Via Electronic Filing November 21, 2022

Ms. April Tabor
Office of the Secretary
Federal Trade Commission
Suite CC-5610 (Annex B)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Commercial Surveillance ANPR, R111004

Dear Secretary Tabor:

The Entertainment Software Association ("ESA") submits these comments in response to the above-referenced Advanced Notice of Proposed Rulemaking ("ANPR") published by the Federal Trade Commission ("FTC") seeking feedback on potential regulations clarifying whether certain practices are "deceptive" or "unfair" under Section 5 of the FTC Act.[1]

ESA is the U.S. association for companies that publish computer and video games for video game consoles, handheld devices, personal computers, and the Internet. ESA's members are the innovators, creators, publishers, and business leaders who are reimagining entertainment and how consumers interact, learn, and play.[2]

ESA's members are committed to providing consumers with transparency and control over their personal information.[3] Together with its members, ESA has been at the forefront of promoting the privacy and safety of consumers, including minors, for nearly three decades. In 1994, ESA founded the Entertainment Software Rating Board ("ESRB").[4] ESRB is a non-profit, self-regulatory body that independently assigns age ratings for video games and mobile apps; educates parents about age ratings, parental controls, and privacy-related topics; enforces industry-adopted advertising guidelines; and works with major retailers to help children access appropriate content. Since 1999, ESRB has operated ESRB Privacy Certified, a compliance and certification program that helps companies in the video game and toy industries implement lawful, transparent, and responsible online privacy practices. The FTC recognized that program as one of only six Safe Harbors under the Children's Online Privacy Protection Act ("COPPA"). Over the decades, this program has evolved to reflect changes in technology, law, and best practices. Our deep and long-standing support for this program and other industry privacy

---

[1] Federal Trade Commission, *Trade Regulation Rule on Commercial Surveillance and Data Security*, Advance Notice of Proposed Rulemaking, 87 F.R. 51273 (Aug. 22, 2022).

[2] For more information on the ESA and its membership, please visit https://www.theesa.com/.

[3] Entertainment Software Association, *Privacy*, https://www.theesa.com/policy/privacy/.

[4] ESRB will separately file comments in this proceeding.

initiatives demonstrates our shared commitment to the FTC's goal of developing clear national standards to guide companies that process consumers' personal information online.

In particular, ESA supports the passage of comprehensive federal privacy legislation.[5] A federal law is preferable to the proposed rulemaking because legislation can address the full range of privacy and security issues raised by the processing of consumers' personal information. In contrast, this rulemaking is statutorily confined to identifying only those prevalent industry practices that are "deceptive" or "unfair" under Section 5 of the FTC Act.[6] This significant limitation prevents the FTC from enacting comprehensive standards and calls into question the FTC's ability to address the myriad topics raised in the ANPR.

To the extent the Commission moves forward with this rulemaking, however, ESA urges the FTC to consider not only any evidence of substantial injury resulting from the processing of consumers' personal information, but also the many significant benefits that such processing enables for consumers and competition. The FTC must focus on practices that result in concrete, objective harms such as monetary injury and unwarranted health and safety risks.[7] Speculative or subjective harm is not a cognizable injury that can support regulation.[8] Moreover, the FTC has long recognized that data processing is critical for benefiting the lives and well-being of consumers and is the fuel that fires the twin engines of innovation and competition.[9] For example, game developers depend on a variety of business models other than paid-for downloads, such as in-app purchases, in-app advertising, subscriptions, and season

---

[5] *See also* FTC, Commercial Surveillance and Data Security Rulemaking Transcript (Sept. 8, 2022), at 57 (Brandon Pugh, senior fellow and policy council at the R Street Institute: "we believe the ANPR is premature in some areas given that Congress is actively considering data privacy legislation, especially considering the ANPR seeks to answer select major policy questions that would significantly impact industry and security."); at 59 (Stephanie Joyce, senior vice president of the Computer Communication Industry Association: "The commission might be served by relying on Congress to create a statutory framework to govern these matters, rather than attempting to adopt rules out of full cloth."); at 68 (Jordan Crenshaw, Vice President of the U.S. Chamber of Commerce Technology Engagement Center: "Congress with the ascent [*sic*] of the president, not the Federal Trade Commission, is the only government entity that can mandate economy wide policies for data privacy, security and algorithms.") https://www.ftc.gov/system/files/ftc_gov/pdf/CommercialSurveillanceandDataSecurityRulemakingTranscript09.08.2022.pdf.

[6] 16 CFR § 1.8(a).

