American Journal of Science, Engineering and Technology
2019; 4(4): 55-65
http://www.sciencepublishinggroup.com/j/ajset
doi: 10.11648/j.ajset.20190404.11
ISSN: 2578-8345 (Print); ISSN: 2578-8353 (Online)

Data Protection and Artificial Intelligence Law: Europe Australia Singapore - An Actual or Perceived Dichotomy

Robert Walters[1, *], Matthew Coghlan[2]

[1]Lecturer, Victoria Law School, Victoria University, Melbourne, Australia

[2]Associate, Asian Law Centre, Faculty of Law, University of Melbourne, Melbourne, Australia

Email address:
Robert.walters@vu.edu.au (R. Walters)

[*]Corresponding author

To cite this article:
Robert Walters, Matthew Coghlan. Data Protection and Artificial Intelligence Law: Europe Australia Singapore - An Actual or Perceived Dichotomy. *American Journal of Science, Engineering and Technology.* Vol. 4, No. 4, 2019, pp. 55-65. doi: 10.11648/j.ajset.20190404.11

Received: November 1, 2019; **Accepted**: November 27, 2019; **Published**: December 5, 2019

Abstract: Artificial Intelligence (AI) is moving so rapidly policy makers, regulators, governments and the legal profession are struggling to keep up. However, AI is not new and it has been used for more than two decades. Coupled with AI, personal data, along with cyber security law, and the challenges posed by the current legal frameworks are nothing short of immense. They are, in part, at odds with each other, and are doing very different things. This paper explores some of the challenges emerging in Australia, Europe and Singapore. The challenge of the interrelationship between personal data and AI arguably begins with who has manufactured the AI. Secondly, who owns the AI. Another challenge that has also emerged is defining AI. Most people are able to understand what AI is and how it is beginning to impact the economy and our daily lives. However, there is no clear legal definition of AI, because AI is so nebulous. This burgeoning area of law is going to challenge society, privacy and economic experts, regulators, innovators of technology, as there continues to be a collision between them. Furthermore, the collection of personal data by AI challenges the notion of where responsibility lies. That is, AI may collect, use and disclose personal data at different points along the technology chain. It will be highlighted how the current data protection laws rather than promote AI projects, largely inhibit its development. This paper identifies some of the tensions between data protection law and AI. This paper argues that there is a need for an urgent and detailed understanding of the opportunities, legal and ethical issues associated with data protection and AI. Doing so will ensure an ongoing balance between the economic and social issues that are attached to the two areas of the law.

Keywords: Artificial Intelligence, Data Protection, Australia, European Union, Singapore

1. Introduction

The protection of personal data is fast becoming one of our generations most important challenges. [1] The challenges surrounding data protection were highlighted by the June 2019 G20 Leaders in Japan. The G20 Leaders Declaration stated that:

innovation is an important driver for economic growth, which can also contribute to advancing inclusiveness. We will work toward achieving an inclusive, sustainable, safe, trustworthy and innovative society through digitalization and promoting the application of emerging technologies. We share the notion of a human-centered future society, which is being promoted by Japan as Society 5.0. As digitalization is transforming every aspect of our economies and societies, we recognize the critical role played by effective use of data, as an enabler of economic growth, development and social well-being. We aim to promote international policy discussions to harness the full potential of data. [2]

The Leaders go on to declare that the cross-border flow of data, information, ideas and knowledge generates higher productivity, greater innovation, and improved sustainable development, while raising challenges related to privacy, data protection, intellectual property rights, and security. By continuing to address these challenges, we can further facilitate data that can flow freely and strengthen consumer and business trust. In this respect, it is necessary that legal frameworks, both domestic and international, should be respected. Such data free flow

with trust will harness the opportunities of the digital economy. [3] This in itself becomes one of the most formidable challenges facing the international community (public and private sectors). The lack of consistency and the divergent approaches taken by states towards the regulation of personal and commercial data, varies greatly. More pervasively, states have different sovereign needs and therefore, the development of the law surrounding the use and application of systems and platforms that support the use of data varies greatly. Another layer of complexity also pervades the various regulatory approaches, such as, the use and interaction of Artificial Intelligence (AI). However, the idea that AI is new could not be further from the truth. It has been used in traffic lights, urinals, the manufacture of motor vehicles and used by pilots in aircraft, amongst others for more than a decade. The new economy will likely use AI across many jobs and functions that have been traditionally undertaken by humans. These systems, but not all, can also capture and use personal data.

The tension between data protection and AI is further challenged by the regulatory approaches taken by nation states. Firstly, AI, to date, has largely been regulated by the market and there is very little government regulation that sets minimum standards, in new and emerging areas. Secondly, data protection law being a recent addition to the regulatory framework, has a specific role that, provides a level of control and protection of personal data. Thirdly, there is a lack of clarity within the law about where responsibility lies within AI. That is, if one was to apply the principles of criminal law to AI and data protection, it requires a mental element and an action. Machine learning AI would come with a mental element and they carry out an action. For example, the owner of a dog that attacks a human and kills them is responsible for that dog, and the dog could be put down (perpetrator via another). [4] Also, the scenario where a robot that is governed by AI kills a human – who has responsibility for that action? It is the manufacturer of the AI? Could it be the programmer? Thus, where does the responsibility lie where a robot captures and uses the personal data? There are many similarities with self-driving cars, robots and other AI systems that are likely to capture personal data. Kingston highlights how using the self-driving car example that is speeding, is a strict liability offense. [5] In referring to Gabrielle Hallevy, Kingston goes onto say that if a self-driving car was found to be breaking the speed limit for the road it is on, the law may well assign criminal liability to the AI program that was driving the car at that time. This is because, unlike the traditional control of the car has been by a human, with which responsibility and liability is apportioned. However, a self-driving car is not controlled by any human, but rather a program. Kingston is of the view that in this case, the owner may not be liable, but rather the programmer. Thus, in AI where the human interface or control, this paper argues that the current concept of consent and definition of personal data may not be adequate.

