SQUIRE PATTON BOGGS

No Children in the Metaverse?

The Privacy & Safety Risks of Virtual Worlds (and How to Deal with Them)

Before We Start…

SQUIRE PATTON BOGGS

- There is no universally accepted definition of Metaverse and we did not try to come up with one.
- The term was first coined from the science fiction novel *Snow Crash* written by Neal Stephenson (and depicts a wild universe).
- The Metaverse could encompass any technology described as “extended reality”, i.e., augmented reality, virtual reality and/or mixed reality. These have a similar goal in allowing users to look and move around an environment which is either enhanced or virtual.

Unique Challenges of the Metaverse

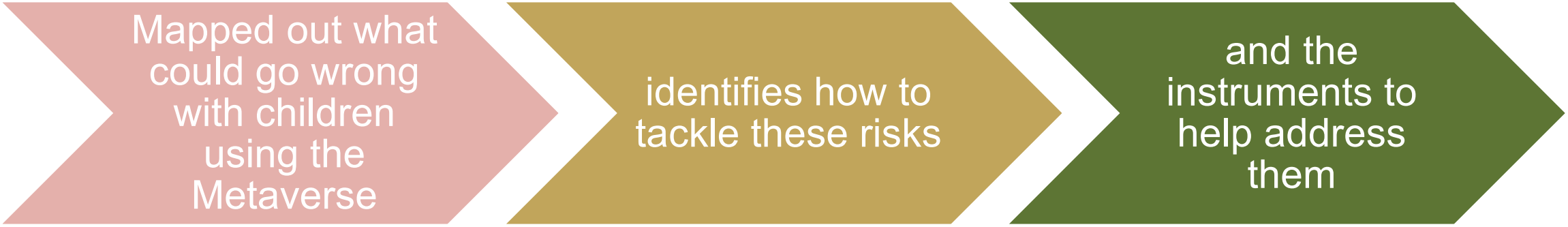
SQUIRE PATTON BOGGS

- 20 minutes of virtual reality ("VR") can generate nearly 2 million data points and unique recordings of body language such as eye gaze, gestures and facial expressions.[1]

- By 2026, around one quarter of people are predicted to spend at least one hour per day on the Metaverse.[2] Children are likely form a large component of this.

Our Paper

SQUIRE PATTON BOGGS



What Could Go Wrong?

SQUIRE PATTON BOGGS

- **Privacy - Territorial Scope**
  - The Metaverse is a global virtual world; several jurisdictional issues.
    - A Belgian child might go to a virtual concert in “Japan” and then attend a language class in “Brazil”. This will make it difficult to ascertain which data protection laws to apply and to enforce.
  - Extra-territorial effect (such as the GDPR) *versus* law of the space?

What Could Go Wrong?

SQUIRE PATTON BOGGS

- **Privacy – Legal Basis**
  - **Consent**
    - Consent for children raises specific privacy challenges. What about age verification? What about reverse-engineering? How to seek consent from the parent/person with legal responsibility.
    - Biometric data (i.e., eye movements) amounts to “special category data” under the GDPR. To process this data, companies must seek explicit consent – increased threshold.

What Could Go Wrong?

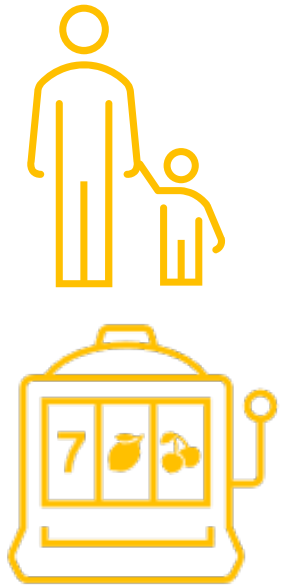
SQUIRE PATTON BOGGS

- **Privacy – Legal Basis**
  - **Necessity for the Performance of a Contract**
    - Performance of a contract is a difficult legal basis for Metaverse companies to rely on as different jurisdictions allow children to enter contracts at different ages.
  - **Legitimate interest?**
    - A more "flexible" legal basis, but to rely on it companies must put children at the forefront of legitimate interest impact assessments – this is onerous.
    - Cannot be relied on for special category data.

What Could Go Wrong?

SQUIRE PATTON BOGGS

- **Child Exploitation and Gambling**
  - Risk of sexual exploitation is one of the key dangers that children are likely to face on the Metaverse. The immersive experience of the virtual worlds is likely to increase the scope upon which child abuse activities occur, particularly solicitation and grooming.
  - Online gambling also remains a major threat to children. Children are particularly vulnerable to gambling because they are less capable of understanding costs and taking probabilities into account. They are also more susceptible to the reward stimuli that gambling provides which puts them at greater risk of developing an addiction.