[7] Transcript, In the Matter of: Informational Injury Workshop (Dec. 12, 2017), https://www.ftc.gov/system/files/documents/public_events/1256463/informational_injury_workshop_transcript_with_index_12-2017.pdf. Careful allocation of the FTC's resources is as important as ever as the agency may no longer seek equitable monetary relief in federal court under Section 13(b) of the FTC Act.

[8] *Id.*; Federal Trade Commission, Policy Statement on Unfairness (Dec. 17, 1980), appended to *In the Matter of Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984).

[9] *See, e.g.*, Dissenting Statement of Commissioner Noah Joshua Phillips, Regarding the Commercial Surveillance and Data Security Advance Notice of Proposed Rulemaking, Aug. 11, 2022, https://www.ftc.gov/system/files/ftc_gov/pdf/Commissioner%20Phillips%20Dissent%20to%20Commercial%20Surveillance%20ANPR%2008112022.pdf; Rebecca Kelly Slaughter, Raising the Standard: Bringing Security and Transparency to the Internet of Things?, Jul. 26, 2018, at 1-2, https://www.ftc.gov/system/files/documents/public_statements/1395854/slaughter_-_raising_the_standard_-_bringing_security_and_transparency_to_the_internet_of_things_7-26.pdf.

passes, in order to enable new game developers to enter the market and provide consumers free or lower-priced access to a wider assortment of high-quality video game content. The approach of balancing consumer injury with consumer benefit and competition also is fundamental to determining whether a practice is "deceptive" or "unfair" under Section 5.[10]

Accordingly, ESA urges the FTC to ensure that any regulations that it might propose under Section 5 provide meaningful protections to the privacy and security of consumers' personal information while also facilitating the significant benefits data processing has on consumers and competition. Specifically:

- Section I of these comments requests that the FTC continue its practice of approaching Section 5 in a manner that is context-dependent and technology-neutral in order to maintain the flexibility needed to accommodate differences in data processing across different industries, to adapt to different consumers' (including parents') varied preferences and expectations, and to evolve with ever-changing technologies;

- Section II explains why *per se* bans on data processing would undermine individual choice, autonomy, and liberty contrary to the purpose of Section 5;

- Section III illustrates the significant benefits to consumers and competition that stem from the processing of personal information;

- Section IV discusses the many ways in which consumers can benefit specifically from automated decision-making; and

- Section V explains how data minimization can coexist with consumer autonomy.

I. Any Regulations Must Be Sufficiently Flexible To Account For Differences Across Industries, Consumer Preferences, and Technologies.

The ANPR asks several questions, including Questions 14, 15, 16, 18, 19, 21, and 95, about how businesses process consumers' personal information, including such information from children and teens. A core objective of these questions appears to be seeking information about ways to protect consumers from certain data processing practices. The video game industry has been committed to providing appropriate safeguards and to promoting transparency about data processing practices in our industry. ESA and its members work closely with the ESRB to provide tools to inform consumers and parents to help them

---

[10] *See, e.g.*, FTC, Policy Statement on Deception (Oct. 14, 1983), at 5 ("[A]s a matter of policy, when consumers can easily evaluate the product or service, it is inexpensive, and it is frequently purchased, the Commission will examine the practice closely before issuing a complaint based on deception. There is little incentive for sellers to misrepresent (either by an explicit false statement or a deliberate false implied statement) in these circumstances since they normally would seek to encourage repeat purchases."); *id.* (identifying factors where representations are likely material based on the likelihood of substantial concrete injury to the consumer); 15 U.S.C. § 45(n) ("The Commission shall have no authority under this section or section 57a of this title to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is ... not outweighed by countervailing benefits to consumers or to competition.").

understand and manage their interactions with their video games, consoles, and handheld devices.[11] In addition, ESA's members have been leaders in ensuring transparency in how personal information is processed for online gaming experiences and in offering tools to make informed decisions about privacy settings, including for parents to manage their child's entertainment choices and ensuring age-appropriate experiences in video games.[12] Building on this deep experience, ESA urges the FTC to ensure that any regulations remain flexible to accommodate important differences (a) across industries and contexts, (b) among consumers' preferences and reasonable expectations, and (c) in ever-evolving technologies.

A. Prescriptive Regulations Would Not Accommodate Industry- And Context-Specific Differences In How Personal Information Can Be Processed.

The FTC has long recognized that there is no "one-size-fits-all" approach to protecting personal information or providing consumers with choices over how such information is processed.[13] This fundamental principle is reflected across the patchwork of federal and state legislation recognizing that different industries and practices (even within the same industry) raise materially different risks and benefits to consumers.[14] Significantly, Section 5 also embodies this industry- and context-specific approach. For example, whether a practice is "deceptive" under Section 5 is dependent in part on who is the "reasonable" consumer under the particular circumstances, the specific format and substance of any disclosures made to the consumer, and whether the personal information at issue is particularly sensitive, which can vary by industry. Similarly, whether a practice is "unfair" under Section 5 depends in part on whether the practice is avoidable by the consumer based, for example, on whether the consumer should have choice over how the personal information is processed in that particular context. Accordingly, any regulations that the FTC proposes also must be flexible to account for significant industry- and context-specific differences.

