Horizon Scanning Series

The Effective and Ethical Development of Artificial Intelligence: An Opportunity to Improve Our Wellbeing

Information Privacy

This input paper was prepared by Mark Burdon

Suggested Citation

Burdon, M (2018). Information Privacy. Input paper for the Horizon Scanning Project "The Effective and Ethical Development of Artificial Intelligence: An Opportunity to Improve Our Wellbeing" on behalf of the Australian Council of Learned Academies, www.acola.org.

BURDON RESPONSE TO ACOLA QUESTIONS

1. WILL AI MAKE IT EASIER TO IDENTIFY AND DELETE DATA?

It is a well-worn and well-justified axiom that computers are superior to humans regarding the processing of vast data sets. At face value, therefore, it would seem obvious that forms of AI would make it easier to identify and delete certain sets of specified data types. For example, as developments and applications of facial recognition technology continue to increase, platform and search engine capabilities based on image recognition will also continue to increase (Singer, 2018). It will thus become progressively possible to identify an ever-increasing trove of text, image and video data that is currently beyond the technological capabilities of individual users. However, the real complexity to this question arises in the context of certain types of data that give rise to legal obligations for data collectors, most notably, personal information (House of Lords, 2018, 28). It is therefore important to think about this question in two ways: the internal implications for data collection organisations and the internal and external impacts of being able to delete stored or published personal information.

Processes of collection, storage and use of personal information currently garner information privacy legal obligations for relevantly regulated entities in Australia (Australian Law Reform Commission, 2008). Large private sector corporations and most Commonwealth government agencies are regulated by the *Privacy Act 1988* (Cth) and most state and territory government agencies are regulated by individual state or territory laws. The definition of personal information at section 6(1) of the *Privacy Act* was amended in 2014 but is conceptually similar to other Australian jurisdictions. Information is personal information if it is ‘about an individual that is identifiable or reasonably identifiable.’ Prior to 2014, personal information was information ‘about an individual that is apparent or reasonably ascertainable’ and this definition is still in operation in most state and territory jurisdictions.

The ability of any AI to identify personal information therefore requires a careful consideration of whether information is about an individual in either an identifiable or reasonably identifiable sense or an apparent or reasonably ascertainable sense. The first element is relatively straightforward as certain categories of information can

generally be classed as personal information: name, email address, unique identifiers and photos or videos that are visually capable of emanating identity. In all of these cases, it should be possible to design algorithmic frameworks that can detect identifiable individuals from a range of different type of data situations because the detection is ultimately based on the ability to categorise information with little analytical recourse as to how the information was generated. For example, a photograph of an identifiable individual is personal information.

However, the situation is more complex regarding the reasonably identifiable element which is not as straightforward and refers to identifications that arise out of data aggregation processes. In such situations, the boundaries of personal information are constantly shifting (Productivity Commission, 2016, 182). In effect, data that does not readily identify an individual can be aggregated together with other data to enable identification. For example, mobile phone metadata, which can be used to create a historical record of location activity, can be used to identify individual life-style patterns (Isaacman et al., 2011) and thus assist to enable identification of an individual. In these situations, understanding the social context of data generation becomes crucial particularly regarding the capabilities, resources and abilities of the data aggregating organisation. In other words, this is a complex legal and regulatory question that requires a significant degree of expert legal analysis.

The current situation in Australia is also legally confused following the 2017 Full Court of the Federal Court decision of *The Privacy Commissioner v Telstra* (2017). The case history involved a journalist, Ben Grubb and his attempt to access his mobile phone location metadata from his provider, Telstra. Telstra refused to provide this information on the basis that it was not personal information and thus it was not obliged to do provide it. Telstra held this information in multiple databases and argued that it was a difficult and challenging task to connect data together in order to reveal the identity of the journalist. The journalist complained to the OAIC and the Privacy Commissioner had to determine whether the journalist's mobile phone metadata was personal information. This culminated in a series of cases that scrutinised the meaning of 'about' in the definition of personal information (Yuvaraj, 2017).

For the purpose of this report, the Court held that 'about' has substantive application and therefore it is necessary to consider whether information is about an individual

before assessing whether it identifies an individual. The Court also accepted at that information can have multiple subject matters, for example, it can be about an individual and it can be about something else, and thus an evaluative conclusion is required that considers information in its totality.