2. Road Map

This paper explores some of the challenges between AI and data protection that is emerging in a select group of countries including Australia, European and Singapore. Section I highlights how AI has no settled definition. Section II discusses the interrelationship between data protection and AI. Section III briefly highlights how data protection law has defined personal data is a very specific way, which is being captured, used and disclosed by AI technology. Section V highlights how it is difficult to determine where ownership of AI begins and concludes. Section VI concludes the paper by providing answers to some of the challenges raised in this paper and a pathway forward. It also highlights the need for a global understanding of the legal landscape between data and AI.

3. Defining Artificial Intelligence

AI is changing society in ways that were once only the ideas and thought of science fiction. [6] However, the English mathematician Alan Turing introduced AI as a concept back in a 1950, and American computer scientist John McCarthy coined the term artificial intelligence during the Dartmouth Conference in 1956. Moreover, AI has not been defined. To date, there is no single definition of AI that has been accepted by all technology practitioners,[7] or legal practitioners. Some define or otherwise categorise AI broadly as a computerized system exhibiting behaviour commonly thought of as requiring intelligence. However, others define AI as a system, capable of rationally solving complex problems or taking appropriate action to achieve its goals in real-world circumstances. [8] AI's technological breakthroughs dramatically accelerated in the last two decades, fueled by advances in ML algorithms, exponential growth in the availability of data, and improved and cheaper computing power. The impressive technological progress of the last decade in particular has led to AI's ability to "perform activities which used to be typically and exclusively human", as well as to develop certain autonomous and cognitive features – e.g. the ability to learn from experience and take quasi-independent decisions. AI is now revolutionizing the way people live, work, learn, discover and communicate, putting them on the threshold of an era where increasingly sophisticated robots, bots, androids and other manifestations of AI are poised to unleash a new industrial revolution. AI has also been categorized on its intelligence level, such as artificial general intelligence, which is a notional form of AI that, exhibits a level of intelligence comparable to that of the human mind. It has also been defined quite narrowly as a technology that solves specific tasks.

On the backdrop of the beginnings of AI and the current lack of a specific definition, computer vision and AI planning, such as, drive video games are now a bigger

entertainment industry than Hollywood. Deep learning, a form of machine learning based on layered representations of variables referred to as neural networks, has made speech-understanding practical on our phones and in our kitchens, and its algorithms can be applied widely to an array of applications that rely on pattern recognition. Natural Language Processing (NLP) and knowledge representation and reasoning have enabled a machine to beat the Jeopardy champion and are bringing new power to Web searches. In targeted applications, substantial increases in the future uses of AI, include more self-driving cars, healthcare diagnostics and targeted treatments, and physical assistance for elder care can be expected. It has also evolved to include home service robots, which have entered people's residential homes, in the form of vacuum cleaners. The future residential home, is likely to be full of AI products. Sinta Dewi *etal* highlight how the private home can contain devices that include, but not limited to, earning thermostats, energy tracking switches, video doorbells, smart baby monitors, and app- and voice-controlled lights, shades, and speakers are all increasingly available and affordable. These connected devices use embedded sensors and the Internet to collect and communicate data with each other and their users, seamlessly integrating the physical and digital worlds inside the home. [9] However, and on the one hand, people are embracing the idea of developing a smart home because of the advantages it brings. That is, smart home technologies have enormous potential to save time, increase personal productivity, and provide a level of convenience that would have been unimaginable just five years ago. Dewi *etal,* go onto assert that it is well understood that, humans are people of habits, who create habits consciously and subconsciously. Thus, the idea of smart home devices will only enhance the habitual behavior of individuals allowing them to create whatever personal environment they wish. In other words, people may employ these devices to create more time with their family for leisure. In addition, better chips, low-cost 3D sensors, cloud-based machine learning, and advances in speech understanding will enhance future robots' services and their interactions with people.

However, in part, reconciling the information revealed in patent data, addressing issues such as existing and potential uses and impact of AI technology, (legal and regulatory questions, data protection) and ethical concerns – raises complex questions moving forward. The initial problem lies in the fact the AI has been difficult to define, even though there have been attempts. In 1985, Phillip Jackson, defined AI as "the ability of machines to do things that people would say require intelligence."[10] The phrase sometimes refers to intelligent machines themselves. Thus, artificial intelligence attempts to emulate the mental steps of human beings. [11] Such mental steps include understanding languages, responding to questions, identifying patterns, solving problems, and learning through experience. [12] Thus, the definition from 1985 falls short of what AI is today. Even the Oxford English Dictionary arguably has taken a very broad approach to defining AI. That is, artificial intelligence has been defined by the Oxford Dictionary to be 'the field of study that deals with the capacity of a machine to simulate or surpass intelligent human behavior'. [13]

The second challenge is to determine who owns the AI? Is it the individual or entity that has purchased the AI from the manufacturer or retailer the owner? This is no different from a person who purchases a motor vehicle and takes full ownership and responsibility for using the care when under their control. Under this scenario a car is registered to a legal entity or individual whereas, AI is most likely not registered to anyone or anything. Why is this so? Put simply, the registration of a motor vehicle is registered with and by the state. AI is not. The person in charge of the car (operating the vehicle) takes full responsibility. However, in determining the answer of ownership, applying the car scenario does not provide all the answers. This is because, AI is likely to be programed and have systems and platforms that interact with each other, but, manufactured by different entities. Therefore, the legal ownership and patent law will have a level a level of influence on where part of the responsibility lies. Furthermore, a self-driving car may capture personal data, whereas the current human controlled vehicle does not.

