EUROPE'S
VIDEO GAMES
INDUSTRY

ISFE Observations on the proposal for an AI Act

March 2022

1. The video game sector plays an important role in research into and development of Artificial intelligence (AI), and AI is used in innovative and creative ways by the industry to create new compelling experiences for players. The simulated world of video games constitutes a safe and researcher-friendly environment, as video games are seen as rich and complex, but controllable environments that allow the provision of important feedback to researchers, particularly on how to collect data to further refine research in this area. At the end of this paper we explain how AI is used in video games.

2. ISFE welcomes the risk-based approach put forward by the European Commission where regulatory burdens would be imposed only when an AI system is likely to pose high risks to fundamental rights and safety and where such uses are not covered by other existing legal frameworks, and where for other, limited low risk AI systems, limited transparency obligations would be imposed, such as to inform users when it may not be apparent that they are interacting with an AI system, but these would not apply to AI uses with no or minimal risks.

3. The type of sophisticated AI that is commonly used in video games, which are developed purely for entertainment, does not meaningfully engage anyone's human, legal or other rights[1], or safety. In video games, unlike other industries, the term AI has a traditional meaning that has been used for decades to choose behavior for computer-controlled opponents within a game. Such AI control could apply to any automated entity in a game, whether that's a direct opponent in a video game version of chess, multiple non-player characters in a story-based game, or a simulation of the behavior of everything within an entire MMO game world[2]. Entities driven by such traditional AI do not learn or adapt new behaviors, in fact their behavior is already established before the player plays the game. The Commission recognises that the regulation does not intervene in cases of AI enabled video games and spam filters as these AI systems represent only minimal or no risk for citizens' rights or safety[3]. ISFE recommends that this is clarified in the text.

4. Low-risk AI must already comply with EU legislation in the field of fundamental rights (e.g. data protection, privacy, non-discrimination, consumer protection legislation, and product safety legislation). ISFE believes this risk-based approach is justified considering the existing legislative acquis. The GDPR already imposes the obligation to inform data subjects of automated decision making and provides them with the right not to be subject to a decision based solely on automated processing if it produces legal effects on them, or similarly affects

[1] Australian Human Rights Commission's report on Human Rights and Technology, 2021
[2] MMO - Massively Multiplayer Online Games
[3] https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682

them. The GDPR also places an obligation on organisations to carry out Data Protection Impact Assessments to mitigate any high risks that AI applications may pose before such an AI application is implemented. Further, the European Commission has recently published Guidance related to the Unfair Commercial Practices Directive which addresses aggressive or misleading digital practices such as data driven practices that may distort the behaviours of consumers, paying particular attention to vulnerable consumers.

5. ISFE also welcomes the fact that the proposal suggests a framework for the creation of **voluntary codes of conduct**, which encourages providers of non-high-risk AI systems to apply voluntarily the mandatory requirements for high-risk AI systems. This proposal is more innovation-focussed than the initial proposal in the White Paper, which had suggested a labelling scheme for low-risk AI systems, intended to become binding once a developer or deployer opted in, and that would *de facto* require compliance with all the requirements foreseen for high-risk applications. Such an approach would have been disproportionate and harmful to innovation and Europe's competitiveness. Indeed, voluntary codes of conduct can form the basis of policies adopted by AI providers themselves and can be particularly helpful as such codes recognise and accommodate the varying requirements relevant to different sectors . Many video games companies have adopted, or are in the process of adopting their own internal policies or best practices around using AI to address any bias and transparency issues. For example, for example, a provider may adopt a policy that human supervision is required in case where AI decisions affect a player. Video game companies are taking these ethical challenges seriously by developing internal policies on these issues.

6. ISFE has identified **three points** in the proposed AI Act which we think should be further clarified. If not, these provisions may lead to a broad scope and application of the text which would go against the objective of addressing specific high-risk applications: (i) **the definition of an AI system**, the (ii) **definition of prohibited practices** and the (iii) **transparency obligation for other, non high-risk AI systems**.