For example, the proposed regulations should not require any ***specific*** default privacy settings, and should instead encourage businesses to use default settings ***generally*** as appropriate to the particular industry and context. Over decades, the video game industry has developed privacy settings and parental controls, including default settings, that are tailored to the video game industry and that accommodate the different contexts in which video game companies might process personal information and the different game functionality that consumers might choose whether to use. For example, the draft regulations should not require all operators to default to avoid collecting precise geolocation information. An augmented reality game might need to collect information about a person's movement or precise location to provide the service, and requiring consumers who have purchased that service to provide an additional consent imposes burdens on both the operator and the consumer. Instead, if the draft regulations encouraged data minimization settings generally, this would permit the

---

[11] *See, e.g.*, "Tools for Parents," ESRB, https://www.esrb.org/tools-for-parents/.

[12] *See, e.g.*, https://www.esrb.org/tools-for-parents/parental-controls/.

[13] Federal Trade Commission, *Internet of Things: Privacy & Security in a Connected World*, FTC Staff Report (Jan. 2015), at v, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf; Federal Trade Commission, Commission Statement Marking the FTC's 50th Data Security Settlement (Jan. 31, 2014), at 1, https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.

[14] *See, e.g.*, 42 U.S.C. §§ 1320d et seq.; 15 U.S.C. §§ 6801-6809; 18 U.S.C. §§ 2721-2725; VT. STAT. ANN. tit. 9 §§ 2430-31, 2447, 2466 (2018).

augmented reality game to collect the location data it needs while requiring a developer of a flashlight app to apply default settings that do not collect such location data.

The ESRB has launched educational initiatives on parental control features to empower consumers to control their experience with particular game content and functionality. All video games published on game consoles and sold in U.S. stores display ratings that the ESRB assigns and that disclose whether the game has features that permit, for example, location information to be visible to other users of the game or the use of user-to-user communications or web browsing. Consumers (including parents) can control which games can be accessed based on these ratings, and whether this functionality is enabled.

Prescriptive regulations that require specific defaults across all industries and technologies would be too blunt an instrument and likely to degrade and disrupt the consumers' preferred experience.[15] Instead, any proposed regulations should leave flexibility for businesses to take into account industry- and context-specific considerations when developing privacy settings (including any defaults), based, for example, on the types and sensitivity of the personal information and the particular functionality or activity at issue.

B. Any Proposed Regulations Should Provide Flexibility To Adapt To The Preferences Of Parents And Teens.

There must be a balance between providing appropriate protections for teens and not usurping parental prerogatives. The Supreme Court has held that the United States Constitution affords each parent the fundamental right "to direct the education and upbringing of one's children," and that as children get older, they should be able to exercise more autonomy.[16] Accordingly, policymakers have recognized the importance of honoring parents' choices with respect to their young children's personal information, and the rights of teens to

---

[15] Omer Tene and Jules Polonetsky, "A Theory of Creepy: Technology, Privacy, and Shifting Social Norms," Yale Journal of Law and Technology 16, no. 1 (2014): 53, at 88, https://openyls.law.yale.edu/bitstream/handle/20.500.13051/7788/Theory_of_Creepy_1.pdf?sequence=2&isAllowed=y (noting that consumers might recognize benefits from using personal information in one context while others might not in other circumstances).

[16] *Washington v. Glucksberg*, 521 U.S. 702, 720 (1997); *see also, e.g.*, *Wisconsin v. Yoder*, 406 U.S. 205, 213–14 (1972); *Pierce v. Soc'y of Sisters*, 268 U.S. 510, 534–35 (1925); *see also, e.g.*, *Meyer v. Nebraska*, 262 U.S. 390, 399–402 (1923). More recently, eight of nine Justices agreed that the Constitution protects parents' fundamental right to make decisions about their children's upbringing and education. *Troxel v. Granville*, 530 U.S. 57, 66–67 (2000) (plurality opinion); *id.* at 77 (Souter, J., concurring in judgment); *id.* at 80 (Thomas, J., concurring in judgment); *id.* at 87 (Stevens, J., dissenting); *id.* at 95 (Kennedy, J., dissenting); *Miller v. Alabama*, 567 U.S. 460, 466–67 (2012) (permissibility of life sentences for juvenile offenders); *JDB v. North Carolina*, 564 U.S. 261, 271–77 (2011) (*Miranda* inquiry); *Hazelwood Sch. Dist. v. Kuhlmeier*, 484 U.S. 260, 272 (1988) (school's ability to censor student newspaper); *Bethel Sch. Dist. No. 403 v. Fraser*, 478 U.S. 675, 683–84 (1986) (school's ability to punish obscene speech); *Kent v. United States*, 383 U.S. 541, 567, (1966) (whether minor tried as adult); *Ingraham v. Wright*, 430 U.S. 651, 662 (1977) (permissibility of corporal punishment); *see also, e.g.*, *Walker-Serrando v. Leonard*, 325 F.3d 412, 416–17 (3d Cir. 2003) (*Tinker* analysis of in-school speech); *Brandt v. Bd. of Educ. of City of Chi.*, 480 F.3d 460, 466 (7th Cir. 2007) (Posner, J.) (constitutionality of protest restrictions).

