Submission for the Future Leaders Competition 2020

The human involvement and privacy breaches

The possibility to breach privacy when there is no human in the loop

Introduction

In this digital age the human right of being protected from privacy breaches become essential with an increasing importance as much as technologies revolutionary get advanced.

The privacy is[i] a fundamental right, essential to autonomy and the protection of human dignity, serving as the foundation upon which many other human rights are built. Privacy enables us to create barriers and manage boundaries to protect ourselves from unwarranted interference in our lives, which allows us to negotiate who we are and how we want to interact with the world around us. Privacy helps us establish boundaries to limit who has access to our bodies, places and things, as well as our communications and our information. The rules that protect privacy give us the ability to assert our rights in the face of significant power imbalances. [1]

Nevertheless, there is no doubt about the importance of data in our life, as Geoffrey Moore said; "*Without big data, you are blind and deaf and in the middle of a freeway*." Such level of data is the main drive for the machine learning and artificial intelligence which incorporated in our life currently was a dormant before the availability of such volume of data. The Information Commissioner's Office of the United Kingdom links the relation between big data, AI and machine learning in a way described as; *big data can be thought of as an asset that is difficult to exploit. AI can be seen as a key to unlocking the value of big data; and machine learning is one of the technical mechanisms that underpins and facilitates AI*. [2]. The data used in big data analytics may be collected via these new channels, but alternatively it may be new data produced by the analytics, rather than being consciously provided by individuals. This is explained in the taxonomy developed by the Information Accountability Foundation, which distinguishes between four types of data – provided, observed, derived and inferred [3]:

Provided data is consciously given by individuals, eg when filling in an online form

Observed data is recorded automatically, eg by online cookies or sensors or CCTV linked to facial recognition

Derived data is produced from other data in a relatively simple and straightforward fashion, eg calculating customer profitability from the number of visits to a store and items bought.

Inferred data is produced by using a more complex method of analytics to find correlations between datasets and using these to categories or profile people, eg calculating credit scores or predicting future health outcomes. Inferred data is based on probabilities and can thus be said to be less 'certain' than derived data.

Those data will be containing personal data, which is defined as any information which are related to an identified or identifiable natural person. The data subjects are identifiable if they can be directly or indirectly identified, especially by reference to an identifier such as a name, an identification number, location data, an online identifier or one of several special characteristics, which expresses the physical, physiological, genetic, mental, commercial, cultural or social identity of these natural persons. [4]

If we formulated an equation that contains those four main elements;

1- ***Data*** about human's life reaches big data level.
2- ***Artificial Intelligence*** possibilities with cognitive computing, machine learning & deep learning.
3- ***Human*** involvement level.
4- ***Privacy*** as a human right that need to be protected.

Then based on the four elements of the equation and considering that;

- The element #2 which is the (AI) become basically existed in our life and fundamentally dependent on the element #1 which is the (Data) as the primary feeder of the AI.
- The advancement of element #2 (AI) has a bidirectional relation with element #3 (Human Involvement level).

Now; do the changes in the element #3 (Human involvement level) may impact or results a breach of the element #4 which is the (Privacy)?

This paper is going to provide an analysis if a privacy breach is possible to happen when there is no human in the loop.

Privacy is a human right, and with the rise of the new emerging technologies, there must be challenges & opportunities. So The Australian Human Rights Commission (AHRC) as an independent organization works to promote human rights in Australia and internationally has started a project at the international conference in Sydney in 2018, the project is addressing how Australia responds to the challenges & opportunities comes from the emerging technologies, which is vital in shaping the (AHRC) roadmap in its Final Report, due in 2020.

The project contains two-phase of consultation, one of them has been completed and produced a paper in Dec 2019 which defines the Commission's preliminary views includes an exciting result out of the before-mentioned phase one consultation and discussions.

In-phase one; (AHRC) asked questions related to Australia's regulatory framework for new and emerging technologies, the (AHRC) received 119 written submissions from different stakeholder's civil society, academia, government, and industry stakeholders and conducted face to face roundtables with around 380 stakeholders attended in Sydney.