The ability of any AI system to identify personal information in a reasonably identifiable sense will therefore need to undertake an evaluative conclusion that considers the aggregated information in its totality and the potential application of multiple subject matters to determine whether the aggregated output is 'about' an individual.

AI identification and deletion of data is consequently not just a technical issue. It is a complex legal issue in which the uncertain requirements of law, particularly regarding the categorisation of personal information, will somehow need to be coded into algorithmic frameworks. Given the information privacy legal obligations that arise, and the increasing penalties for breaching those obligations, it would seem likely that AI or machine learning frameworks could be utilised to assist with the provenance of data aggregation processes but that the degree of legal interpretation skills required are still such that the ultimate identification of personal information will still remain a human analytical task, particularly given the legal uncertainty regarding interpretative processes of categorisation.

2. How might we ensure citizens retain a right to their data, and have the capacity to opt out?

As above, one of the crucial questions here is whether 'a right to their data' regards data that would be classified as personal information. If that is the case, then citizens will already have access to a suite of protections derived through the application of information privacy principles.

The traditional forms of information privacy law provide procedural protections that seek to imbue fairness in personal information exchange processes. Individuals are provided with a limited range of process rights that provide a degree of control over how personal information is collected, handled, and used by data collectors. Individuals can access and amend collected personal information, can request to see personal information held about them and ask that 'out of date' information about them

be deleted or amended. Similarly, data collectors are obliged to inform users about when and why collections are undertaken, to collect personal information only for relevant and specified purposes, to store personal information securely and to ensure that subsequent uses are in accord with the purpose of collection.

At the heart of information privacy protections is the notion that life-cycle management processes of personal information should be processed fairly and lawfully. Fair and lawful activities are thus the guiding frame for how life-cycle management of personal information should operate.

Accordingly, Australian citizens already have a suite of protections and the real issue is whether those protections will still have the same substantive application in structures of automated collection and analysis. That in itself is a contentious issue given the many criticisms that have been put forward about the veracity of Australia's information privacy law framework to adequately provide individual protections (Lindsay, 2005, Burdon and McKillop, 2013, Greenleaf, 2001, Signato and Burdon, 2015), particularly in the recent context of those now available to EU citizens under the General Data Protection Regulation (GDPR).

Along with the traditional types of information privacy protections highlighted above, the GDPR introduces several enhanced information privacy protections for individuals specifically relating to automated profiling, which would include an AI decision-making context (Article 29 Data Protection Working Party, 2016). These include:

- Articles' 13 and 14 provide enhanced transparency measures that require data controllers to inform individuals about the existence and scope of automated decision-making;
- Articles' 17 and 18 provide the ability to rectify or erase personal information used as part of an algorithmic output and the output itself; and
- Articles' 21 and 22 provide rights to object to data processing, particularly in the latter context which provides a right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

It is currently unclear, exactly how Article 22(1) will apply (Edwards and Veale, 2018, Kaminski, 2018, House of Lords, 2018, 30) but it has been argued that it establishes a general prohibition for decision-making based solely on automated processing, unless certain exemption situations arise (Article 29 Data Protection Working Party, 2016). What is clear, however, is that while some of these protections are conceptually similar to the principled protections of Australian information privacy law, namely, the Australian Privacy Principles (APPs 12 and 13 regarding access and correction) the regulatory focus in the EU on automated processing is novel, compared to Australia. One of the perennial criticisms of the *Privacy Act* is that it is woefully under-litigated and thus we do not have significant judicial consideration as to how the key protections and components of the Act should be interpreted (Burdon and McKillop, 2013). As such, it is unclear whether the Australian framework would provide the same degree of protections to personal information in an AI processing and decision-making context.

The question to ask therefore is how well positioned is the Australian information privacy law to ensure the retention of existing protections that allow citizens to retain appropriate levels of control about what happens to their personal information? The answer appears that it is seemingly not well placed to provide suitable and specific protections for automated decision-making environments, at least under the model of traditional information privacy principles and protections. Instead, the Australian Government appears to be more focussed on the development of a new form of data right, predicated on data portability, such as Article 20 of the GDPR.

