An ounce of prevention is worth a pound of cure

- The norms that are set early on define the culture of a space moving forward.
- It is much easier (and cheaper) to build with privacy by design from the start than try to bolt it on later.
- As consumers become more interested in and concerned about their privacy, platforms that do not respect privacy may have a loss of adoption or loss of customers, leading to a loss in revenue.
- A lack of respect for privacy may lead to the inability to do business in other jurisdictions, stifling growth opportunities.

Privacy vs. protection

- Data protection is focused on protecting assets from unauthorized use while data privacy defines who has authorized access.
- Data protection is mostly a technical control while data privacy is more of a process.
- Data protection is the mechanism – the tools and procedures – to enforce the policy and regulation while data privacy is the regulations or policies that governs the use of data by an entity.

Why privacy?

- Privacy is a “gateway” right – it is foundational to the exercise of other fundamental human rights such as freedom of expression, thought, consciousness, belief, association and assembly, as well as the right to be free from discrimination.
- Privacy allows us to figure out who we are and provides individuals with the space to think, develop opinions and their own voice without intrusion.
- Restrictive environments on controversial issues – greater anonymity or privacy can support greater freedom of association and assembly.

Learning from other jurisdictions

United States

- No federal privacy law = fragmented patchwork of privacy laws. Compliance is difficult, costly, time consuming and confusing. Privacy laws should be written with all stakeholders and experts.
- Few privacy rights + high government surveillance = no adequacy decision from the European Union. Cost of data transfers and compliance is so high that some companies just choose not to the business in the EU at all, leading to a large loss of potential revenue.
- Cambridge Analytica – loss of customers and future and existing revenue, loss of trust and loss of future customers, fines and costly litigation, calls for more stringent privacy legislation.

Learning from other jurisdictions

European Union

- Well thought out and comprehensive legislation. However, some rules such as the cookie consent rules have led to privacy and consent fatigue where consumers no longer pay attention to what they are consenting to.
- Laws have difficulty adapting to latest technologies. Which comes first – technology or the law?

Other considerations

- Biometric data – subject to increased protections or not collected at all.
- Actions in the metaverse could reveal extremely personal information about an individual in the real world.
- Children's privacy – and parental consent;
- Health data and privacy and security;
- What rights should individuals have with regard to their privacy in the metaverse?
- Who should be able to access the metaverse?
- What happens if privacy rights and safeguards are not included?
- Cybersecurity risks and bad actors.
- Who is data shared with?

Other considerations

- Compliance with laws in all jurisdictions – compliance may need to become more standardised. Should you follow the most strict requirements?
- International norms related to privacy such as Article 17 of the International Covenant on Civil and Political Rights – compliance with the International Covenant on Civil and Political Rights.
- Impact of privacy issues to non-users;
- Augmented Reality technology and the merging of AR and VR.

Next steps

Governments and regulators

- Create proactive legislation that sufficiently covers and prepares for the privacy and security issues inherent in the metaverse.
- Legislation should be created with the help of experts and all stakeholders (including consumers).

Companies

- Go beyond legislation to build trust with consumers.
- Implement privacy by design principles.
- Perform an assessment to fully understand the privacy and security risks of operating in the metaverse.
- Build transparency and practice informed consent.

Bar associations

- Raise awareness and understanding among the legal community of emerging privacy issues with respect to the metaverse.
- Provide programming that helps the legal community advise their clients on the issues with respect to the metaverse.