More importantly, one of the most pressing issues is the balancing act that, states and jurisdictions such as the European Union (EU) have to play in providing a conducive environment for AI to develop while protecting personal data. A further pressing issue is posed by the fact that both AI and data protection can be compromised by cybersecurity infringements. What has emerged is a tension between data protection (personal data) and AI law, policy and practical initiatives. In other words, the data protection laws and rules of the EU and other states make it difficult and impede the development of AI projects, because companies are afraid to give access to personal data. [14]

4. The Interrelationship Data Protection and Artificial Intelligence

There are proponents and opponents to the interrelationship between data protection and AI. On the one side, scholars are arguing that AI will pose the greatest threat to privacy over the Internet, and allow personal data to be misused with great effect. On the other side, there are entities that are developing technology, which aim to enhance privacy and protection of personal data over the Internet, through AI systems. Greenburg argues that privacy, in AI applications that use machine learning to "read a privacy policy it's never seen before and extract a readable summary, displayed in a graphic flow chart, of what kind of data a service collects, where that data could be sent, and whether a user can opt out of that collection or sharing". [15] Greenburg argues for the need for the issue to be fleshed out more as to what the IT does-achieves. That is, that systems are being developed to read privacy policies through machine pertaining applications. However, this does not go far enough to protecting personal data through AI systems. As noted by

Rob Sumroy and Natalie Donovan note that not all potential applications for AI use personal data, however, a significant number will and currently do. Personal data can be processed both when training an AI algorithm and when deploying the AI. AI can even determine whether information falls within the definition of personal data, as the ability of AI to recognise patterns in data, or link data sets, can potentially enable data that would not normally be considered personal data to become "identifiable". [16] At issue is the difference between AI cognitive behavior and decision making, when compared with the human approach. That is, accurate AI systems can reduce or eliminate human bias in decision-making, it is also possible that data-intensive applications are affected by potential bias, as both deterministic and machine learning AI uses data input to extract further information (analytics) or create and train ML models. [17] The Council of Europe opined that AI algorithms benefit from the allure of mathematical objectivity, which, combined with the complexity of data management and the subordinate position of those taking decisions in an organisation, can make it harder for a human decision-maker to take a decision other than the one suggested by the algorithm. Therefore, the distinction to be made is between cases where the human decision- maker has effective freedom and those where she does not. Here the Guidelines on Big Data already highlighted the importance of protecting the effective freedom of the human decision-maker. However, and on the background of the above, a further issue arises because of the fragmented approach currently taken towards regulating and defining personal data, along with the concept of consent.

Notwithstanding the above, jurisdictions have begun to consider priority areas of the policy and the law. This section provides a snap shot of what the EU, Australia and Singapore have determined as some of the issues and tension between AI and personal data. What has emerged, to date, has seen jurisdictions tackle these matters quite differently, obviously addressing their own sovereign needs. The European Commission (EC) presented in December 2018 a draft of the AI Ethics Guidelines produced by the European Commission's High-Level Expert Group on Artificial Intelligence (AI HLEG), including a set of ethical guidelines considering principles such as data protection and transparency.

The Australian Human Rights Commission is running a Human Rights & Technology project that has produced an issues paper on human rights and technology to consult on human rights based approaches to AI [18] and a white paper in conjunction with the World Economic Forum (WEF) to explore models of governance and leadership in AI in Australia. The project's final report is expected in early 2020. In its issues paper, the AHRC lists the human rights that might be affected by new technologies including the right to privacy:

"New technologies have spawned products and services that adapt to the particular preferences and other characteristics of the individuals they interact with. But this is only possible if the product or service 'understands' the individual it is relating with – something that requires the collection, storage, use and transfer of personal information.

This has created unprecedented demand for personal information – with unprecedented implications for the right to privacy. Where personal information is misused, the consequences can be grave. For example, individuals can be influenced or manipulated by targeted information on digital platforms." [19]

The most fundamental legal expressions of the right to privacy can be found in Article 13 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which both state that "No one shall be subjected to arbitrary or unlawful interference with his privacy…" and "Everyone has the right to the protection of the law against such interference or attacks." Moreover, under international human rights law, States must respect, protect and fulfill the human rights set out in treaties to which they are Parties. In the case of Article 17 of the ICCPR which 173 countries have now signed or ratified, this means that they must refrain from interfering with enjoyment of the right to privacy, protect people against privacy violations, and take positive actions to fulfil the right to privacy. However, the right is not absolute, and governments can restrict it by taking measures that are necessary to protect a legitimate public interest; for example, public order or national security. This along with the development and rise of data protection law will pose challenges to the development, deployment and application of AI, particularly as the community demands greater protection.

The AHRC and WEF acknowledge the challenges ahead and the recent scandal and controversy connected to new technologies have increased public concern regarding decision-making that uses AI, data privacy, cyber security, political influence and labour market shifts. Importantly, they reinforce the issues that are emerging in AI and personal data. That is, to date, the community, regulators and various professions has focused on the right to privacy: such as who owns, controls and exploits the personal data of individuals using AI-powered social media. Furthermore, the AHRC and WEF understand that personal data is the 'fuel' for AI. In other words, there are many similarities to a motor vehicle that requires fuel to run effectively transporting people from point A to point B. What they are saying is that, personal data is one fuel type that AI requires in order to run effectively and provide the necessary data for the future economy. The problem lies in the fact that hackers can, and have been very effective in reverse engineering algorithms, which result in individual's personal data being breach, and subsequently their privacy being infringed upon. Even those the study by AHRC and WEF has largely focused on addressing the issues associated human rights such as discrimination, it is our view that the issues raised above flow onto other areas of AI and data protection technology and the law.