The (AHRC) preliminary paper about the human rights and technology [5] is an international example addressing the new technologies challenges includes the privacy subject as well as the human intervention and its relation to the AI informed decision making.

In order to assess the possibility of a privacy breach while no human in the loop, first requires defining who the human is and the level of the human involvement/participation (being in the loop & not being in the loop).

Who is the Human?

1- *Human as an end-user*; the human here is a public end-user of a product or service, and he/she is the one who is the data belongs. Those data can be consciously given by the same individual or observed and recorded automatically through sensors or CCTV linked to facial recognition.

2- *Human as a service provider in human intelligence (HI) based technologies*; like the services of camera-based assistive technologies which empower people with visual impairments to obtain more independence.

3- *Human as a Controller/ AI Designer*; the human here plays different roles includes defining how and why the data will be used, developing the software and AI centered products. And importantly, implementing & monitoring the system's full cycle starts from the processes design, coding, algorisms building, securing, testing until being operational also human here is the one who is doing the administration.

Human Involvement & Breach Risks

- The human as a public end-user of product or service is by default in the loop and cannot be utterly out-of-the-loop as this is the one who is utilizing the service and getting its benefits. And there will be human mistakes. Human error caused 90% of cyber data breaches in 2019, according to a CybSafe analysis of data from the UK Information Commissioner's Office (ICO). According to the cybersecurity awareness and data analysis firm, nine out of 10 of the 2376 cyber-breaches reported to the ICO last year were caused by mistakes made by end-users. [6]

- The human involvement in human intelligence (HI) based technologies as a service provider; as an example of using cameras for assistive purposes for people with visual impairments can be risky as they may capture objects that reveal personal information such as prescription medication or credit card numbers in the background. Since most applications share their data with third parties, such personal information can be leaked or misused by their human agents. Another major risk of using cameras is that users may share private or embarrassing information inadvertently [7].

- The human intervention in AI-informed decision making where the human roles can be the controllers and AI designers. In this regard; the (AHRC) paper has stated that stakeholders emphasized the importance of the role played by humans in overseeing, monitoring and intervening in AI-informed decision making. While the

European Commission's 'Ethics Guidelines for Trustworthy AI' refer to various levels of human involvement in AI-informed decision making [8]:

A. Human-in-the-loop; referring to the 'capability for human intervention in every decision cycle of the system (although the Guidelines also acknowledge that 'in many cases this is neither possible nor desirable').

B. Human-on-the-loop; referring to human intervention during the design phase and monitoring of the system in operation

C. Human-in-command; referring to the 'capability to oversee the overall activity of the AI system (including its broader economic, societal, legal and ethical impact) and the ability to decide when and how to use the system in any particular situation' including deciding not to use AI, establishing levels of human discretion or giving human decision makers the ability to override a decision.

The (AHRC) observes that the use of AI in decision making can increase efficiency, enable more data-driven decisions and minimize some types of human bias, but it can also lead to opaque decisions, introduce new forms of bias (or replicate old ones), and undermine human rights. The Commission considers that accountability is central to harnessing these benefits and addressing these risks [9].

This proves that; whenever the human is not the loop and either being on the loop or in command, we are evacuating more space for the AI to expand.

Let's discover where the Artificial Intelligence (AI) now and what is the next AI to be able to respond to the core question; Is it possible to breach privacy when there is no human in the loop?

The Artificial Intelligence Now & Next

Artificial Intelligence is probably the most complex and astounding creations of humanity yet. Classification of AI that is more generally used in tech parlance is the classification of the technology into Artificial Narrow Intelligence (ANI), Artificial General Intelligence (AGI), and Artificial Superintelligence (ASI): [10]

1- Artificial Narrow Intelligence (ANI)

This type of artificial intelligence represents all the existing AI, including even the most complicated and capable AI that has ever been created to date. Artificial narrow intelligence refers to AI systems that can only perform a specific task autonomously using human-like capabilities. These machines can do nothing more than what they are programmed to do, and thus have a very limited or narrow range of competencies.