Data portability encourages interoperability of data formats and the adoption of common data storage/data processing standards to facilitate and individual's ability to move, copy or transmit data from one IT environment to another (Article 29 Data Protection Working Party, 2017). In effect, data portability provides a protection for consumers from having their data stored in closed platform 'silos' that are incompatible with each other thus locking the consumer into a service provider (Article 29 Data Protection Working Party, 2017). The right therefore has three components: access; reception and transmission which operate together to provide enhanced individual protections to foster competitive opportunities for further innovations

The advent of an Australian data portability right is important because of unfolding Australian policy developments via the Productivity Commission's recent report on 'Data Availability and Use' (Productivity Commission, 2017) and the Open Banking Review. Both appear to herald a new response to Australian information privacy regulation that places a much greater emphasis on consumer protection as a desired societal outcome of information privacy law. That in itself, may signal some significant regulatory shifts that are unfolding. It is therefore possible, at a regulatory model level, that the Australian framework is about to enter a space of hybridity regarding the retention of existing information privacy rights and the development of new consumer privacy rights that will impact upon processes of automated data collection and analysis.

The emerging and seemingly innocuous data portability rights are a case in point because they provide an insight into the shifting regulatory landscapes of information privacy, consumer protection, competition law and trade innovation that are unfolding as the backdrop to consider citizen data rights in the context of organisational AI decision-making.

3. WHAT ARE THE IMPLICATIONS FOR THE USE OF DATA FROM PEOPLE NO LONGER LIVING?

I don't really have anything to add on this particular point. My only observation is that discussions around the digital assets of deceased persons have thus far been limited to questions of ownership and proper procedural implications, such as how to close social media accounts and who should be able access data.

That said, these implications are likely to increase manifold in the future particularly in the context of automated decision-making by expert systems. As we keep moving into societies where data about everything is collected, stored and used then the sophistication of detailed historical accounts of individual activities and behaviours will increase. If a sufficiently detailed account of activity can be generated then it is likely that decision-making capabilities of individuals will be able to be increasingly predicted or inferred. Again, the development of data portability rights and the advent of personal information management systems (PIMS) are instructive. Both will allow the historical accumulation and storage of all kinds of data, to the extent, that life-long histories of

activities and behaviours can be accumulated in a data format. At that point, it could then become possible to infer the decision-making outcomes of deceased persons. As such, while much of the discussion currently regards who has access to accounts and owns digital assets after death, in the future, there may also be issues of automated and inferred decision-making of deceased persons based on extended, historical data holdings. This could lead to arguments about the creation or identification of new forms of legal identity predicated on expert system, decision-making inferences regarding the historical accumulation of deceased individual life-long data repositories.

4. HOW IMPORTANT WILL DATA INTEGRITY BE TO DEVELOPING MACHINE LEARNING AND USE IN ALGORITHMS?

Answers to the first two questions put forward arguments about the continuing relevance of information privacy law regarding automated decision-making in the context of AI. It should of course be noted that the demarcated boundaries of information privacy protections are themselves being challenged due to the changing structures of data collection, storage and analysis. In effect, the very notion of organisational life-cycle management of personal information is under stress which is directly relevant to the role of data integrity and machine learning (Academy and Society, 2017).

Information privacy laws were first implemented at a time where the traditional data lifecycle was definable and capable of being managed by each individual organisation. Information privacy protections accorded a set of accountability measures that tied the provider, collector and on-user of personal information together in a binary chain of rights and obligations. Each information privacy principle logically dovetailed with other principles to provide a coherent, life-cycle protection mechanism. Personal information could only be collected for certain requirements which meant that its uses were restricted. Individual providers have to be notified of collection purposes and uses. Unrequired personal information has to be destroyed or de-identified.

The processes and structures of data collection have changed to the extent that the notion of operational and organisationally independent data lifecycles are now being increasingly strained (Academy and Society, 2017). Data, and personal information

particularly, is no longer provided. Rather, it is generated in increasingly sensorised environments and contexts (Andrejevic and Burdon, 2014). As such, it may no longer be sufficient to think about organisationally independent data lifecycles and it has been argued that it is more suitable to think of developing structures as interconnected and interdependent exchangeable networks of data (Academy and Society, 2017). It is this environment, and the underlying data logics that dominate it, which stretches the bounds of information privacy law application and could thus reduce the scope of protections by diminishing the ability to protect across organisational lifecycle management processes.