exercise these rights more directly.[17] Prescriptive regulations that impose blanket bans on data processing activities would undermine these fundamental individual rights and liberties. [18]

In lieu of blanket prohibitions on data processing activities, the regulations should take a balanced approach that appropriately considers the rights of parents, their younger children, and teens. Specifically, for children under 13 years old, parental consent should remain the touchstone for controlling the online collection, use, disclosure, and retention of personal information from children. For more than 20 years, COPPA has served parents well in affording them meaningful controls over their children's online experiences, while adapting to the development of new technologies. COPPA notably does not create a blanket ban on any particular data processing but rather creates a framework in which parents may decide what is appropriate for their particular child. Overly prescriptive regulation that instead prohibits data processing would upend COPPA's objective of keeping parents in control of their children's upbringing and bestow this power upon unelected officials.[19]

While parents of young children should have the final say over processing of their children's data, teenagers should have more autonomy to manage how their personal information is processed. Any regulations regarding specific types of processing or parental consent should not subject teens to the same restrictions imposed for children younger than 13. For example, instead of prohibiting minors from engaging with certain types of content, the regulations could focus on allowing teens to remove their online posts from public view.[20] This approach also helps diminish the risk of undermining important First Amendment principles.[21]

---

[17] *See, e.g.*, Cal. Civ. Code § 1798.120(c) (requiring parents to opt into sales of data from consumers who are younger than 13 but permitting minors between the ages of 13-16 to opt into sales of their own personal information); COLO. REV. STAT. § 6-1-1308(7), VA. CODE ANN. § 59.1-574(A)(5), CONN. GEN. STAT. ANN. § P.A. 22-15, § 6(a)(4) (requiring parental consent to process sensitive personal information of children younger than 13); Cal. Bus. & Prof. Code § 22581 (providing minors right to remove information they have posted on a website, online service, online application, or mobile application).

[18] *Wisconsin v. Yoder*, 406 U.S. 205 (1972) ("The history and culture of Western civilization reflect a strong tradition of parental concern for the nurture and upbringing of their children. This primary role of the parents in the upbringing of their children is now established beyond debate as an enduring American tradition."); *Meyer v. Nebraska*, 262 U.S. 390, 399 (1923) (stating Fourteenth Amendment right "establish a home and bring up children").

[19] We understand the Commission is concerned that there is a "lack of clarity about the workings of commercial surveillance behind the screen or display." Federal Trade Commission, *Trade Regulation Rule on Commercial Surveillance and Data Security*, Advance Notice of Proposed Rulemaking, 87 F.R. 51273 (Aug. 22, 2022). Nevertheless, the Commission should focus on appropriately tailored solutions to such concerns. A prescriptive ban is not tailored at all; it completely deprives parents of choices.

[20] Cal. Bus. & Prof. Code §§ 22580-22582.

[21] "Minors are entitled to a significant measure of First Amendment protection, and only in relatively narrow and well-defined circumstances may government bar public dissemination of public materials to them." *Brown v. Ent'm't Merchants Ass'n*, 564 U.S. 786, 794–95 (2011); *see also id.* at 795 (government's power to protect children from harm does not "include a free-floating power" to restrict ideas or images to which they may be exposed). Although the State doubtless has an interest in protecting children's privacy, that interest cannot justify such "unnecessarily broad suppression of speech directed to adults." *Reno v. ACLU*, 521 U.S. 844, 875 (1997).