What Could Go Wrong?

SQUIRE PATTON BOGGS

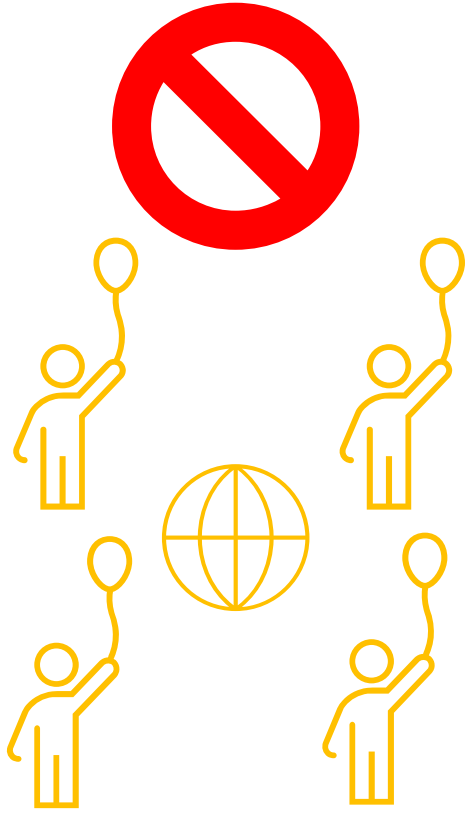
- ICO guidance on how to apply the GDPR in the context of children.[3] It maps 13 specific risks:

1. Physical harm	7. Undermining parental authority or responsibility
2. Online grooming or other sexual exploitation	8. Loss of autonomy or rights (including control over data)
3. Social anxiety, self-esteem issues, bullying or peer pressure	9. Compulsive use or attention deficit disorders
4. Access to harmful or inappropriate content	10. Excessive screen time
5. Misinformation or undue restriction on information	11. Interrupted or inadequate sleep patterns
6. Encouraging excessive risk-taking or unhealthy behaviour	12. Economic exploitation or unfair commercial pressure
13. Any other significant economic, social or developmental disadvantage	

How to Tackle Those Problems?

SQUIRE PATTON BOGGS

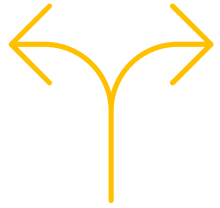
- No kids in the Metaverse at all?
  - At the most extreme end, children could be banned from the Metaverse and banned from purchasing the devices which allow them to access it. However, this risks children becoming digitally excluded (or engineer access).
- A Metaverse for kids?
  - Lower the risk of children becoming digitally excluded. Main issue comes from different jurisdictions having different views on what is appropriate. Some countries might want to create a LGBTQIA+ friendly environment for children, whilst others might be vigorously opposed to this.

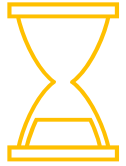


Which Instruments?

SQUIRE PATTON BOGGS

- **Horizontal Metaverse Proposal**
  - The European Commission started to think about the Metaverse more seriously. In its Work Programme for 2023 it referred to the development of *"[…] open human-centric virtual worlds, such as metaverses*." A Virtual and Augmented Reality Industrial Coalition has also been set up to develop dialogue between the European VR/AR ecosystem and policymakers.
  - However, there appears to be a divergence of approach. Thierry Breton, the Commissioner for the Internal Market has indicated that existing laws, such as the Digital Services Act, should be sufficient for now. Whilst Margrethe Vestager, the Commissioner for Competition is pushing more towards a specific regulation for the Metaverse.
  - The reality is that it is probably too early for a specific regulation given the nascent nature of the technology (and too late politically as well).





Which Instruments?

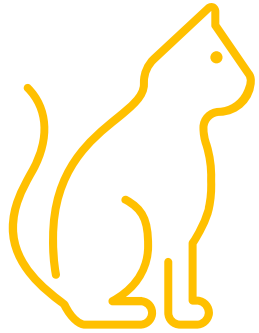
SQUIRE PATTON BOGGS

- **Consumer Laws: Labels for Hardware**
  - At the design phase of VR devices, consumer law already goes some way in protecting children. The Unfair Commercial Practices Directive 2005 ("UNPD") requires companies not to use commercial practices which distort the economic behaviour of vulnerable groups such as children. It also prohibits advertisements which are direct exhortations for children to buy products. Companies creating VR devices must ensure they do not sell in a manner which contravenes this prohibition.
  - Ideally, EU wide consumer laws would be introduced which target the risks of VR devices. For example, a law which requires the packaging of VR devices to state the quantity and type of personal data processed and the risks if it is hacked (safety approach).
  - New standards or certifications which specifically ensure that child privacy is protected when children access VR devices (standards first).