If that is the case, and this point is in itself a point of contention, then the application of information privacy protections may no longer have the same intended lifecycle ambits. That in turn, may assist to explain some of the underpinning conceptual shifts that are taking place regarding the regulatory context of AI decision-making, namely, the increasing focus on ethical focus and the legal and regulatory enhancement of component life-cycle protections, such as, data portability.

The effect of these changes could mean an even more important role for data integrity in relation to machine learning uses for algorithmic frameworks. Information privacy principles create protected points of interaction and obligation that imbue fairness into the process of personal information exchange. If those points of fairness are removed, or ameliorated, then that will place greater emphasis on the provenance and veracity of information itself in order to preserve at least some degree of component fairness protections.

The quality and accuracy requirements of personal information are already recognised as a key information privacy protection. For example, APP10 requires organisations to take reasonable steps to ensure personal information is accurate, up-to-date and complete particularly with regard to use or disclosure purposes. There is thus an explicit recognition that the use and disclosure of inaccurate personal information can give rise to significant detrimental impacts for individuals.

Given that the quality of data is instrumental to the construction of final machine-generated outputs (House of Lords, 2018, 29), then issues regarding the provenance, quality and integrity of data will become more important particularly in open networks

of data exchange in which the points of collection, disclosure and analysis become continually blurred. Similarly, the advent of new processes, such as data portability, are also going to augment the requirements for enhanced data integrity measures given that a significant variety of different data types will become tradeable. The consequence of moving away from organisationally independent data lifecycle controls means that issues of data integrity will become visible and thus more accountable across a much wider network of participants.

5. WHAT ARE THE BENEFITS FROM BEING ABLE TO LINK DATA SETS?

This is a contentious question because potential benefits from increasing forms of ubiquitous data collection, storage and aggregation cannot be judged solely on their own outcomes. These benefits are not just technical considerations but exist equally in a political, social and legal context. The cumulative acceptance of data accumulation logics, particularly in the public sector (Academy and Society, 2017, 42), are starting to give rise to voluble public concerns regarding key public policy issues, such as, the mandatory opt-out process of the MyHeathRecord implementation, the loosely specified uses of census data for government-wide data analytics and automated welfare debt collection processes. Concerns also emanate in relation to private sector data accumulation strategies and where the boundaries lie between enhanced forms of personalised customer-focussed services and the development of hyper-personalised, individual and collective monitoring macro-structures (Yeung, 2016, Calo, 2017, 423), which gives rise to new forms of surveillance or informational capitalism (Zuboff, 2015, Cohen, 2017, Yeung, 10).

With that in mind, the benefits from enhancing the ability to link data sets can be broadly defined as follows:

- *Enhanced Policy and Service Insights* – the accumulation and aggregation of greater amounts of data will provide a more accurate insight into the intricate complexities of societal life (Executive Office of the President and National Science and Technology Council, 2016). It is important to bear in mind that the ability to link data sets is just one factor of gaining enhanced insight. Equally important is the amassed sensorised generation of data outputs from ever-increasing sources, unhelpfully defined as the ‘Internet of Things.’ Insightfulness

from data analysis is thus being increasingly shaped by the ability to dip into continuous streams of sensorised data flows as opposed to the ability to link static data sets;

- *Better choices* – as highlighted above in relation to telematics, enhanced insights into activities could enable better choice making mechanisms by consumers. Increased access to data could and analytical outputs could thus assist better consumer choice making (Productivity Commission, 2016, 84);
- *Better Resourcing* – the combination of enhanced forms of data collection and analysis are giving rise to improved knowledge for resource allocation (Productivity Commission, 2016, 89). For example, smart grids operate in conjunction with smart meters which are the next generation of gas and electricity meters. Smart meters provide a number of benefits for both user and supplier alike because they generate near to real-time data on energy consumption. For the supplier, the collective use of smart grids provides a much more detailed understanding of electricity usage at every stage in the grid. Demand can be identified much more quickly across the grid and in the home. The activities of the individual, the building and the environment are again connected and it becomes possible to see, for the first time, the visible effects of individual action in the home and its concomitant impact across the grid;
- *Enhancing Transdisciplinary Approaches* – the increased focus on data as a the primary point of public policy and corporate service development will mean that there will be a continuing homogenisation of different professional and academic disciplines around data-driven processes. Crawford and Calo call for the development of enhanced forms of social-systems analysis that involve transdisciplinary collaboration to generate the broader questions of AI application and to generate a ‘more holistic and integrated understanding’ of consequences that move beyond disciplinary silos {Crawford, 2016 #3541, 313}. Automated processes of data linkage, in this sense, will therefore extend the boundaries of disciplinary considerations regarding the development of AI and automated structures of governance.