ESA requests that the FTC encourage businesses to use privacy settings and controls as an alternative to outright bans on data processing. Depending on the context, this could include defaults that consumers, including teens and parents of young children, can change to accommodate their specific preferences. The FTC should avoid outright bans on data processing when there are control options that would address the concern. For example, parents can use parental controls in game systems to address concerns about how children are interacting online. ESRB also has a longstanding history of educating consumers about existing parental controls for data processing, such as controls for location sharing, targeted advertising, and spending and time limits, as well as providing step-by-step guides on how to activate these controls.[22] ESA also believes that default settings for certain activities, varying based on the context, can be useful at helping protect consumer privacy and safety. For example, some of ESA's members set spending limits to zero as the default on child accounts but permit parents to change these settings. In addition to their console-based controls, PlayStation, Nintendo, and Xbox also offer free applications or mobile-based tools that allow parents to manage gameplay. Parents can use these controls to, for example, monitor and limit time spent playing games and the types of games played as well as restrict certain gameplay features such as VR settings, voice chat, and find a friend features. Accordingly, it is unnecessary for the Commission to resort to outright bans on certain data processing activities.

In addition, any proposed regulations should not institute blanket requirements on companies to verify consumers' ages or institute different protections for younger and older teens.[23] Requiring companies to collect additional information to engage in age assurance could result in the collection of additional information the business otherwise might not need and could encourage businesses to track users across different platforms, sites, and services to ensure that they continue to apply any applicable protections for that consumer. These results are in tension with data minimization principles and would be inconsistent with the FTC's longstanding guidance.[24] Moreover, insisting on granular age bands for teens flies in the face of evidence showing their ineffectiveness; such bands would be operationally complex.

---

[22] "Parental Controls," ESRB, https://www.esrb.org/tools-for-parents/parental-controls/; "What Parents Need to Know About Privacy in Mobile Games: Five Tips for Your Parenting Toolkit," ESRB, https://www.esrb.org/blog/what-parents-need-to-know-about-privacy-in-mobile-games-five-tips-for-your-parenting-toolkit/.

[23] For example, under COPPA, websites and online services that are directed to a general audience "have no duty to investigate" age; and child-directed services may, but are not required, to do so in certain circumstances. 16 C.F.R. § 312.2; FTC, Complying with COPPA: Frequently Asked Questions (last updated July 2020), FAQs D.7, E.2 https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions. Moreover, while the California Age-Appropriate Design Code encourages operators to estimate the age of certain users, age assurance is only one alternative compliance approach and is triggered only for online services, products, and features that are "likely to be accessed by a child." Cal. Civ. Code §§ 1798.99.29-31, 1798.99.31(a)(5).

[24] Eric Goldman, *Will California Eliminate Anonymous Web Browsing?* (Jun. 2022) https://blog.ericgoldman.org/archives/2022/06/will-california-eliminate-anonymous-web-browsing-comments-on-ca-ab-2273-the-age-appropriate-design-code-act.htm; Consumer Reports, *Re: AB 2273, California Age-Appropriate Design Code (Wicks, Cunningham) – Support if amended* (Apr. 2022) https://advocacy.consumerreports.org/wp-content/uploads/2022/04/CR-letter-AB-2273-support-if-amended.pdf; Federal Trade Commission, *Start with Security* (Jun. 2015), at 2, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf ("Don't collect personal information you don't need… Hold on to information only as long as you have a legitimate business need.").

Significantly, because age verification requirements would have the effect of requiring companies to authenticate all users in order to determine which are children and teens, age assurance requirements and prescriptive age bands also are likely to result in an undue burden on adult consumers' ability to access and engage in constitutionally protected speech. For these reasons, age assurance requirements must be avoided. However, to the extent that the Commission considers age assurance requirements, they must be based on a risk-based approach. That is, any requirements should only require age assurance in contexts where data processing creates a heightened risk of harm to the consumer, and where such risks outweigh the security and privacy risks of collecting the information needed for age assurance.

C. Any Proposed Regulations Also Must Be Flexible To Avoid Becoming Stale As Technology Evolves.

As the FTC has recognized, consumers "constantly encounter new technologies."[25] In order to efficiently accommodate these rapid changes in technology, the FTC should avoid prescriptive rules that would be specific to any particular technologies. Instead, the FTC should focus on principles-based standards that can be adaptable across all technologies and keep pace with change. This approach is not only consistent with the intent and purpose of Section 5 of the FTC Act, but also is consistent with the approach many other regulators have taken.[26] Relatedly, the Commission should also not create rules that prematurely rely on technology that has yet to have been widely adopted and proven workable in the market for all companies.

II. Any Proposed Regulations Must Allow For Individual Choice, Autonomy, And Liberty.

The ANPR also asks several questions, including Questions 50 and 79, regarding how consumers should be notified about their options with respect to data processing. The FTC has long recognized that data privacy standards must "embrace the notion that transparency empowers individuals to make informed choices" and that "consumers need clarity regarding how their data is collected, used, and shared [when using goods so that they can] effectively evaluate the value of those goods for themselves."[27] This framework—which respects individual freedom and autonomy in response to transparency regarding data processing—has not only worked well for consumers, but is embodied in Section 5's "deception" and "unfairness" standards. For these reasons, any draft regulations should continue to allow for individual choice, autonomy, and liberty, rather than outright bans on data processing.