Singapore have taken a slightly different approach to the other jurisdictions, calling for a more balanced approach towards AI governance. Singapore is calling for the

development of an accountability-based framework for discussing ethical, governance and consumer protection issues related to the commercial deployment of AI in a systematic and structured manner. In a services-driven economy like Singapore, AI will likely be deployed in intelligent systems that process personal data. Hence, this framework is also relevant to personal data protection. [20] Using this framework in the design of systems or processes Singapore is of the view that they can encourage data protection by design. Arguably, this approach falls within their current legal framework in relation to data protection. However, one consideration from this approach is the application of use of AI systems and the capture, use and disclosure of personal data is not necessarily going to be limited to a single nation state. To address the tension between AI and personal data, Singapore propose to incorporate decision-making and risk assessment considerations into the framework. Doing so, they believe will address the risk severity of harm to the customer. However, it would appear that further work is required to confirm what a type of risk assessment approach will be adequate to address these issues.

At issue is the extent of personal data collected, used and disclosed is far greater than any other time in history. It was no more than 2 decades ago when personal data was collected predominantly by hand written notes. The difference between the past and the current day is the same personal data that is collected such as health and medical information, has become so much more accessible in the contemporary world. The only way to reconcile this historical, now modern day tension begins with how personal data has been defined within data protection law. Even so, the question arises does the current day definition of personal data provide an adequate solution for current and future AI technology?

5. What Is Personal Data

Personal data is a recent addition to the regulatory framework. The law has had to adapt and change, along with develop a definition of personal data. However, defining personal data has not been a simple process. This section provides a comprehensive outline of the respective jurisdictions data protection and how personal data has been defined. It deliberately highlights, in detail, the varied approaches taken by the respective jurisdictions.

The Organization for Economic Co-operation and Development (OECD) defines personal data as any information related to an identified or identifiable person. This includes, but is not restricted to, a data subject's full name, address, occupation, affiliations, physical and mental health, sexual orientation, and even his or her opinions. However, the OECD is of the view that due to the new and advanced information communication technologies, intrusive devices, use of biometrics, social media, powerful search engines and transnational databases, the definition of personal data has been hard to pin down. Even so, jurisdictions have through their respective data protection laws attempted to provide a definition of personal data.

Beginning with the EU, the GDPR defines personal data to mean any information relating to an identified or identifiable natural person ('data subject') an identifiable natural person is one who can be identified, directly or indirectly. In particular, and by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

In Australia, personal data captured over the Internet has been defined as personal information. The difference in language and use of words, while it may be perceived as confusing or meaning a different thing, personal information and personal data are one in the same. The definition of personal information constitutes whether a person can be reasonably identifiable from the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not. [21] Section 6 of the Act does define what information can identify a person such as a person's full name, alias or previous name, date of birth, sex, current or last known address and driver's license. Important identifying information also includes current and last employer. Australia, has also determined that further identifying information can be a person's Tax File Number (TFN). [22] Furthermore, section 6 of the Act defines the data that is considered sensitive information,[23] which includes but not limited to racial or ethnic origin; political opinions; membership of a political association; religious beliefs or affiliations and philosophical beliefs. The collection of this sensitive data cannot be undertaken without the individual data subjects consent. Biometrics is an interesting example because the technology capturing this data can come in the form of AI. The broad approach taken by the AU arguable provides for a great deal of flexibility as to where and what personal data means. Other jurisdictions have taken a similar but more narrow approach.

The Singapore Personal Data Protection Act 2012, defines data as being true or not, about an individual who can be identified from that data; or from that data and other information to which the organization has or is likely to have access. Personal data used to identify a person or otherwise includes their full name of a person; NRIC Number or FIN (Foreign Identification Number); passport number and mobile telephone number; facial image of an individual (e.g. in a photograph or video recording); voice of an individual (e.g. in a voice recording); fingerprint; iris image and DNA profile. The definition of personal data includes many elements similar to other countries who have also defined this data as sensitive (data).

The definition or personal data or personal information in our view is far from settled. When coupled with AI technology, it is arguable whether the current definition is adequate enough. This area of the law alone requires a lot more work given the likely uncertainty over how AI technology will capture personal data in the future. A further

challenge for AI is the capture, use and disclosure of sensitive personal data such as health records. While some jurisdictions have specifically categorized sensitive personal data, other have opted to group this data with general data. When coupled with human bias and decision, along with varied approach taken the law, further work is needed to reconcile the differences. More importantly, and as highlighted above, AI algorithms can be developed to understand a definition, quite easily, where there are minimal variables. However, and while outside of the scope of this paper, the fragmented global approach to data protection law, will make this increasingly more difficult. In addition, the fragmented approach to the law in relation to consent when coupled with AI only compounds the challenges that lie ahead.

The concept of consent within data protection law underpins the definition of personal data. It is important to understand the detail of the law, because children who are the most venerable in the community will be in contact with AI and robots. The OECD Guidelines place a high level of importance on the concept of consent, and consider it to be fundamental to the lawful collection and processing of personal data. However, within the law, the concept of consent does vary.

Article 7 of the GDPR requires that consent to be freely given. [24] Moreover, Article 4.11, states that 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. [25] This takes away any ambiguity surrounding what an agreement might constitute. Next, Recital 32 requires consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data. In other words, by the data subject ticking a box that they have visited the internet website, is enough to constitute consent. It is a new process introduced by the GDPR and enables consent to be tracked, by the data subject. This places responsibility on the organization to have a system in place on their website, which will require a tick box of some description that has the user, for example 'accept all cookies, accept first party cookies or reject cookies. How can or does a robot or some other form of AI carry out this function? However, where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

Moreover, the data subject has the right to withdraw his or her consent at any time. Consent is not provided if the individual has no genuine or free choice or is unable to refuse or withdraw consent at any time. However, and within AI or a robot, the machine learning platform would need to understand this, and so too other forms of AI. It is debatable whether this technology has matured enough to undertake this task.