6. ARE THERE IMPLICATIONS FOR INDIVIDUALS FOR THEIR DATA BEING LINKED - E.G. COULD THERE BE UNKNOWN NEGATIVE EFFECTS AS WELL AS POSITIVE ONES, SUCH AS INCREASED HEALTH INSURANCE PREMIUMS?

There will be a range of individual implications from increased forms of data accumulation and aggregation. Some foreseen implications will provide positive individual and societal benefits through greater insights and enhanced anticipatory forms of resource allocation. It is likely that some unforeseen effects will also negatively impact individuals and communities. These potential negative impacts could be ameliorated through the committed application of information privacy law that would define and determine legally acceptable bounds of data linkage involving personal information. However, as highlighted in the answers above, the future scope and application of Australian information privacy law is becoming uncertain and is being actively challenged by the increasingly dominant policy paradigm of data innovation, in which data, including personal information, is being characterised as a tradeable asset to stimulate growth in digital economies (Productivity Commission, 2016, 47).

These challenges to the foundational basis of information privacy law will become increasingly important as the transition to processes of automated data collection, accumulation and aggregation persist. The advent of sensorised collections is powering new forms of data collection logic. More sensors in more devices create more data which in turn open more avenues for new data collection by newly developed sensors and devices. Thus, the type of data collection that now drives the processes of data linkage are very different to previous data collection environments. In the past, data collection was a specific and purposeful act. Now, data collection from device sensorisation is circular, continuous and never ending (Andrejevic and Burdon, 2014).

As highlighted above, the historical accumulation and analysis of data will increase governmental and corporate abilities to identify individual behavioural insights (Academy and Society, 2017, 43). Once these insights are generated, then nudging actions can be taken to influence individual behaviours in both positive and negative ways, such as in the burgeoning telematics industry for car insurance.

For example, data-driven insights from individual driver activity can be used to 'nudge' policyholders towards more positive behaviours that are less risky and are less likely to result in claims arising in the first place (Naylor, 2017, Canaan et al., 2016). For example, smartphone usage and sensorised devices are increasingly being used to monitor and measure customers' driving behaviours, such as the distance driven, driving speed, location, how abruptly the car brakes and phone usage during driving (Canaan et al., 2016). By furnishing drivers with this data, or by supplying customers with automated reminders, real-time coaching or scoring, to track safe driving behaviours, individual driving habits could be improved which benefits both the insured individual, the insurer and society at large (Clarke and Libarikian, 2014).

However, the same telematics infrastructure can also be used to infer more sensitive states of emotional being. For example, in-cabin sensors and cameras can also detect complex driver cognitive states such as emotions, frustration and fatigue (Goadsuff, 2018, el Kaliouby, 2017). The reasoning behind these telematics-based insurance models pertains to the correlation of certain moods and emotions as being predictive of risky patterns of decision-making, such as impulsive decisions or being inattentive whilst on the roads (Canaan et al., 2016). The point here is that the same data collection processes can be used to power different forms of modelling and thus it becomes attractive to disregard the difference between a primary use of collected data for car insurance purposes with the secondary use of emotional state identification of drivers. Thus it becomes continually possible for organisations to derive intimate knowledge about an individual from the availability of continuous data flows (Calo, 2017, 421).

At one level, this is an issue regarding the bounds of individual information privacy protection. Individuals should retain control over their personal information which should not be used for purposes that have not been previously specified. However, at a societal level this is a signifier of a much larger concern.

A world of data accumulation and aggregation is fundamentally different from the world we have previously lived in. We cherish our private spaces as they fulfil our need for individual autonomy and enhance personal growth. Privacy is an intrinsic feature of liberal societies and is representative of our tacit, and often, under-articulated desire for freedom. Information privacy law recognises the dangers of omnipotent collections

of information and provide individuals with a range of limited rights of access and control over what happens to their personal information. These laws set the boundaries of socially acceptable behaviour regarding the exchange of personal information and thus ultimately seek to protect individual autonomy.