---

[25] Federal Trade Commission, *How the FTC Keeps up on technology* (Jan. 4, 2018), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2018/01/how-ftc-keeps-technology.

[26] Office of the Colorado Attorney General, Pre-Rulemaking Considerations for the Colorado Privacy Act, https://coag.gov/app/uploads/2022/04/Pre-Rulemaking-Considerations-for-the-Colorado-Privacy-Act.pdf; *Submission of Amendments to The California Privacy Rights and Enforcement Act of 2020*, Version 3, No. 19-0021, Sec. 3(C)(1) ("The rules should not unduly burden anybody from developing creative, adaptive solutions to address challenges presented by advances in technology."); California Privacy Rights Act, Preamble Section (C)(4), ("The law should adjust to technological changes…").

[27] Christine S. Wilson, A Defining Moment for Privacy: The Time is Ripe for Federal Privacy Legislation (Feb. 6, 2020), at 13, https://www.ftc.gov/system/files/documents/public_statements/1566337/commissioner_wilson_privacy_forum_speech_02-06-2020.pdf.

The video game industry's approach for providing streamlined, easy-to-understand, and actionable notice to promote parental engagement and choice is a great example of how this framework can benefit consumers in practice. The ESRB not only assigns content ratings to video games, but also provides succinct indications of whether certain online features that require data collection and processing are available in a particular game, such as sharing of location information with other users, user-to-user interactions, and unrestricted access to the Internet via a browser or search engine.[28] This approach has created an essential, go-to source of information for parents or any other consumers interested in this functionality. A June 2022 survey found that 84% of parents say they are aware of ESRB age ratings, and 74% say they check them before buying a game "every time" or "most of the time." The survey also reported that "[a] large majority of parents also find that all three parts of the rating system [i.e. rating categories, content descriptors (of certain categories of content), and interactive elements (e.g., location sharing, purchases)] are 'extremely' or 'very' important when making decisions about appropriate video games for their family."[29]

This framework also has served consumers well in understanding privacy in the context of advertising. ESA and its members are committed to ensuring that consumers have clear and accurate information about how their information is collected, used, and disclosed for purposes of advertising. With this information, millions of consumers choose every day to play advertising-supported services, such as games that provide users access with no initial fee or purchase required.

Importantly, this framework also is embodied in the statutory "deception" and "unfairness" standards. Whether a practice is "deceptive" depends in significant part on the effectiveness of the notice the business provides to the consumer.[30] And whether a misrepresentation or omission is "material" is dependent on whether it changes whether and how a reasonable consumer would ***choose*** to use the product or service.[31] Similarly, under the "unfairness" standard, a company's notice to consumers regarding the data processing choices that they provide to consumers can affect whether any substantial injury in a particular circumstance ***is avoidable***.[32]

Depriving consumers of their rights to make individualized choices about how their personal information is processed by enacting regulations that outright ban various data processing practices raises serious questions about administrative overreach and threatens

---

[28] Interactive Elements, ESRB, https://www.esrb.org/ratings-guide/.

[29] Parents Press Start to Help Pick Appropriate Video Games (Sept. 28, 2022), https://www.esrb.org/blog/parents-press-start-to-help-pick-appropriate-video-games/.

[30] Federal Trade Commission, Policy Statement on Deception (Oct. 14, 1983), appended to *In the Matter of Cliffdale Assocs., Inc.*, 103 F.T.C. 110 (1984).

[31] *Id.*

[32] Federal Trade Commission, Policy Statement on Unfairness (Dec. 17, 1980), appended to *In the Matter of Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984). The FTC has stated that harms are unavoidable when a defendant's behavior "unreasonably creates or takes advantage of an obstacle to the free exercise of consumer decisionmaking" such that it "unjustifiably hinder[s] [] free market decisions." *Id.*

consumer autonomy and liberty.[33] Accordingly, any blanket prohibitions must be limited to only extremely rare circumstances where there is substantial concrete injury that has no benefits to consumers or competition.