Nonetheless, consent should be given by a clear affirmative act. For example, the GDPR suggests that this could include ticking a box when visiting an internet website, choosing technical settings for information society services. Consent could come in the form of another statement or conduct which clearly indicates the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. It is debatable whether this would work within AI systems. Consent should cover all processing activities carried out for the same purpose or purposes. To process the data the individual 'has given consent to the processing of his or her personal data for one or more specific purposes'. Furthermore Article 9 provides that 'explicit consent' is generally required to process 'special categories' of personal data. Businesses must inform individuals about this right to withdraw consent. [25] Moreover, the idea of enabling children to provide their personal data is problematic. A person under the age of 16 who wishes to use online services, can only provide consent through one of the child's parents. [27] Children 16 years or older may give consent for processing data related to themselves. However, member states may introduce domestic laws to lower this age to not less than 13 years. [28] Age becomes problematic because many children may not understand what they are providing consent for, especially to a robot or AI. The converse argument is however that, children that are growing up with this technology may not consider it an issue and freely provide their personal data.

In Australia, consent can be expressly or inferred (implied), [29] written, verbal or silence. [30] The definition of consent constitutes an individual being adequately informed of the issues and obligations before giving consent (express or implied). [58] Consent must be current and specific, or voluntary and more importantly the person must have the capacity to understand and communicate that consent. [31] This protection ensures people who require assistance or specialist advice to provide consent, can do so. To date there is no court authority as to how far this protection extends, and how it will be determined that a person has the capacity to provide consent. Nevertheless, there are exceptions to this. APP 7.2, 7.3, 7.4 allow an organization to use or disclose personal data in direct marketing, when the organization has collected the information of the person. [32] Moreover, it is sufficient that the individual is advised and consents in broad terms. [33]

Notwithstanding the above, a data subject may withdraw their consent at any time, and this should be an easy and accessible process. Once an individual has withdrawn consent, an APP entity can no longer rely on that past consent for any future use or disclosure of the individual's personal information. Individuals should be made aware of the potential implications of withdrawing consent, such as no longer being able to access a service. [34] Therefore, the emergence of AI systems have emerged as being able to provide a data subject with a toll to consent. An organization cannot collect personal information unless that information directly relates to one or more of the organization's functions.

Personal information cannot be collected unless the person provides consent and the information is required under Australian law, a court or tribunal order. These situations would be in the public and national interest, in the same way as requiring data to be collected for the purposes of communicable disease outbreak (health purposes). The Privacy Act does not specify an age after which individuals can make their own privacy decisions. An APP entity will need to determine on a case-by-case basis whether an individual under the age of 18 has the capacity to consent. An individual under the age of 18, can have the capacity to consent when they have sufficient understanding and maturity to understand what is being proposed. In some circumstances, it may be appropriate for a parent or guardian to consent on behalf of a young person. However, if it is not practicable or reasonable for an APP entity to assess the capacity of individuals under the age of 18, the entity may presume that an individual aged 15 or over has capacity to consent, unless there is something to suggest otherwise. [35] An individual aged under 15 is presumed not to have capacity to consent in Australia.

Consent in Singapore can be obtained by an organization however they required to prove that it had obtained the consent. [36] An organization may also obtain consent verbally although it may correspondingly be more difficult for an organization to prove that it had obtained consent. For these types of situations, at a minimum, the organization should document, in some way, the consent that was provided, for example, by noting that oral consent was provided by an individual for a certain purpose. [37] In circumstances where the organization fails to inform the individual of the purposes for which data will be collected, used and disclosed, any consent provided does not amount to an actual consent. [38] To reinforce this point, the person must be informed and have provided consent for the use or disclosure of the data that has been collected in relation to them. However, the PDPA does not prescribe the precise mechanisms by which organizations should obtain consent. [39] Moreover, the PDPC notes that it is good practice to obtain consent that is in writing or recorded in a manner that is accessible for future reference.

Section 14 (1) of the PDPA states how an individual provides consent. Sections 13 to 17 of the PDPA deal with a number of issues relating to the Consent Obligation. Importantly, the PDPA does not affect existing legal or regulatory requirements that organizations have to comply with. Organizations may collect, use and disclose (as the case may be) personal data without the individuals' consent if required or authorized to do so under the PDPA or other written law, although those organizations may need to comply with other requirements of the Data Protection Provisions which are not inconsistent with its obligations under other written law. [40] In particular, an individual has not provided consent unless that individual has been notified of the purposes for which his personal data will be collected, used or disclosed and the individual has provided consent for those purposes. [41] If an organization fails to inform the individual of the purposes for which his personal data will be collected, used and disclosed, any consent given by that individual would not amount to consent under section 14 (1). Further details on the organization's obligation to notify the individual are explained in the section on the "Notification Obligation". [48]

The PDPA provides that personal data can be collected, used and disclosed without consent. [49] This would apply when the disclosure of personal data of an individual who has been dismissed, blacklisted or undergoing disciplinary proceedings for the purpose of warning others. However, the PDPA neither defines collection, use and disclosure, as specific terms. They are subjective terms to enable broad interpretation so as technology evolves collection, use and disclosure of data is likely to also evolve. In addition, section 13 (b) provides that the consent of the individual is not required in circumstances where the collection, use or disclosure of personal data is statutorily mandated or authorized. [50] Generally, collection refers to any act or set of acts through which an organization obtains control over or possession of personal data. Secondly, use refers to any act or set of acts undertaken by an organization to use the data. Notwithstanding the above, these exceptions are generally characterized by necessity, reasonableness and/or fairness. Yip argues that some of the exemptions appear to be very wide, for instance, collection *necessary* for "evaluative purposes" and where the personal data is publicly available. These exemption are likely to be left to the courts to make a final determination of when and how such exemptions will apply. Section 18 of the PDPA becomes important because it limits the purposes for which an organization may collect, use, or disclose personal data. Section 18 states that an organization may collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances. Benjamin Wong YongQuan is of the view that under the Purpose Limitation Obligation principle, if the organization has notified the individual of the purposes of the collection, use or disclosure pursuant to section 20, then the organization may only collect, use or disclose the personal data for those purposes.