Which Instruments?

SQUIRE PATTON BOGGS

- **Design of the Metaverse for Kids**
  - The GDPR requires companies to implement "data protection by design and default". In the context of the Metaverse, this means companies must implement technical measures which limit the processing of child personal data.
  - Privacy Enhancing Technologies ("PETS"): these are technological solutions which assist companies to comply with "data protection by design and default" and could be useful for minimizing the risks to children. Options?
    - *Zero Knowledge Proofs ("ZKPs"):* this is a technological solution which would allow companies to test the age of a child (i.e., whether they are over 18) without collecting the child's precise age. This assists companies to comply with GDPR's data minimization principle as well as the security principle because the child's age does not have to be shared with 3rd parties.



Which Instruments?

- *Trusted Execution Environments ("TEEs"):* these are technological solutions which focus on data "in use", i.e., data which is being processed. This has traditionally been a security weak point and represents a challenge for Metaverse companies given the volume of child data they could process. TEEs work by segmenting the processing of personal data away from non-secure applications in an operating system. This means that certain categories of data, such as biometric data, could be more easily safeguarded against hacking.

- Digital Identities: The European Commission is working on the creation of personal digital wallets which will enable companies to securely test attributes such as age helping to prevent children from accessing inappropriate content.

Which Instruments?

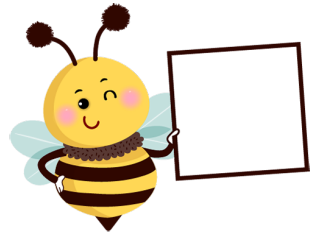
SQUIRE PATTON BOGGS

- **<u>Data Protection Impact Assessments ("DPIAs")</u>:**
  - Processing of child personal data in the contexts of marketing, profiling (including automated) and offering direct online services. Also deployment of new technology.
  - What to do? Identify the risks and mitigate. For example, a child bullied at school could be at risk of being bullied on the Metaverse (the bullies acting through online avatars). A solution to this would be a blocking feature or a "ghost" feature where child users can become invisible in the event of harassment.

Which Instruments?

SQUIRE PATTON BOGGS

- **Augmented Privacy Notice**
  - Transparency requires that users are informed about the nature of the processing of their personal data, their data subject rights and the identity of the controller (amongst other obligations). This information is usually served in a privacy notice which is available on a company's website.
  - If companies are offering services to children, then these notices must be in a language suitable for a child and formatted in an easily accessible manner. Providing information in "bite sized" chunks is a way of achieving this.
  - To engage children, the notices could be presented as a game with information provided in concise modules. Alternatively, a "privacy avatar" could inform the child of the personal data processed as they traverse the Metaverse.



Which Instruments?

SQUIRE PATTON BOGGS

- **Child Exploitation and Gambling**
  - EU law requires member states to have in place laws which tackle child pornography and child solicitation.[5] New EU regulation in motion which would require internet companies to limit the dissemination of child abuse material and report it when detected.[6]
  - Specific training or police in “virtual police stations” so that parents could report predatory behavior. As previously discussed, children could also have a “ghost” function so they disappear if receiving unwanted attention from an adult.
  - VR devices could also be designed with parental controls so that children could only access the Metaverse with a parent present. Controls could be adapted so that parents can monitor their children whilst they are on the Metaverse with this capability receding as the child becomes older.
  - For online gambling, EU or global rules should be agreed so that the Metaverse does not become a gateway to child gambling.

Questions?

Footnotes

SQUIRE PATTON BOGGS

1. Jerome, Joseph and Greenberg, Jeremy.: Augmented Reality + Virtual reality: Privacy & Autonomy Considerations in Emerging, Immersive Digital Worlds, Future of Privacy Forum, p. 16 (FPF-ARVR-Report-4.16.21-Digital.pdf)
2. Wiles, Jackie.: What is the Metaverse? And Should You Be Buying In? (https://www.gartner.com/en/articles/what-is-a-metaverse)
3. ICO.: Age appropriate design: a code of practice for online services (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/)
4. Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive (Text with EEA relevance)
5. Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA
6. Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse (Text with EEA relevance)(2022/0155 (COD))

Charles Helleputte

Partner (Brussels and Paris)

E: charles.helleputte@squirepb.com

Diletta De Cicco

Counsel (Brussels and Milan)

E: diletta.decicco@squirepb.com

James Downes

Associate (London)

