**Date:** Friday 20 September 2019

**Venue:** Monash Conference Centre, 30 Collins St, Melbourne

**Length:** 30 minutes

Introduction

* Thank you to Moira and Monash Law School for the invitation to speak to you today.
* Acknowledgement of country:

I would like to acknowledge the Wurundjeri people of the Kulin Nation as the Traditional Custodians of the land on which we are meeting today. I would also like to pay my respects to their Elders, past and present, and the Elders from other communities who may be here with us today.

*Role of OVIC*

* For those of you not familiar with my office, OVIC was established in September 2017, combining the former Office of the Freedom of Information Commissioner and the Office of the Commissioner for Privacy and Data Protection.
* We are the primary regulator for FOI, privacy and information security in Victoria, administering both the Victorian Privacy and Data Protection Act and the Freedom of Information Act.
* As an office, our goal is to drive systemic and cultural change in the Victorian public sector in the information management space, as well as assist public sector organisations as they navigate the complex challenges of today’s digital landscape, a couple of which I will be speaking more about shortly.
* However, these challenges aren’t unique to the public sector alone – they also affect the wider community, so it’s important that we hear from the individuals and groups that also face these challenges.

*Youth Advisory Group*

* Young people are one particular stakeholder group that OVIC regularly engages with, through our Youth Advisory Group, or YAG as we like to call it.
* YAG is made up of around 12 young people aged between 15-20. The group gets together every two months to talk about privacy issues and work on projects aimed at raising privacy awareness amongst young people in Victoria. A key project that YAG assisted in was the development of a privacy postcard targeted at young people, and which was distributed to over 400 schools across Victoria.
* YAG is an important avenue through which OVIC is able to learn about young people’s perspectives on privacy, and is unique insofar as no other privacy regulators in Australia have a similar group (that we’re aware of, anyway).
* Our work with YAG has highlighted that contrary to what the popular misconception may be, young people do value and care about their privacy – but in a different way to other generations. As digital natives who have grown up with technology and online platforms, our YAG members experience privacy in different ways, and they offer a unique perspective that OVIC greatly values.
* We have some members here with us today, and they’ll be participating in panel to talk about their perspectives on privacy, which I’m sure we will all benefit from.

Context

* Data driven digital age – new and emerging technologies (e.g. AI, internet of things, wearable devices etc.) changing the way we interact, how our personal information is generated, collected and used.
* Privacy remains a key issue – GDPR, Cambridge Analytica, ACCC Report into Digital Platforms Inquiry, scrutiny into big tech practices, introduction of new privacy legislation internationally (for example, different state legislation being introduced in the US).
* Privacy regimes are therefore still important; however, we need to consider whether they are fit for purpose today in their current form – e.g. consent as one of the key tenets of privacy legislation

Limits of transactional consent model

* Need to consider whether transactional model of consent is still viable in today’s digital environment
* Challenges of consent
* Technical:
* AI developers and users don’t/can’t know how personal information will be used by an algorithm, making it difficult – if not impossible – to inform individuals;
* AI technologies able to extract meaning and draw inferences from data, therefore challenging to inform individuals of all the instances in which their information will be used;
* generation and collection of personal information is often invisible, so people don’t know when their information is being collected.
* Behavioural:
* privacy paradox – people say they care about their privacy but just give up their personal information indifferently;
* consent fatigue – people get sick of providing consent and so just accept, consent therefore not meaningful;
* difficult to quantify privacy risks and uncertainty about the nature of privacy trade-offs.
* Practical:
* Reading all the privacy policies/terms that apply is too time consuming;
* Many privacy policies are difficult to comprehend;
* With the advances in technology, often even companies collecting personal information might not know at the time of collection how or what it will be used for in the future – how can we expect individuals to consent to all possible uses of their personal information, if not even companies know all the different purposes for which it may be used in the future?
* These challenges highlight the limitations of thinking about privacy and data exchange as a transactional thing involving consent – we still assume that individuals read privacy policies and make informed and meaningful decisions about consent when in reality, this is not necessarily the case.
* Also unrealistic to expect individuals to understand complex information flows and complicated algorithms by themselves in order to make informed choices about when to provide consent – burden should not fall to individuals alone without the appropriate support mechanisms in place to facilitate the consent process.
* For example, stronger consent and notification requirements like those under the GDPR or recommended by the ACCC in its final report.
* Note the PDP Act does not set a minimum age at which an individual can make decisions about their personal information. However in terms of providing consent, whether a child (i.e. under 18) has the capacity to do so (an element of consent) depends on the individual. Need to consider whether the child has sufficient understanding and intelligence to give valid consent.
* Or should we rely on consent at all given the challenges of obtaining meaningful consent, which will only likely be further exacerbated as AI and other technologies continue to become more sophisticated.
* In many other areas of our lives regulation is there to protect us – e.g. buildings, pharmaceutical drugs are all regulated to ensure they are safe. However with privacy, a key element of our current regulatory model – consent – means that individuals have to take steps to protect themselves and their information.
* We don’t have the answers yet – but we need to have these discussions and think about alternatives or mechanisms to supplement consent so that we can continue to preserve individuals’ control over their personal information to the greatest extent possible.