(i) Definition of an AI system

7. The definition of an AI system as proposed in Article 3(1) is very (too) wide in its scope and, in combination with Annex 1, would seem to encompass a wide range of AI systems. Developers and businesses would face difficulties in understanding if their activities would fall within the scope of the legislation and, as drafted, may include applications not intended to be within the scope of the proposal. Considering the importance of this legislative text, and the fundamental objective of providing a secure framework for specific and clearly defined high-risk uses, the broad definition seems to clash with that objective. ISFE would also encourage collaboration with international organisations such as the OECD, CEN CENELEC (and ISO/IEC JTC1 SC42) to find consensus on what is meant by AI. These efforts should aim to find a universal understanding of AI systems, to be fed into the definition of AI system in Article 3(1) and associated provisions thus providing legal certainty and predictability.

8. Because the Commission recognises that the Regulation does not intervene in cases of AI enabled video games and spam filters as these AI systems represent only minimal or no risk for citizens' rights or safety[4], ISFE recommends that this is clarified in the text, either in the Article itself or in Recital 6.

[4] https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682

(ii) Definition of prohibited practices

9. The list of prohibited practices in Title II comprises AI systems whose use is considered unacceptable as they contravene Union values, such as violating fundamental rights. The explanatory statement suggests that *"practices that have a significant potential to manipulate persons through subliminal techniques beyond their consciousness or exploit vulnerabilities of specific vulnerable groups such as children or persons with disabilities in order to materially distort their behaviour in a manner that is likely to cause them or another person psychological or physical harm*" should be prohibited. While prohibiting certain clearly defined AI practices for reasons related to health and safety and European values, can be justified, such practices should however be defined narrowly, to ensure legal certainty and predictability and to avoid unintended consequences.

10. As regards Article 5(1)(a) and (b), several notions remain vague[5].

    a. "*Subliminal techniques*" are not defined in the proposal and should be clarified. In particular, AI technologies used in immersive video games could be prohibited under this provision, as it could be argued that every immersive video game uses subliminal techniques. ISFE considers that the threshold for what constitutes a subliminal technique should be carefully considered and defined so as to prevent low or no risk AI technologies being unintentionally caught by this provision. As suggested by the Australian Human Rights Commission's report on Human Rights and Technology, the type of sophisticated AI that is commonly used in video games, which are developed purely for entertainment, does not meaningfully engage anyone's human, legal or other rights.
    b. Furthermore, "*to materially distort their behaviours in a manner that causes or is likely to cause them psychological harm*" leaves it open to interpretation what is meant by "to materially distort" and how the connection between the use of the AI system and the change in behaviour can be properly assessed and validated. We would suggest that making the causation element subject to a reasonableness test ("*that causes or is **reasonably** likely to cause them psychological harm")* would help, however further clarity is also required.
    c. Finally, how should *"psychological harm*" and the notion of "*likely to cause"* such psychological harm be determined and validated? As an example, and in contrast, the Unfair Commercial Practices Directive provides a framework for what to "*materially distort the behaviours*" means within the scope of that directive. A similar level of clarity is not achieved in the AI proposal.

11. Article 5(1)(a) and (b) create legal uncertainty and unpredictability and could potentially be prohibitive for many users, deployers or developers of AI systems because of the unclear

[5] *The following artificial intelligence practices shall be prohibited:*
(a) the placing on the market, putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person physical or psychological harm;
(b) the placing on the market, putting into service or use of an AI system that exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm;

language. Recital 16[6] provides some guidance by including the important notion of "*intent*" as an applicable condition to Article 5(1)(a) and (b). It states that there must be an intention to materially distort the human behaviour. Nevertheless, it does not solve the issue that the connection between the use of the AI system and the change in behaviour would still need to be properly assessed and validated, as would *"psychological harm"* as discussed above.

12. The GDPR (which already imposes an obligation to inform data subjects of automated decision making and provides them with the right not to be subject to a decision based solely on automated processing, if it produces legal effects on them or similarly affects them, and under which specific safeguards as regards data processing of children apply) is effective, and additional guidance has been adopted. The GDPR also places an obligation on organisations to carry out Data Protection Impact Assessments to mitigate any high risks that AI applications may pose before such an AI application is implemented. Further, the Unfair Commercial Practices Directive Guidance now addresses data driven practices with vulnerable consumers in focus. ISFE recommends EU lawmakers to reassess Article 5(1)(a) and (b) in light of the above. If Article 5(1)(a) and (b) remain in the text, the notion of intent should be part of the Article itself to limit the current potentially very large scope, and it should be clarified that AI systems that poses low/minimal risks are not covered by the provision.