III. The Regulations Must Balance The Benefits Of Processing Data With Its Costs.

Several questions in the ANPR, including Questions 24, 29, and 86, ask about the costs and benefits of promulgating rules regarding the topics discussed in the ANPR. The FTC must issue rules that take into account both the costs ***and*** benefits of data processing.[34] Under Section 5, a practice is only unfair if any substantial injury it causes is not outweighed by any countervailing benefits to consumers or competition and it is unavoidable.[35] Inherent in the unfairness standard is a recognition that no practice is *per se* unfair and that, instead, a balancing test is required. As Commissioner Wilson has recognized, "[u]sing a narrowly circumscribed focus on 'data protection' could preclude an appropriate analysis of the societal costs and benefits from data processing, so it will be important to use a holistic approach."[36]

Because the costs and benefits of the collection, use, and disclosure of data are incredibly context-specific, the rules should not institute categorical bans on certain activities or deem certain conduct *per se* unfair. Instead, they should account for the nuances of data processing in particular contexts and how the processing affects the parties in each. For example, a business-to-business website that collects IP addresses only might not need to share data with a third party. However, if the regulations categorically ban sharing IP addresses, many companies might be unable to gather the information they need to protect their consumers. For example, online gaming companies might need to share IP addresses to effectively detect patterns of fraudulent conduct (e.g., that several account takeovers across online gaming platforms are originating from a single IP address). Such a gaming company also might need to engage a third party that can combine and analyze IP addresses that it observes engage in fraudulent conduct across platforms.

Some legal frameworks have balanced industry's need to process data by providing consumers with rights to control such processing. Importantly, though, no framework has provided consumers with absolute rights.[37] Before giving consumers rights with respect to their

---

[33] *See, e.g.*, Chris Jay Hoofnagle, *Federal Trade Commission: Privacy Law and Policy*, "The KidVid Controversy" (2016) at 60-66.

[34] 15 U.S.C. Sec. 57a (authorizing the FTC to prescribe "rules which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce" within the meaning of Section 5(a)(1) of the Act.)

[35] 15 U.S.C. § 45(n); Federal Trade Commission, Policy Statement on Unfairness (Dec. 17, 1980, appended to *In the Matter of Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984).

[36] Christine S. Wilson, A Defining Moment for Privacy: The Time is Ripe for Federal Privacy Legislation (Feb. 6, 2020), at 13, https://www.ftc.gov/system/files/documents/public_statements/1566337/commissioner_wilson_privacy_forum_speech_02-06-2020.pdf.

[37] For example, the EU's General Data Protection Regulation ("GDPR") and laws modeled after it in other jurisdictions require a legal justification to collect consumer data, and recognize legal bases other than a consumer's consent to do so, such as legitimate interests or necessity to enter into and/or fulfill a contract with the consumer. Similarly, while the GDPR and similar laws recognize a number of rights over

data, the FTC should consider how bad actors might abuse them.[38] In protecting against such abuse, the regulations should preserve businesses' ability to implement reasonable anti-fraud and security measures as well as to protect intellectual property and trade secrets. Every state has recognized the importance of preserving these abilities.[39] These abilities are crucial to prevent bad actors from abusing their data rights to circumvent anti-theft and security measures that protect consumers and similar controls. The regulations should preserve ESA members' ability to thwart such attempts.

IV. The Regulations Should Enable Consumers To Benefit From Automated Decision-Making Systems.[40]

The ANPR asks several questions, including Questions 57 and 61, about the benefits of automated decision making. ESA supports providing consumers with the opportunity to decide whether their personal information can be used to make automated decisions affecting them; however, ESA urges the FTC to build upon the broad consensus that such regulations should focus on those automated decisions that have a legally significant effect and that do not include any human involvement.[41] For example, Article 22 of the EU General Data Protection Regulation provides individuals the right to avoid being subject to automated decision-making, including profiling, where it "produces legal effects concerning him or her or similarly significantly affects him or her."[42] Additionally, states provide decisions to opt out of automated decision making that results in "legal or similarly significant effects."[43] This focus is consistent

---

personal data, these rights are subject to certain restrictions (*see, e.g.*, the limitations on the right to erasure in Article 17(3) GDPR).

[38] *See* Martino et al., Personal Information Leakage by Abusing the GDPR "Right of Access", USENIX (Aug. 12-13, 2019), www.usenix.org/system/files/soups2019-di_martino.pdf.

[39] *See* VA. CODE ANN. § 59.1-578(A)(4), (A)(6), (A)(7); COLO. REV. STAT. § 6-1-1304(3)(a)(IV), (a)(IX), (a)(X); Utah Code Ann. § 13-61-304(1)(d), (1)(g), (1)(h); CONN. GEN. STAT. ANN. § P.A. 22-15, § 10(a)(4), (a)(8), (a)(9); Cal. Civ. Code §§ 1798.105(d)(2), 1798.145(a)(4), (j).

[40] Furthermore, before the FTC considers rules related to automated decision-making we urge the FTC to provide greater detail regarding its core concerns, as the ANPR provides limited insight. In addition, the regulation should consider the beneficial uses of this technology; for example, the use of automated detection systems for identifying harmful content in the course of gameplay. As the FTC notes in the ANPR, Section 5 only allows remedies where the FTC can quantify financial injury or other harm. ANPR at 51280.