2- Artificial General Intelligence (AGI)

Artificial General Intelligence is the ability of an AI agent to learn, perceive, understand, and function completely like a human being. These systems will be able to independently build multiple competencies and form connections and generalizations across domains, massively cutting down on time needed for training. This will make AI systems just as capable as humans by replicating our multi-functional capabilities.

3- Artificial Superintelligence (ASI)

The development of Artificial Superintelligence will probably mark the pinnacle of AI research, as AGI will become by far the most capable forms of intelligence on earth. ASI, in addition to replicating the multi-faceted intelligence of human beings, will be exceedingly better at everything they do because of overwhelmingly greater memory, faster data processing and analysis, and decision-making capabilities. The development of AGI and ASI will lead to a scenario most popularly referred to as the singularity.

We've merely scratched the surface of AI development makes the future even more exciting. We are now in the Artificial Narrow Intelligence (ANI) age. Even the most complex AI that uses machine learning and deep learning to teach itself falls under Artificial Narrow Intelligence. [11]

Possibility to breach the privacy when there is no human in the loop

When the human is in the loop, risks for privacy breach are very high due to the inadvertently human mistakes or intended misuse of the information by the humans. But when the human is not in the loop, that's gradually giving more space for the AI, like the levels of human involvement in AI-informed decision making, which is Human-on-the-loop & Human-in-command and both is completely different from being in the loop.

The AI is different as emerging technology almost always brings with it important privacy considerations, yet the scale and application of AI creates a unique and unprecedented environment of challenges to information privacy. In some ways, the implications of AI can be seen as an extension of those created by big data, yet AI technology brings with it not only the ability to process huge amounts of data, but also to use it to learn, develop adaptive models and make actionable predictions - much of this without transparent, explainable processes.

Much of information privacy discourse around AI has not accounted for the growing power asymmetries between institutions that accumulate data, and the individuals who generate it. Current models generally treat data as a good that can be traded, which does not fully acknowledge the difficulty for people to make decisions about their data when dealing with systems they do not understand – particularly when the system understands them well and has learnt, by way of ingesting their data, how to manipulate their preferences. Further, many adaptive algorithms used in AI change constantly, to the extent that often those who create them cannot fully explain the results they generate. Established notions of information privacy are based on the idea that humans are the primary handlers of information and were not designed to contend with the computational ability of AI that does not conform to traditional ideas of data collection and handling. The way we currently think about concepts such as informed consent, notice, and what it means to access or control personal information have never before been so fundamentally challenged as they are by AI. [12]

As artificial intelligence evolves, it magnifies the ability to use personal information in ways that can intrude on privacy interests by raising analysis of personal information to new levels of power and speed. The impact of big data is commonly described in terms of three "Vs": volume, variety, and velocity. More data makes analysis more powerful and more granular. Variety adds to this power and enables new and unanticipated inferences and predictions. And velocity facilitates analysis as well as sharing in real time. Streams of data from mobile phones and other online devices expand the volume, variety, and velocity of information about every facet of our lives and puts privacy into the spotlight as a global public policy issue. [13]

Privacy concerns are cropping up as companies feed more and more consumer and vendor data into advanced, AI-fueled algorithms to create new bits of sensitive information, unbeknownst to affected consumers and employees. This means that AI may create personal data. When it does, "it's data that has not been provided with an individual's consent or even with knowledge". [14]