Moreover, section 21 (1) of the PDPA allows an individual to request access to their personal data and information about the ways in which that personal data has been or may have been used or disclosed by the organization within a year before the date of the individual's request. An individual can submit a request to gain access to personal data about him or her, and to some or all personal data and information about the ways the personal data has been used. However, there are limitations to such a request that include, but are not limited, to an organization only providing such personal data if it is feasible for it to do so. This subjective and broad approach does provide an organization significant flexibility.

6. Conclusion

Data protection is being, and will continue to be

challenged by the rapid development, implementation and deployment of AI. However, AI, while considered a recent phenomenon, has been with us for more than two decades in various forms, and integrations. With the rise if technology and the internet, it is fair to say that the community is expecting greater protection and oversight of their personal data over the Internet. Thus, protecting personal data is, in some countries, becoming more important than ever given the speed, impact, difficulty of understanding the application of AI to the contemporary world. The resulting effect, is a significant conundrum which has heightened the importance of expanding the focus of the debate from compliance with existing laws to the need to consider other approaches to enhance the quality of data protection and effective governance in the face of AI and other emerging digital tools. This has created significant tensions between the two.

This paper has identified some of the basic, but, important tension between AI and data protection law. It has also confirmed that a dichotomy does exist in the law of data protection and AI. AI and its technology has multiple applications in various industries. However, when applying for a patent, AI doesn't come under a specific category. It will depend of the jurisdictional laws whether a patent can be assigned to AI, and principally whether that AI can be determined that it is an invention amongst other things. Nevertheless, as AI evolves and change, the likelihood that AI may be subject to legal disputes, not over whether a patent applies, but because of the infringement to other laws such as data protection law. The resultant effect, is the emergence of unpredictability and uncertainty in the law. Furthermore, identifying where ownership of AI and its technology is currently difficult to determine. It is technically complicated and when data is collected, it can sometimes be hard to know what and how that data will be used, and more importantly, for what purpose. There are also concerns in some areas that too much transparency may allow individuals to manipulate a system in areas such as fraud detection, raise security issues by making it easier to infer private information about the individuals used to train the AI model, or create commercial sensitivities such as intellectual property infringement. Therefore, a better understanding is required to determine at what stage of the AI technology chain is personal data collected, stored, used and disclosed. On the other side, this is likely to involve different stages of the AI technology chain. It is not inconceivable that the different stages of the AI technology chain may be the responsibility of different entities. However, practically one would like to think a common sense approach would apply and the person in actual control of the AI technology would be responsible for its use, and protection of personal data. Yet, this has not been reconciled by the law.

On the backdrop of the above, a significant dichotomy has emerged between the varied definition of personal data and information of the respective jurisdictions discussed in this paper. What has been demonstrated is that the current definition of personal data is unlikely to be adequate, because AI will be able to capture and use more personal data that, is otherwise not currently captured within the definition today. This will increasingly be an issue, particularly as AI is able to capture, store, use and disclose biometric data that does not fall within the definition of personal data. Furthermore, and while the concept of consent has evolved into as an important legal concept that underpins the definition of personal data, its definition and application varies greatly between data protection laws. It is argued that until such time that this area of the law is reconciled, the challenges facing personal data protection in AI algorithms and system is likely to accentuate. More pervasively, the current day data protection laws provide a definition of personal data, although this varies from jurisdiction to jurisdiction. On the other hand, there is not clear legal or other definition of AI, because of its variable status and application. It may be some time before the courts determine a clear definition, and in any case, this is likely to be undertaken on a case by case basis.

Apart from the need for any new development of AI to better consider the impact to personal data, some jurisdictions have, in part provided a level of safe guards, by requiring impact assessments to be undertaken. However, the question arises whether the current day data protection laws provide an adequate level of assessment. Are the impact assessments provided by the law sufficient enough to enable AI technology to be assessed for the capture, storage, use and disclosure or personal data? For instance, Article 35 (3) of GDPR, the DPIA shall be required, *inter alia*, in case of a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person. Accordingly, most AI systems would require a DPIA before carrying out any personal data processing. This will require a detailed [impact] assessment of AI systems, the AI technology chain purely from a data protection perspective, while having regard to the relevant security measures which are applied. However, the question arises will the impact assessment be adequate enough to determine whether AI technology, no matter where along the technology chain, will fully assess any impacts to personal data.

Australia and Singapore, have adopted varying approaches. Some have established law, policy and/or guidelines to ensure that assessments are undertaken. In Singapore, Organizations would need to conduct a risk and impact assessment to mitigate against any risk. However, there is no mention of AI, and focuses on identifying, assessing and addressing personal data protection risks based on the organisation's functions, needs and processes. Arguably, there is enough scope to include AI technology as part of this assessment. However, further work is needed to update and provide greater direction to organisations about assessing AI for data protection needs. Similarly, Australia has released the *Guide to undertaking privacy impact assessments* (PIA Guide) has been prepared by the Office of the Australian Information Commissioner (OAIC) to describe a process for undertaking a privacy impact assessment (PIA).

While the guidelines are limited in describing what constitutes and assessment, and largely provides entities with guidance of the privacy legislation, it could be improved to include AI technology. Nonetheless, under the *Privacy Act 1988* provides the Information Commissioner a power (that is exercisable by the Privacy Commissioner) to direct an agency to provide a PIA to the OAIC, if the Commissioner considers that a proposed activity or function of the agency might have a significant impact on the privacy of individuals. This includes when the agency proposes to engage in a new activity or function, or substantively change an existing activity or function, or a substantive change to the system that delivers an existing function or activity. Arguably this approach is flexible enough to include AI. Thus, further work is needed to ensure these approaches speak with each other and develop a consistent approach, as this new technology does not know national borders. It is international that, requires an international response, while balancing sovereign needs of individual countries.