The application of information privacy law should therefore not be the only factor from which to examine the implications for individuals from data linkage. It is an individual strand in a broader societal fabric but it is a strand that requires careful consideration (Calo, 2017, 424). The increasing use of automated data collection and decision-making processes, without proper legal safeguards pertaining to information privacy, will have the effect of diminishing individual privacy protections but will also weaken the societal fabric of any liberal society predicated on interests and values that purport to promote autonomous individuals (Yeung, 2016).

7. ARE ISSUES AROUND INTERNATIONAL STANDARDS FOR DATA COMPATIBILITY AND INTEROPERABILITY?

I don't have anything to add in relation to this question specifically regarding international standards. However, following above, I make a couple of comments on data portability as a policy vector that will create legal obligations involving enhanced forms of data compatibility and interoperability for personal information.

For example, Article 20 of the GDPR creates a new right of data portability which goes beyond the access principles of traditional information privacy laws, such as APP12. Under Article 20, a data subject (e.g. an individual) can receive their personal data, provided to a data collector in digital format, in a structured, commonly used and machine-readable format for their own use. Portability standardisation is intended to empower individuals by providing them with more control over their data and also to foster competition between data collectors by making it easier for customers to switch between different service providers without hindrance (Article 29 Data Protection Working Party, 2017).

The data portability right thus encourages interoperability of data formats and the adoption of common data storage/data processing standards to facilitate and

individual's ability to move, copy or transmit data from one IT environment to another (Article 29 Data Protection Working Party, 2017).

In effect, data portability provides a protection for consumers from having their data stored in closed platform 'silos' that are incompatible with each other thus locking the consumer into a service provider (Article 29 Data Protection Working Party, 2017). The right therefore has three components: access; reception and transmission which operate together to provide enhanced individual protections to foster competitive opportunities for further innovations.

As highlighted above, the core jurisprudential basis of EU information privacy law is to provide expansive rights-based protections for individuals. This gives rise to broad interpretations of personal data and, in the context of data portability, broad interpretations of digital personal data provided to a data controller by an individual. A narrow reading of this requirement could only choose to focus on the types of personally identifiable information provided when establishing a customer account, namely, name, address, etc. Instead, the types of personal data covered by the data portability right is unsurprisingly expansive and includes:

- Data actively and knowingly provided (e.g. name, mailing address etc.) and
- Observed data arising from the use of a service or a device (e.g. search histories, traffic data, location data and raw data from wearable devices).

However, the right to data portability does not extend to all circumstances and does have limits in application.

- The right does not apply when the data processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller, or when a data controller is exercising its public duties or complying with a legal obligation (Article 29 Data Protection Working Party, 2017).
- The right only applies to digital data provided to a data controller by an individual. It therefore does not cover personal information acquired by the controller from other sources.

- More importantly, the right also does not apply to portability in respect of profiling or analytics work undertaken by data controllers. It therefore does not include 'inferred' or 'derived' data where an algorithmic assessment has been made about an individual based on behavioural monitoring (Information Commissioner's Office (UK), 2018). Thus, the raw data is portable but the analytic insight is not. Accordingly, while the right seeks to increase the control individuals have over the use of their personal data, including creating new options of consumer-oriented trade, the purpose of the right, and indeed the GDPR in general, is to regulate personal data rather than competition in the EU data ecosystem (Article 29 Data Protection Working Party, 2017, Lynskey, 2017). Corporations can thus still safeguard their competitive advantage by being able to retain algorithmically-driven insights.

Data portability is therefore viewed as an important update to traditional information privacy rights, it also has a significant innovation-oriented focus that seeks to enhance consumer protections and stimulate competitive digital economies at the same time. Unlike the EU position in which rights-based information privacy modes, competition considerations and consumer protections are enmeshed through the data portability right, the Productivity Commission's Comprehensive Right is specifically focussed on expanding consumer control and use of data to stimulate digital economy innovations that is separate from information privacy regulatory models. However, it can be said that both the EU and Australian policy positions will give rise to a much greater focus on the exchange of information to customers which will start to establish legal standards of compatibility and interoperability.

2017. *The Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFC 4 (19 January 2017.

ACADEMY, B. & SOCIETY, R. 2017. Data management and use: Governance in the 21st century.

ANDREJEVIC, M. & BURDON, M. 2014. Defining the Sensor Society. *Television and New Media***,** 1-18.