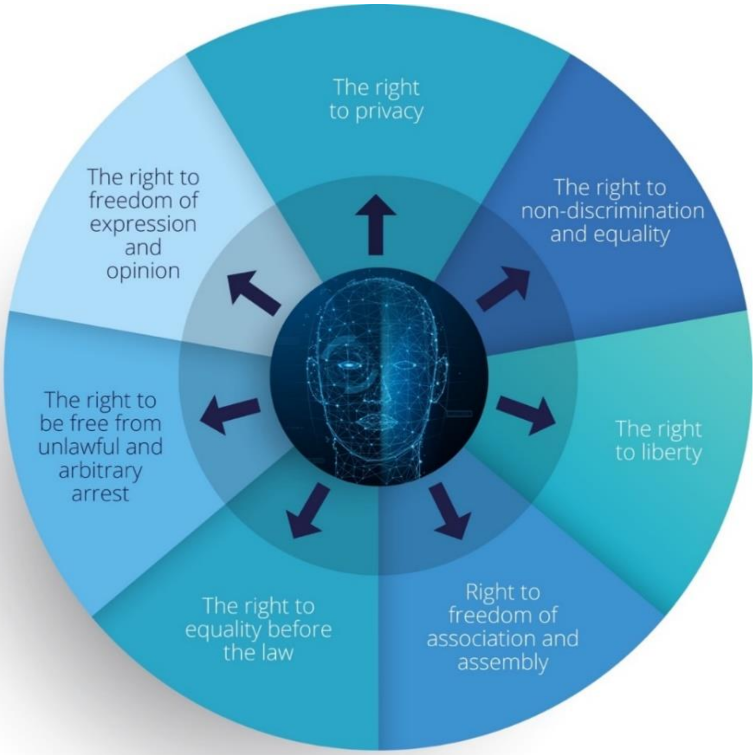
This indicates that it is possible to breach privacy when there is no human in the loop. Such a possibility is increasing by AI evolvement while being in the Artificial Narrow Intelligence (ANI) age, however we have not reached the Artificial General Intelligence (AGI) and the Artificial Superintelligence (ASI) age yet. So, policies and frameworks should cope with the evolvement to deal with such challenges.

Benefits & Challenges:

The (AHRC) observes that the use of AI in decision making can increase efficiency, enable more data-driven decisions and minimize some types of human bias, but it can also lead to opaque decisions, introduce new forms of bias (or replicate old ones), and undermine human rights.

The Commission's preliminary view in regards the application of A human rights approach; Given the pace of technological change, it will be a significant challenge to ensure that the regulatory system provides effective accountability where technology is used in ways that infringe human rights. Community trust in new and emerging technologies has been decreasing. Building confidence that our human rights are protected in this new era will be important in creating an environment that supports responsible technological innovation and the growth of Australia's digital economy. [15]

The AHRC highlighted with a practical example on a real challenge for maintaining human rights including the privacy rights; the example is referenced to the use of facial recognition by the government and non-government organization and how the human rights shown in the below figure can be protected.


The right to privacy
The right to non-discrimination and equality
The right to liberty
Right to freedom of association and assembly
The right to equality before the law
The right to be free from unlawful and arbitrary arrest
The right to freedom of expression and opinion

[16]

Biometric data that is collected from an individual in one setting and for one purpose may be collected and merged with personal data from other surveillance mechanisms such as drone footage, satellite imagery and encrypted communications. This type of surveillance will affect the right to privacy and may engage other rights such as the right to non-discrimination and the right to liberty. Where a person is under surveillance in certain contexts, they may fear potential consequences from participating in lawful democratic processes such as protests and meetings with individuals or organizations, including increased surveillance or scrutiny by police. [17]

Merged data of this kind may be used to draw inferences about an individual which are shared with third parties, without any meaningful consent from the affected individual. Sensitive personal information may be extracted or inferred from biometric identifiers, including in relation to the person’s age, race, sex and health. This can be used to undertake ‘profiling’ activity, where intrusive action is undertaken by reference to people’s age, race, sex or other characteristics.

In the context of new and emerging technologies, the traditional lines between public and private accountability are becoming increasingly difficult to navigate. Private companies are developing new forms of technology that can have significant positive and negative human rights impacts. Companies outside the technology sector, and even governments, are integrating these new developments into their products and services. Many of these new technologies rely on personal information, with large databases of personal information now held outside government, including a small number of unprecedentedly large holdings.