Finally, and while this paper did not examine the regulatory arrangements surrounding impact assessments within data protection law, they may be able to assists. That is, impact assessments can go some way to addressing the tension, although further work is required to ensure that any assessment (s), including the law, policies or guidelines are adequately equipped to manage AI technology that is capturing and using personal data. Apart from the gaps within technology, regulators and governments; the technology sector would benefit from greater legal convergence, because the issues identified in this paper know no national boundaries, and it is fast becoming an international problem. Data protection authorities will need to maintain string vigilance in this area of the law and while some AI products are likely to be licensed for their use, further consideration will be needed to possibly licensing other products. However, this will be problematic for everyday household goods that are used in the home. Nonetheless, it could go some way to including a whole of stakeholder response when having to consider ethical and other data protection control mechanisms. Therefore, there is an urgent need for a much wider and more comprehensive study of the issues between data protection and AI – at a global level.

References

[1] Robert Walters, Leon Trakman, Bruno Zeller, Data Protection Law: Data Protection Law: A Comparative Analysis of Asia-Pacific and European Approaches, Springer (2019).

[2] Japan Times, Full text of the G20 Osaka leaders' declaration https://www.japantimes.co.jp/news/2019/06/29/national/full-text-g20-osaka-leaders-declaration/#. XTu6qWVeK8U

[3] Ibid. To further promote innovation in the digital economy, we support the sharing of good practices on effective policy and regulatory approaches and frameworks that are innovative as well as agile, flexible, and adapted to the digital era, including through the use of regulatory sandboxes. The responsible development and use of Artificial Intelligence (AI) can be a driving force to help advance the SDGs and to realize a sustainable and inclusive society. To foster public trust and confidence in AI technologies and fully realize their potential, we commit to a human-centered approach. We affirm the importance of protection of intellectual property. Along with the rapid expansion of emerging technologies including the Internet of Things (IoT), the value of an ongoing discussion on security in the digital economy is growing. We, as G20 members, affirm the need to further work on these urgent challenges.

[4] MIT Technology Review, When an AI finally kills someone, who will be responsible? Legal scholars are furiously debating which laws should apply to AI crime, https://www.technologyreview.com/s/610459/when-an-ai-finally-kills-someone-who-will-be-responsible/

[5] J. K.C. Kingston, Artificial Intelligence and Legal Liability, https://arxiv.org/pdf/1802.07782.pdf.

[6] Stanford University, One Hundred Year Study on Artificial Intelligence (AI100), (2016) https://ai100.stanford.edu/sites/g/files/sbiybj9861/f/ai_100_report_0901fnlc_single.pdf

[7] The National Science and Technology Council, The National Artificial Intelligence Research and Development Strategic Plan (2016), https://www.nitrd.gov/PUBS/national_ai_rd_strategic_plan.pdf.

[8] World Economic Forum, Artificial Intelligence Collides with Patent Law, White Paper, 2018, http://www3.weforum.org/docs/WEF_48540_WP_End_of_Innovation_Protecting_Patent_Law.pdf.

[9] Sinta Dewi Rosadi, Robert Walters, Bambang Pratama, Siti Yuniarti, Personal Data and Smart Appliances Used in the Home (forthcoming)

[10] Phillip Jackson, Introduction To Artificial Intelligence 1, Dover Publ'n, Inc., 2d ed. (1974), pp. 192-338.

[11] World Intellectual Property Organization Technology Trends, Artificial Intelligence, https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf.

[12] Greenberg, A., An AI That Reads Privacy Policies So That You Don't Have To, wired.com (2018), available at https://www.wired.com/story/polisis-ai-reads-privacy-policies-so-you-dont-have-to/.

[13] Rob Sumroy, Natalie Donovan, AI and Data Protection Balancing Tension, Slaughter and May https://www.slaughterandmay.com/media/2537572/ai-and-data-protection-balancing-tensions.pdf

[14] Council of Europe, Artificial Intelligence and Data Protection: Challenges and Possible Remedies https://rm.coe.int/artificial-intelligence-and-data-protection-challenges-and-possible-re/168091f8a6 Accurate testing of the training phase before the deployment of AI algorithms on a large scale could reveal hidden bias. Moreover, hidden bias may also involve machine-generated bias which is different from human bias. In the AI context, the assessment of potential bias can also become controversial, given the multiple variables involved and the classification of people into groups which do not necessarily correspond to the traditional discriminatory categories. Questions regarding machine bias cannot be deflected by the argument that human decisions are fallible, and that AI is a way to reduce human error.

[15] Australian Human Rights Commission, Human Rights and Technology Issues Paper, July 2018, https://tech.humanrights.gov.au/sites/default/files/2018-7/Human%20Rights%20and%20Technology%20Issues%20Paper%20FINAL.pdf

[16] Australian Human Rights Commission and World Economic Forum 2019, Artificial Intelligence: governance and leadership, White paper, January 2019, https://www.humanrights.gov.au/sites/default/files/document/publication/AHRC%20WEF%20White%20Paper%20online%20version%20FINAL.pdf. They note that the potential impact of AI, including on other human rights, goes beyond privacy. For example, AI and related technologies could: bring radical changes in how we work, with predicted large-scale job creation and destruction and new ways of working, transform decision-making that affects citizens' basic rights and interests increase our environmental impact, become so important in how we live that accessibility of that technology becomes an even more important human rights issue, have a profound impact on our democratic institutions and processes.

[17] Human Rights and Technology, Decision making and Artificial Intelligence, https://tech.humanrights.gov.au/our-work

[18] Personal Data Protection Commission Singapore, Discussion Paper on Artificial Intelligence (AI) AND Personal Data – Fostering Responsible Development and Adoption of AI, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/Discussion-Paper-on-AI-and-PD---050618.pdf.