(iii) Transparency obligation

13. ISFE believes that the text must clarify that the transparency obligation in Article 52(3) to label "deep fakes" does not apply to computer generated imagery (CGI) in the context of video games. CGI is an integral part of the creative and artistic process of video game visuals and cannot be considered as "deep fakes" as defined in Article 52 (3). ISFE recommends clarifying that CGIs used in a creative and artistic endeavour are not deep fakes as defined in Article 52 (3).

14. Further, the reference to the exercise of the right to freedom of expression and the right to freedom of the arts and sciences as guaranteed in the Charter of Fundamental Rights of the EU in Article 52 (3) must be preserved.

15. The Commission recognises that the regulation does not intervene in cases where AI systems represent only minimal or no risk for citizens' rights or safety[7]. Therefore Article 52 must provide the necessary clarity for such AI uses that have been in place for decades, such as those in AI enabled video games, where such AI uses does not learn or adapt new behaviours.

16. As regards other uses of AI in the video games sector which lie outside the artistic and creative process (customer support, cheats and account abuse, gesture tracking for VR, moderation tools etc), the transparency obligation in Article 52(1), which states that providers must notify natural persons when interacting with an AI system unless it is obvious from the circumstances and the context of use, should be expanded and further explained, especially in cases of

[6] *Recital 16 The placing on the market, putting into service or use of certain AI systems intended to distort human behaviour, whereby physical or psychological harms are likely to occur, should be forbidden. Such AI systems deploy subliminal components individuals cannot perceive or exploit vulnerabilities of children and people due to their age, physical or mental incapacities. They do so with the* ***intention*** *to materially distort the behaviour of a person and in a manner that causes or is likely to cause harm to that or another person. The intention may not be presumed if the distortion of human behaviour results from factors external to the AI system which are outside of the control of the provider or the user. Research for legitimate purposes in relation to such AI systems should not be stifled by the prohibition, if such research does not amount to use of the AI system in human-machine relations that exposes natural persons to harm and such research is carried out in accordance with recognised ethical standards for scientific research*

[7] https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682

content moderation, where transparency obligations may at times conflict with effective digital safety to players.

a. First, it would be helpful if the preamble to the Regulation could set out some examples of AI systems that fall under this provision, in addition to chatbots to help explain in particular when interaction is 'obvious from the circumstances and context of use'.

b. Secondly, it would also be helpful to explain the meaning of 'interact' to help understand the intended scope of transparency requirements.

c. Thirdly, ISFE would welcome guidance on how companies should notify natural persons that they are interacting with an AI system, for example how often must providers notify natural persons – each time an AI system is used or only the first time of use? And can natural persons have the option actively to select not to be further notified once they have received the notification and confirmed they have read and understood it? It would be helpful to have further guidance on how the transparency obligations will work in practice.

About ISFE www.isfe.eu

ISFE represents the video games industry in Europe and is based in Brussels, Belgium. Our membership comprises national trade associations across Europe which represent in turn thousands of developers and publishers at national level. ISFE also has as direct members the leading European and international video game companies, many of which have studios with a strong European footprint, that produce and publish interactive entertainment and educational software for use on personal computers, game consoles, portable devices, mobile phones and tablets.

The video games sector represents one of Europe's most compelling economic success stories, relying on a strong IP framework, and is a rapidly growing segment of the creative industries. In 2020, the *size* of Europe's video games industry was €23.3 billion and registered a growth rate of 22% year on year in European key markets[8]. Today 54% of Europe's population aged 6-64 plays video games and 47% of the players are women. ISFE's purpose is to serve Europe's video games ecosystem by ensuring that the value of games is widely understood and to promote growth, skills, and innovation policies that are vital to strengthen the video games sector's contribution to Europe's digital future

[8] ISFE Key Facts 2020 from GameTrack Data by Ipsos MORI and commissioned by ISFE https://www.isfe.eu/isfe-key-facts/

AI uses in video games

<u>AI enabled video games:</u> In video games, unlike other industries, the term AI has a traditional meaning that has been used for decades to choose behavior for computer controlled opponents within a game. Such AI control could apply to any automated entity in a game, whether that's a direct opponent in a video game version of chess, multiple non-player characters in a story-based game, or a simulation of the behavior of every feature within an entire MMO game world. Entities driven by such traditional AI do not learn or adapt new behaviors, in fact their behavior is already established before the player plays the game. [9]

<u>Content creation:</u> Many video games rely on large open worlds providing spaces for players to explore. Creating such large levels and worlds is resource intensive when crafted completely by hand. Leveraging large data sets of real-world LIDAR-mapped terrain to help AI learn how to automatically create realistic and interesting terrain is an area for further research and development. The results could give artists and level designers a head start on creating the large, realistic worlds that players enjoy.