Exercising privacy rights

* Given the challenges regarding consent, it may seem like exercising our privacy rights as adults – let alone children and young people – is too hard.
* However our personal information is valuable and we need to protect it; the information we give up to companies and organisations – whether on purpose or unbeknownst to us – can be used in ways that have real and significant consequences, not only on us as individuals but also society as a whole.
* Online tracking; targeted/personalised advertising – these might seem like pretty innocuous consequences of the use of our personal information, and indeed in many cases it’s very useful – think recommendations on Netflix, Spotify etc.
* However, in other cases how our personal information is used can have a more profound impact –consider the use of data analytics involving personal information for political purposes, such as micro-targeting political messages to individuals to influence them to vote a particular way. This invisible ‘behind the scenes’ use of personal information has implications for the integrity of our democratic processes, and can erode public trust in our systems, institutions, processes.
* Our personal information can also be misused to create online echo chambers – certain types of information are shown to certain individuals and groups but not others, based on discriminatory use of their personal information. This limits the possibility for meaningful public debate, freedom of thought, expression. Privacy as a gateway to these other human rights.
* Given our increasingly digital lives, governments need to take action to protect our right to privacy; however we as citizens also need to ensure we exercise our privacy rights.
* Not our responsibility alone (organisations, governments have a part) but we also have a role in protecting our privacy rights – protecting privacy is everyone’s responsibility. Need to think about the information we are providing and the impacts of our decisions, and remember the information we choose to disclose may not relate to us alone – e.g. Cambridge Analytica.
* We need to educate and inform the youth of today about these issues and how they can protect their privacy, especially given their formative years are being spent online. We need regulation and legislation, but these develop at a slow pace compared to the speed of technology. Education and awareness are important, proactive and accessible solutions.
* Educating young people early is crucial; current generation is in a unique situation as they have been exposed to technology and online services their whole lives, and view privacy differently as we will hear later in the panel.

What kind of society do we want?

* In this digital age and with the increasing pervasiveness of technologies in all facets of our personal lives, it’s crucial that we take a moment to reflect and make fundamental choices about the kind of society we want to live in.
* A key question we always need to consider when making policies and designing systems using technologies – and more broadly in general – is *‘What is the problem we are trying to solve and who are we trying to solve it for?’*
* Also need to consider whether the ‘solutions’ are proportionate; e.g. use of facial recognition, CCTV surveillance in schools – use of these technologies is becoming more common, but what problem are they actually trying to solve? Is the solution more privacy invasive than the problem itself?
* We also need to think about the effect of these technologies on a deeper level – what is the cost to us as a society from using all these technologies?
* E.g. surveillance – not just through surveillance cameras but through all the data being generated and collected about our personal lives – companies knowing when we exercise, when we sleep, where we’re going, what we watch. As this becomes more ubiquitous, do we want our children to think that constant surveillance is normal?
* Importantly, what effect is this having on children and young people’s development into adulthood? For example, if they are aware that they are being constantly surveilled and their habits and preferences tracked, will they be less inclined to express themselves, less willing to be different, less willing to challenge existing practices and orthodoxy? What about their ability to think critically? And if this is the case, what is the effect on us as a society – will we cease to move forward?
* Now that may seem a bit extreme, but consider another example: tracking. Online platforms such as Netflix and Spotify are collecting information about our preferences, and using that information to microtarget and recommend similar products and services.
* What will this kind of targeting do to children and young people’s development, if from an early age their preferences are defined and determined by existing preferences, and they only get suggestions similar to what they already like – what will this mean for their artistic expression and ability to make new discoveries about themselves? This is an important element of being a human, and for our society.
* I’m not here to say that surveillance – whether through CCTV, facial recognition, or through our lives being tracked through Internet of Things or wearable devices – is inherently bad. But it’s imperative that we stop and think: surveillance at what cost?

Conclusion

* All of these challenges and questions that I’ve raised today about the limitations of consent, misuses of personal information and the societal impact of technologies may make it seem like protecting privacy is too hard, that the erosion of privacy is inevitable.
* And yes, it may be hard – but that’s not an excuse. As regulators we have a responsibility to do the hard work of identifying these issues and helping to steer the sector in the right direction, where citizens’ information privacy is respected and where the public interest in the benefits derived from technologies is balanced against the public interest in protecting our human rights, including our right to privacy.
* Lots of legislative reform happening concerning personal information – data sharing reforms, introduction of Consumer Data Right, automated vehicles etc. Also development of ethical frameworks re AI.
* In the context of these reforms and new technologies we need to think about how we want to safeguard our personal information and how we want governments and organisations to use it.
* Need community-wide engagement to make sure community expectations of how personal information is used is considered and reflected in reform, legislation etc. Also need to engage minority groups – e.g. children, young people – in this discussion to hear about their perspectives, rather than just assume we know what they are.
* As parents, we need to take more responsibility and be more aware of what our children are consuming, what products, services, platforms they are using and what data might be potentially collected about them. Additionally, we also have a responsibility to help children and young people be more resilient in this digital age – as I mentioned earlier, education and awareness are key to achieving this.
* Finally, we also have a responsibility as individuals to defend our privacy rights – for example, by stopping to think about what information we are giving up whenever we’re asked for data, and reflecting on whether we need to give up our personal information.
* To finish, I would just like to leave you with this message: despite the challenges we face today, the erosion of privacy is not inevitable. As regulators, as parents, and as individuals, we can all take steps to protect our privacy, and we all have a responsibility to do so.
* Thank you.