald Arkin, Edward Barrett, Jason Borenstein, Lyn Gaudet, Orde Kittrie, Patrick Lin, George Lucas, Richard O'Meara, and Jared Silberman, 'International Governance of Autonomous Military Robots' (2010) 12 *Columbia Science and Technology Law Review* 272; Kyle Graham, 'Of Frightened Horses and Autonomous Vehicles: Tort Law and its Assimilation of Innovations' (2012) 52 *Santa Clara Law Review* 101.

[6] Matthew Tokson, 'Automation and the Fourth Amendment' (2011) 96 *Iowa Law Review* 581.

[7] Ugo Pagallo, 'The Impact of Domestic Robots on Privacy and Data Protection, and the Troubles with Legal Regulation by Design', in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection* (Springer 2016).

[8] Daniel Fagnant and Kara Kockelman, 'Preparing a nation for autonomous vehicles: opportunities, barriers and policy recommendations' (2015) 77 *Transportation Research Part A: Policy and Practice* 167.

[9] Bibi van den Berg, 'Mind the Air Gap: Preventing Privacy Issues in Robotics', in Serge Gutwirth, Ronald Leenes and Paul De Hert (eds), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection* (Springer 2016).

[10] European Parliament, *Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics* (2015/2103(INL)) <http://www.europarl.europa.eu/sides/getDoc .do?type=TA&reference=P8-TA-2017-0051&language=EN&ring=A8 -2017-0005>