<u>Improving animation quality</u> by the use of motion and facial capture to put an actor's performance into the game. Now that hundreds of games have been made with these techniques, video game companies are experimenting with machine learning on the large volume of performance capture data collected over the years. Some studios experiment with neural networks trained on such data sets, to help create more realistic animations within games, giving a lifelike quality to their character animations.

<u>Adapt the level of the game:</u> AI can help designers find the right level of challenge for a game. Tracking the data behind how the very best players engage with games can provide machine learning insights into how automated computer players can make the game more challenging without being overly difficult. Using machine learning, personal player data can improve AI performance and provide strategy recommendations to its players on what options to next pursue within a game.

<u>Facilitate playtesting:</u> AI can also be used to learn and mimic how the average player would approach the game, allowing designers, on mobile games for example, to more rapidly playtest than before and to focus on their creative work. Analysis of gameplay data also helps match players based on non-precise location and skill in order to set up multiplayer game sessions and ensure the most competitive gaming experience for the player.

<u>Improving digital and player safety:</u> Online game environments can be comprised of many players. Protecting the safety of these players is a foundational concern for game platforms and publishers. Increasingly AI techniques are being applied to this space to complement the role of human moderators. This is to protect users of game platforms against profane and other damaging content to which they might be exposed unwittingly. Many video game companies use a web-based moderation and legal-escalation system for reactive moderation. A human moderator checks reports raised by players, reviews the evidence to see if there has been a breach of the terms of service and use and decides whether to allow or remove the content. Inside this system many companies also leverage functionality, in limited cases, which automatically applies a previously recorded human decision if the same content is reported again, e.g. 6 months later. However, this tool has a safeguard which prompts a subsequent human moderator review if there are multiple further grief reports about

[9] This type of AI often uses Finite State Machines or Behavior Trees to determine the next game move to be made by a computer, but there are many known techniques. For example, the ghosts in Pacman react to the players actions using a Finite State Machine that can be in the roam, chase or evade states. The game BioShock uses behavior trees to dictate the movement and action behavior of enemies in the 3d environment.

previously actioned content, so protecting against potentially unsound primary decisions. Many video game companies also use advanced word filtering and URL filtering tools to block damaging content. These are automated but dynamic systems which are constantly under review by human moderators and subjected to categorisation changes.

Improving integrity in play by combatting cheating, fraud and abuse: A small segment of players attempt to use cheats and exploits within games to get an advantage within the video games communities. Increasingly AI is used to detect when a player might be cheating and to make recommendations to human administrators on whether or not a player's activity should be investigated further[10]. Video game companies are developing AI to detect patterns of transactions consistent with fraudulent behaviour. For example, a player could employ market manipulation and unauthorised third-party sites which digital items can be bought and sold to gain not only an unfair advantage, but financial benefits as well.

Improving player support: As with many products and services, players sometimes call up support when something goes wrong within a game. Collecting data on these calls with their correlated resolutions provides a rich data set that AI can leverage to provide insights to improve player support[11].

Quality assurance optimisation: Video game companies are looking at using AI to make their quality assurance processes in game development more efficient, improving the gameplay experience as well as helping to keep games affordable.[12]

[10] For example, Microsoft is looking at using AI and machine learning capabilities to detect cheating in video games by isolating outliers in player progress data, rankings, etc., to determine whether or not a player should be flagged for unfair play.

[11] For example, EA's Worldwide Customer Experience player support division has experimented with using AI to classify player issues to prioritise support efforts and to help players resolve their technical issues faster.

[12] For example, Sony Interactive Entertainment is looking at using AI for automatic glitch detection in both video and audio, gameplay bug detection (e.g. where players become stuck due to non-passable terrain etc.) and for Technical Requirements Checklist ('TRC') compliance testing, a procedure used at the end of a game's development cycle to ensure that the software works correctly within the constraints of the console.