E: james.downes@squirepb.com

Disclaimer

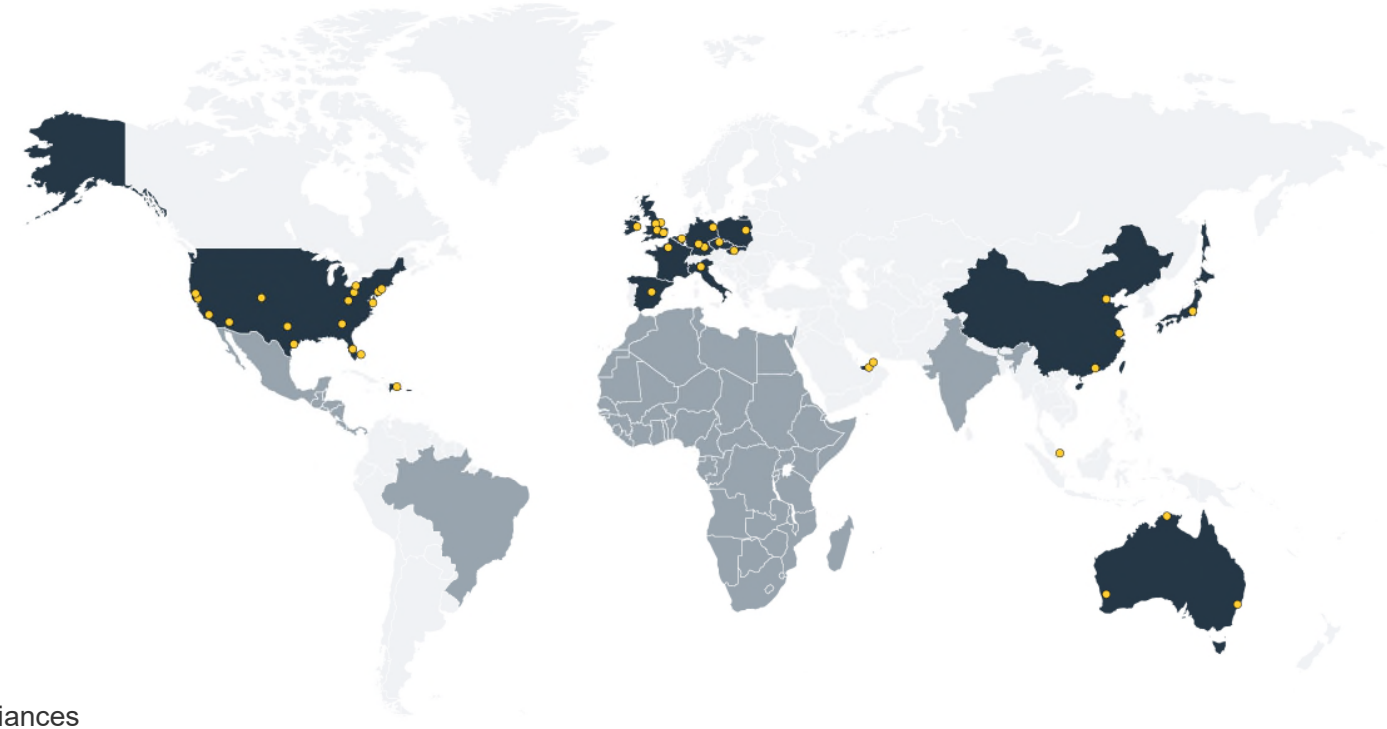
SQUIRE PATTON BOGGS

The material in this presentation is provided for informational purposes only and does not constitute legal or other professional advice. You should not and may not rely upon any information in this presentation without seeking the advice of a suitably qualified attorney who is familiar with your particular circumstances. Squire Patton Boggs assumes no responsibility for information provided in this presentation or its accuracy or completeness and disclaims all liability in respect of such information.

SQUIRE PATTON BOGGS

Abu Dhabi
Atlanta
Beijing
Berlin
Birmingham
Böblingen
Bratislava
Brussels
Cincinnati
Cleveland
Columbus
Dallas
Darwin
Denver
Dubai
Dublin
Frankfurt
Hong Kong
Houston
Leeds
London
Los Angeles
Madrid
Manchester
Miami
Milan
New Jersey
New York
Palo Alto
Paris
Perth
Phoenix
Prague
San Francisco
Santo Domingo
Shanghai
Singapore
Sydney
Tampa
Tokyo
Warsaw
Washington DC

Africa
Brazil
Caribbean/Central America
India
Israel
Mexico



Office locations

Regional desks and strategic alliances