[19] The Organization for Economic Cooperation and Development (OECD) Guideline, governing the Protection of Privacy and Transborder Flows of Personal Data' ('OECD Guidelines. The OECD member countries are: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States of America. The Commission of the European Communities takes part in the work of the OECD, http://www.oecd.org/sti/ieconomy/49710223.pdf, accessed 15 June 2018. A notable absentee from this list is Singapore.

[20] Regulation 2016/679 Of the European Parliament and the European Council, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union L 119/1, Article 4.

[21] Privacy Act 1988, section 6.

[22] Ibid. Additional categories of personal information include, Membership of a professional or trade association; Membership of a trade union; Sexual orientation or practices; Criminal record; Health information about an individual; Genetic information (that is not otherwise health information); Biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or Biometric templates.

[23] Australian Privacy Principle 3, the collection is reasonably necessary for an APP entity's functions or activity, or a listed exception applies.

[24] Personal Data Protection Act 2012, section 2.

[25] Personal Data Protection Act 2012. rganization for the Economic Co-operation and Development, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 2013. http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.ht m.

[26] EPrivacy Regulation, European Data Protection Supervisor, Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation), Article 10 and Recital 23.

[27] Ibid, Article 7. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. Notably, the word shall provide a flexible approach to whether the data subject is informed or otherwise. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract. This also includes the provision of a service, which is conditional on consent to the processing of personal data that is not necessary for the performance of that contract. iller v Procopets (2008) 24 VR 1.

[28] Office of Information Commissioner, Australian Government: Key Concepts, https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts, accessed 12 November 2018.

[29] Privacy Act 1988.

[30] Ibid. In Direct Marketing, APP 7.15 The 'reasonably expect' test is an objective test that has regard to what a reasonable person, who is properly informed, would expect in the circumstances. This is a question of fact in each individual case. It is the responsibility of the organization to be able to justify its conduct. 7.16 Factors that may be important in deciding whether an individual has a reasonable expectation that their personal information will be used or disclosed for the purpose of direct marketing include where: the individual has consented to the use or disclosure of their personal information for that purpose (see discussion in paragraph 7.23 below and Chapter B (Key concepts) for further information about the elements of consent): the organization has notified the individual that one of the purposes for which it collects the personal information is for the purpose of direct marketing under APP 5.1 (see Chapter 5 (APP 5)) the organization made the individual aware that they could request not to receive direct marketing communications from the organization, and the individual does not make such a request (see paragraph 7.21).

[31] Australian Privacy Principles, 7.2, 7.3, 7.4. Express consent is given explicitly, either orally or in writing. This could be a handwritten signature, oral statement, or use of an electronic or voice signature. Generally, it cannot be assumed a person has provided consent on the basis they did not object in the first place to allow their data to be processed or transferred to a third party. Furthermore, it will be difficult for an APP entity to establish that an individual's silence can be taken as consent.

[32] Rogers v Whitaker (1992) 175 CLR 479, 490.

[33] Office of Australian Information Commissioner, Australian Government, https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts.

[34] Australian Privacy Principles 3.

[35] Office of Information Commissioner, Australian Government: Key Concepts, https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts.

[36] Personal Data Protection Act 2012, Division 1.

[37] Wong YongQuan, B Data privacy law in Singapore: the Personal Data Protection Act 2012 International Data Privacy Law, Vol. 7, No. 4 (2017).

[38] Personal Data Protection Commission, Advisory Guidelines on Key Concepts in the Personal Data Protection Act at para 12.5.

[39] Personal Data Protection Act 2012, division 1, section 13-17.

[40] Personal Data Protection Commission, Advisory Guidelines on Key Concepts in the Personal Data Protection Act, (2017).

[41] Personal Data Protection Act 2012, section 15 and 17. In accordance with Second Schedule (collection), Third Schedule (use) and Fourth Schedule (disclosure).

[42] Yip, M Personal Data Protection Act 2012: Understanding the consent obligation, Singapore Management University (2017).

[43] Personal Data Protection Act 2012, section 13.

[44] Personal Data Protection Act 2012, section 20, Notification Obligation.

[45] Yip, M Personal Data Protection Act 2012: Understanding the consent obligation, Singapore Management University (2017). The PDPA acknowledges that certain forms of socially, morally or legally acceptable uses of personal data do not require the individual's consent.

[46] Personal Data Protection Act 2012, section 21.

[47] Personal Data Protection Act 2012, section 21 (2), Third, Fourth and Fifth Schedule provides a list of exemptions. Use of Data without consent, Disclosure of data without consent and Exemption from Access. Section 21 (3), provides circumstances in which an organization 'must not' provide personal data or other information. A provision such as is this is important for, and applies to, the protection of physical or mental health, or, reveals the identity of an individual who has provided personal data about another individual. Therefore, no data or information is to be released that is in the national interest.

[48] Data Protection Impact Assessment (DPIA) and prior consultation of the Supervisory Authority, Articles 35 and 36 of GDPR. In addition, "where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk", the data controller shall consult the relevant Data Protection Supervisory Authority under Article 36 of GDPR.

[49] Personal Data Protection Commissioner, Guide to Data Protection Impact Assessments (2017). Data protection risks are best addressed when the system or process is i) new and in the process of being designed, or ii) in the process of undergoing major changes. Introducing changes to address data protection risks after the design of a process or system has been finalised or implemented will likely lead to increased cost and effort. Some examples of when to conduct a DPIA include: creating a new system that involves the handling of personal data (e.g. new website that collects personal data); creating a new process, including manual processes, that involves the handling of personal data (e.g. receptionist collecting personal data from visitors); changing the way that existing systems or processes handle personal data (e.g. redesign of the customer registration process); and changes to the organisational structure that affecting the department handling personal data (e.g. mergers and acquisition, restructuring).

[50] Office of the Australian Information Commissioner, Guide to undertaking privacy impact assessments, https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments.