acm Europe Technology Policy Committee

3 May 2023

COMMENTS IN RESPONSE TO
EUROPEAN COMMISSION CALL FOR EVIDENCE ON
AN EU INITIATIVE ON VIRTUAL WORLDS[1]

The Association for Computing Machinery (ACM) is the world's largest and longest established professional society of individuals involved in all aspects of computing. It annually bestows the ACM A.M. Turing Award, often popularly referred to as the "Nobel Prize of computing." ACM's Europe Technology Policy Committee ("Europe TPC") is charged with and committed to providing objective technical information to policy makers and the general public in the service of sound public policymaking. ACM and Europe TPC are non-profit, non-political, and non-lobbying organizations. Europe TPC is pleased to submit the following comments in response to the European Commission's consultation on *Virtual worlds (metaverses) – a vision for openness, safety and respect* [2] and its associated Call for Evidence, *EU initiative on virtual worlds: a head start towards the next technological transition*.[3]

The deployment of virtual worlds accessible to the wider public raises a number of important issues that must be addressed to ensure a fair, safe, and secure environment for users and a competitive environment for economic actors. Europe TPC supports the promotion of an EU virtual ecosystem based on EU values and protection of fundamental rights. Specifically, Europe TPC makes the following recommendations with respect to:

Interoperability -- The EU should ensure interoperability across virtual worlds, including of avatars, virtual objects, and virtual content. Several organizations and initiatives are already working on standards and recommendations at the European and international levels, such as the W3C, Khronos Group, MPEG expert group and the recently created Metaverse Standards Forum. These efforts should be consolidated at the level of European standard bodies, such as ETSI and CEN/CENELEC and strong incentives, perhaps even regulation, should be put forward to apply to the operators of virtual worlds.

[1] These Comments were authored for Europe TPC by Michel Beaudouin-Lafon, Vice Chair of ACM's Technology Policy Council, with the contributions of Europe TPC Chair Chris Hankin and past chairs Fabrizio Gagliardi and Oliver Grau.

[2] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13757-Virtual-worlds-metaverses-a-vision-for-openness-safety-and-respect_en

[3] See link in Note 2 above to download Commission document "Ref. Ares(2023)2474961 - 05/04/2023."

Intellectual property protection/Content creation – Virtual worlds rely on the work of creators of virtual content. The intellectual property of these content creators must be protected and portable from one virtual world to another. Current copyright law and property rights must be assessed in the context of these new environments and adapted if necessary. We note specifically that mechanisms must be devised to permit smaller businesses and self-employed content creators to retain control over their work in an environment presently dominated by large-scale content producers and aggregators. Easy access to content due to interoperability standards also increases the risk of AI-driven content generation from mined data without proper attribution or compensation to the original content providers. Since this is not a problem specific to virtual worlds, we recommend that this be addressed by the co-legislators negotiating the proposed AI Act.

Personal data protection -- Virtual worlds provide the technical capabilities to collect a large amount of personal data, data so personal that it might more accurately be called *intimate* data. Such information might include user intimate identifiers, such as: body and eye movements, facially expressed emotions, and physiological reactions (*e.g.*, galvanic skin response or even brain state tracking). While GDPR covers personal data, intimate data must be recognized as particularly sensitive and strong controls established over its collection and use. Such data should be processed locally, *i.e.,* on the end-user's device, as much as technically possible. It should not be stored in any personally identifiable way beyond the immediate effects of the user's interaction in the virtual world, such as the user's avatar mimicking their movements or facial expressions.

User safety -- Cases of harassment in virtual worlds already abound and current solutions are not satisfactory.[4] The real-time aspect of such interactions makes it impossible to interdict or moderate offensive behavior, while the power of embodiment (the user's sense that the avatar's body is its own body) makes the human behind an avatar physiologically and psychologically react to the avatar's experiences as if they are happening in the real world. Current solutions, such as activating a "protection bubble" or teleporting oneself to a "safe zone" are not satisfactory because they negatively affect the victim, not the attacker.

The legal status of avatars must therefore be clarified, *e.g.*, by making the user controlling an avatar legally responsible for the effect of its actions on other users. The status of robots, *i.e.,* avatars controlled by AIs rather than humans, must also be addressed as such robots are likely to populate virtual worlds as much as "real" avatars. Finally, impersonation poses a high risk in virtual worlds as an avatar can present itself as a person different from the person or the AI controlling it. In all three situations (offensive behavior, AI-controlled robots and impersonation), the solutions are likely to require the application of rules and laws that apply in the real world to the humans controlling avatars in virtual worlds.

[4] See, *e.g.*, "A barrage of assault, racism and rape jokes: my nightmare trip into the metaverse," *The Guardian*, 25 April 2022 [https://www.theguardian.com/tv-and-radio/2022/apr/25/a-barrage-of-assault-racism-and-jokes-my-nightmare-trip-into-the-metaverse] and "The Metaverse's Dark Side: Here Come Harassment and Assaults," *New York Times*, 30 December 2021 [https://www.nytimes.com/2021/12/30/technology/metaverse-harassment-assaults.html].

Fair competition/consumer protection -- Effective interoperability will not be sufficient to ensure a level-playing field for all actors. The cost of bringing assets into a virtual world, or transferring them from one virtual world to another, should be minimal and not discriminatory. Since most transactions in virtual worlds are done with NFTs and crypto-currencies, appropriate consumer protection against scams and the volatility of these markets will be required.

Cybersecurity -- Virtual worlds, like any digital infrastructure, are susceptible to cyber-attacks, including attacks meant to disrupt infrastructure or collect personal data. Another category of attacks, similar to those mounted against social media and networks, seeks to spread disinformation and harass individuals online. As described in the previous point, due to the power of embodiment provided by immersive virtual reality devices like head-mounted displays, the effects of these attacks on individuals are likely to be much more profound than those seen to date on social networks. Unfortunately, there is little to no available effective technical protection against these attacks, making it all the more important that a robust legal framework be put in place to deter them.

Environmental impact -- The environmental impact of immersive virtual worlds is difficult to quantify at this point. On the one hand, social and other activities that take place online can save emissions by reducing travel. On the other hand, the infrastructure that is necessary to run a virtual world at scale, which involves servers, networks, end-user devices, as well as potential reliance on energy-intensive crypto-currencies, may easily offset these savings. Possible amelioration measures might include assessing and making public the greenhouse gas emissions related to the production of the equipment and operation of virtual worlds, or certifying such virtual worlds that meet or exceed an established standard to be "green."

Conclusion

ACM's Europe Technology Policy Committee stands ready to leverage the expertise of its thousands of European members to assist the European Commission in its further consideration of these matters, or otherwise with respect to technical matters implicating any aspect of general computing and its societal impacts. To request such technical, apolitical input please contact ACM's Director of Global Policy & Public Affairs, Adam Eisgrau, at acmpo@acm.org.