ARTICLE 29 DATA PROTECTION WORKING PARTY 2016. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.

ARTICLE 29 DATA PROTECTION WORKING PARTY 2017. Guidelines on the right to "data portability".

AUSTRALIAN LAW REFORM COMMISSION 2008. *For Your Information: Australian Privacy Law and Practice,* Canberra, Law Reform Commission.

BURDON, M. & MCKILLOP, A. 2013. The Google Street View Wi-Fi Scandal and Its Repercussions for Privacy Regulation. *Monash University Law Review,* 39**,** 702-738.

CALO, R. 2017. Artificial Intelligence Policy: A Primer and Roadmap. *UC Davis Law Review,* 51**,** 404-429.

CANAAN, M., LUCKER, J. & SPECTOR, B. 2016. Opting in: Using IoT connectivity to drive differentiation. *In:* DELOITTE (ed.).

CLARKE, R. & LIBARIKIAN, A. 2014. *Unleashing the value of advanced analytics in insurance* [Online]. Available: https://www.mckinsey.com/industries/financial-services/our-insights/unleashing-the-value-of-advanced-analytics-in-insurance [Accessed].

COHEN, J. E. 2017. The Biopolitical Public Domain: the Legal Construction of the Surveillance Economy. *Philosophy & Technology*.

EDWARDS, L. & VEALE, M. 2018. Slave to the Algorithm? Why a 'Right to Explanation' is Probably Not the Remedy You Are Looking For. *Duke Law and Technology Review,* 16**,** 18.

EL KALIOUBY, R. 2017. We Need Computers with Empathy. *MIT Technology Review*.

EXECUTIVE OFFICE OF THE PRESIDENT & NATIONAL SCIENCE AND TECHNOLOGY COUNCIL, C. O. T. 2016. Preparing for the Future of Artificial Intelligence.

GOADSUFF, L. 2018. *Emotion AI Will Personalize Interactions* [Online]. Gartner. Available: https://www.gartner.com/smarterwithgartner/emotion-ai-will-personalize-interactions/ [Accessed].

GREENLEAF, G. 2001. 'Tabula Rasa': Tens Reasons Why Australian Privacy Law Does Not Exist. *University of New South Wales Law Journal,* 24.

HOUSE OF LORDS, S. C. O. A. I. 2018. AI in the UK: ready, willing and able?

INFORMATION COMMISSIONER'S OFFICE (UK) 2018. Guide to the General Data Protection Regulation (GDPR).

ISAACMAN, S., BECKER, R., CÁCERES, R., KOBOUROV, S., MARTONOSI, M., ROWLAND, J. & VARSHAVSKY, A. Identifying Important Places in People's Lives from Cellular Network Data. *In:* LYONS, K., HIGHTOWER, J. & HUANG, E. M., eds. Pervasive Computing, 2011// 2011 Berlin, Heidelberg. Springer Berlin Heidelberg, 133-151.

KAMINSKI, M. 2018. The Right to Explanation, Explained.

LINDSAY, D. 2005. An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law. *Melbourne University Law Review,* 29**,** 131-178.

LYNSKEY, O. 2017. Aligning data protection rights with competition law remedies? The GDPR right to data portability' *European Law Review,* 42**,** 793-814.

NAYLOR, M. 2017. *Insurance Transformed*, Springer.

PRODUCTIVITY COMMISSION 2016. Data Availability and Use.

PRODUCTIVITY COMMISSION 2017. Data Availability and Use.

SIGNATO, J. & BURDON, M. 2015. The Privacy Commissioner and Own-Motion Investigations into Serious Data Breaches: A Case of Going through the Motions? *University of New South Wales Law Journal,* 38**,** 1145.

SINGER, N. 2018. Facebook's Push for Facial Recognition Prompts Privacy Alarms. *New York Times*, 9 July 2018.

YEUNG, K. 2016. 'Hypernudge': Big Data as a mode of regulation by design. *Information, Communication & Society***,** 1-19.

YEUNG, K. 2017. Algorithmic regulation: A critical interrogation. *Regulation & Governance*.

YUVARAJ, J. 2017. How about me? The scope of personal information under the Australian Privacy Act 1988. *Computer Law & Security Review*.

ZUBOFF, S. 2015. Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology,* 30**,** 75-89.