The challenge of assigning accountability, liability and responsibility for human rights protection in this context was identified by several stakeholders. One answer to this challenge lies in the evolution of the international framework in business and human rights. [17]

Way Forward

The Australian Human Rights Commission (AHRC) discussion paper proposed that [18]; The Australian Government should develop a National Strategy on New and Emerging Technologies. This National Strategy should:

A. Set the national aim of promoting responsible innovation and protecting human rights.
B. Priorities and resource national leadership on artificial intelligence (AI).
C. Promote effective regulation-this includes law, coregulation and self-regulation.
D. Resource education and training for government, industry and civil society.

The proposed National Strategy on New and Emerging Technologies should promote the role of ethical frameworks to complement enforceable human rights and other laws. So, proposed that the Australian Government should commission an appropriate independent body to inquire into ethical frameworks for new and emerging technologies to:

A- Assess the efficacy of existing ethical frameworks in protecting and promoting human rights
B- Identify opportunities to improve the operation of ethical frameworks, such as through consolidation or harmonization of similar frameworks, and by giving special legal status to ethical frameworks that meet certain criteria.

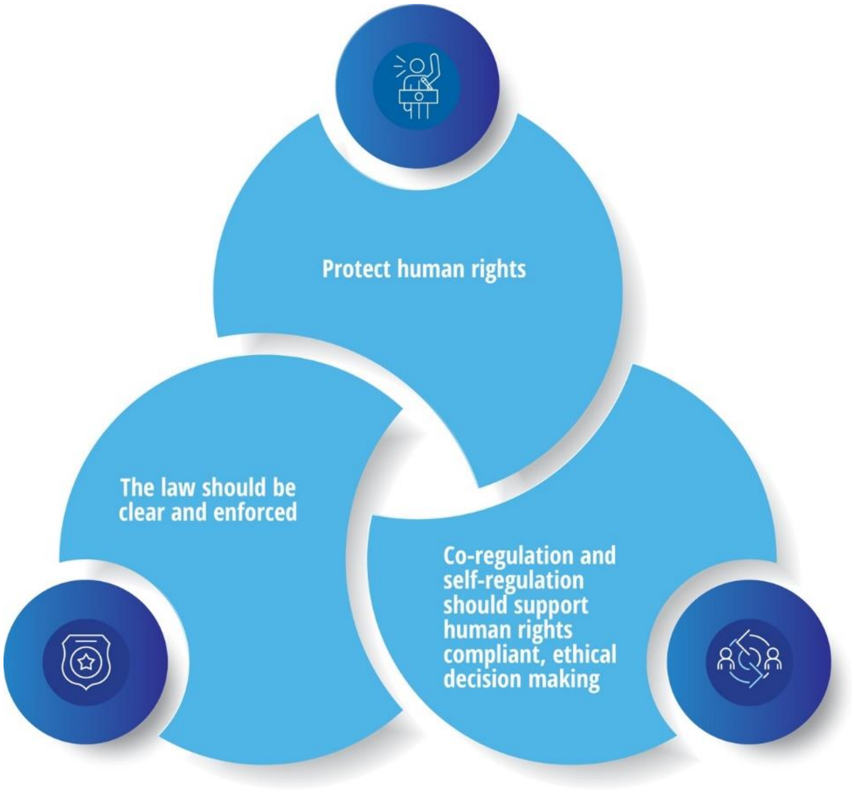
Effective national regulation should uphold and protect human rights and instill public trust about how new technologies are used in Australia.

Three key principles should apply: [19]

1. Regulation should protect human rights. All regulation should be guided by Australia's obligations under international law to protect human rights.

2. The law should be clear and enforceable. Australian law should set clear, enforceable rules regarding the design, development and use of new technologies. Our law should promote human rights and liberal democratic values. Australia's law-makers should fill any gaps necessary to achieve these regulatory aims.

3. Co-regulation and self-regulation should support human rights compliant, ethical decision making. The law is not required to address every social implication of new technologies. Good co- and self-regulation— through professional codes, design guidelines and impact assessments—can promote sound, human rights compliant development and use of new technologies.


Protect human rights
The law should be clear and enforced
Co-regulation and self-regulation should support human rights compliant, ethical decision making

[i] References

1- Privacy International Org. https://privacyinternational.org/explainer/56/what-privacy

2- The UK Information Commissioner's Office (ICO), Big Data, artificial intelligence, machine learning and data protection, 2017, p 8. https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

3- The UK Information Commissioner's Office (ICO), Big Data, artificial intelligence, machine learning and data protection, 2017, p 12. https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

4- GDPR Info. https://gdpr-info.eu/issues/personal-data/

5- The Australian Human Rights Commission (AHRC): https://humanrights.gov.au/our-work/rights-and-freedoms/publications/human-rights-and-technology-discussion-paper-2019

6- Info Security Magazine : https://www.infosecurity-magazine.com/news/90-data-breaches-human-error/

7- The USENIX Association: https://www.usenix.org/sites/default/files/soups2019posters-akter.pdf

8- The Australian Human Rights Commission (AHRC), Human Rights and Technology: Discussion Paper (2019) page 89: https://humanrights.gov.au/our-work/rights-and-freedoms/publications/human-rights-and-technology-discussion-paper-2019

9- The Australian Human Rights Commission (AHRC), Human Rights and Technology: Discussion Paper (2019) page 89 : https://humanrights.gov.au/our-work/rights-and-freedoms/publications/human-rights-and-technology-discussion-paper-2019

10- Forbes: https://www.forbes.com/sites/cognitiveworld/2019/06/19/7-types-of-artificial-intelligence/#5002496a233e

11- Forbes: https://www.forbes.com/sites/cognitiveworld/2019/06/19/7-types-of-artificial-intelligence/#5002496a233e

12- Office of the Victorian Information Commission-Artificial intelligence and privacy-Issues paper. page 7,8: https://ovic.vic.gov.au/wp-content/uploads/2018/08/AI-Issues-Paper-V1.1.pdf

13- Brookings Report on Protecting privacy in an AI-driven world: https://www.brookings.edu/research/protecting-privacy-in-an-ai-driven-world/

14- Financial Management Magazine Report on data privacy risks to consider when using AI: https://www.fm-magazine.com/issues/2020/feb/data-privacy-risks-when-using-artificial-intelligence.html

15- The Australian Human Rights Commission (AHRC), Human Rights and Technology: Discussion Paper (2019) Page 31, 89: https://humanrights.gov.au/our-work/rights-and-freedoms/publications/human-rights-and-technology-discussion-paper-2019

16- The Australian Human Rights Commission (AHRC), Human Rights and Technology: Discussion Paper (2019) Page 28: https://humanrights.gov.au/our-work/rights-and-freedoms/publications/human-rights-and-technology-discussion-paper-2019

17- The Australian Human Rights Commission (AHRC), Human Rights and Technology: Discussion Paper (2019) Page 28,30 : https://humanrights.gov.au/our-work/rights-and-freedoms/publications/human-rights-and-technology-discussion-paper-2019

[18] The Australian Human Rights Commission (AHRC), Human Rights and Technology: Discussion Paper (2019)-Executive Summary- page 6,7 : https://tech.humanrights.gov.au/sites/default/files/inline-files/TechRights2019_DiscussionPaper_Summary.pdf?_ga=2.238243136.1102338397.1598617136-2088622484.1597412703

[19] The Australian Human Rights Commission (AHRC), Human Rights and Technology: Discussion Paper (2019) Page 40: https://humanrights.gov.au/our-work/rights-and-freedoms/publications/human-rights-and-technology-discussion-paper-2019

[20] The Australian Human Rights Commission (AHRC), Human Rights and Technology: Discussion Paper (2019) Page 40: https://humanrights.gov.au/our-work/rights-and-freedoms/publications/human-rights-and-technology-discussion-paper-2019