[41] FTC, *Big Data, A tool for Inclusion or Exclusion*, at 32, https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf ("It may be worthwhile to have human oversight of data and algorithms when big data tools are used to make important decisions"); *see, e.g.*, EU AI Act Preliminary Draft (setting forth requirements for higher risk AI applications); Press Release, *Wyden, Booker, and Clarke Introduced Algorithmic Accountability Act of 2022 To Require New Transparency and Accountability for Automated Decision Systems* (Feb. 8, 2020), https://www.wyden.senate.gov/news/press-releases/wyden-booker-and-clarke-introduce-algorithmic-accountability-act-of-2022-to-require-new-transparency-and-accountability-for-automated-decision-systems (announcing a bill to require assessments for high-risk decisions).

[42] Regulation (EU) 2016/679 (Apr. 27, 2016).

[43] *See* VA. CODE ANN. § 59.1-573(A)(5)(III); COLO. REV. STAT. § 6-1-1306(1)(a)(I)(C); CONN. GEN. STAT. ANN. § P.A. 22-15, § 4(a)(5)(C).

with important public policy goals, because without it, consumers might not be able to avail themselves of a number of socially beneficial uses of automated decisionmaking. By way of an example, automated detection efforts can help identify deepfakes used in voice chats in video games.[44] These systems will improve over time, including by developing the ability to recognize the context and meaning of text. It would be premature to stifle the development of these technologies, or limit the data on which they operate.

V. Any Data Minimization Regulations Should Not Interfere with Safety Measures, Consumer Satisfaction, and Consumer Choice.

In Question 50, the ANPR asks for input about the impact of data minimization on the services that consumers are able to access online. ESA members recognize the value of data minimization. Our members strive to minimize data processing where doing so is compatible with the purpose of the service, particularly where sensitive personal information is at issue. For example, many of our members limit their collection of biometric information consistent with applicable law unless it is necessary to provide a service. However, we would caution that too strict of a data minimization standard will inhibit companies' efforts to improve security, impede game development, and deprive consumers of choices over features and functionality that they enjoy. As discussed above, bad actors have sought to abuse the services our members offer by falsifying their identity to evade bans on their accounts or to access protected information such as trade secrets. Developers also often need personal data to analyze and detect bugs in a system, or to inform technical improvements.

In addition, overly strict data minimization standards would limit opportunities for game development and improvement, particularly for new entrants to the market. For example, for some game developers that offer free or discounted versions of their games, it would not be feasible to offer these free and discounted versions without the collection of data for activities such as advertising.[45] If the data minimization rules foreclose such offerings, developers might struggle to support their paid alternatives. This struggle might be particularly acute for new entrants to the market, who might find it difficult to convince consumers to pay to use their new products.[46] Ultimately, this would result in consumers having fewer choices of content. Too strict of a data minimization standard also might deprive consumers of the choice to engage

---

[44] FTC, *Combatting Online Harms Through Innovation: Federal Trade Commission Report to Congress* (Jun. 16, 2022), at 17, https://www.ftc.gov/system/files/ftc_gov/pdf/Combatting%20Online%20Harms%20Through%20Innovation%3B%20Federal%20Trade%20Commission%20Report%20to%20Congress.pdf.

[45] FTC, Protecting Kids from Stealth Advertising Rough Transcript (Oct. 19, 2022), at 126 https://www.ftc.gov/system/files/ftc_gov/pdf/stealth-advertising-rough-transcript.pdf ("I think one, which I have not had an opportunity to scwus [*sic.*] before is how important digital advertising is actually to our economy, to the content that provide-- that kids get to use. All of that is subsidized by the fact that you can use digital advertising to sort of-- the cost of development of the content and producing it and things like that. That wouldn't exist but for the ability to use advertising …").

[46] Kumar, Vineet. "Making 'Freemium' Work." *Harvard Business Review*, May 1, 2014, https://hbr.org/2014/05/making-freemium-work.

with personalized and dynamic experiences in video games— experiences that our members provide and that delight consumers.[47]

Accordingly, ESA respectfully requests that if the FTC issues regulations governing data minimization, the FTC allows companies to balance the principle of data minimization with the benefits of processing data for both (1) commonly accepted practices that pose minimal risk to consumers' privacy or result in countervailing benefits to consumers and competition and (2) practices that the consumer chooses.[48]

* * *

For the reasons discussed above, ESA urges the FTC to take a nuanced approach to this rulemaking, in which it recognizes that regulations governing data cannot take a one-size fits all approach. Instead, they must account for context, the current and future state of technology, as well as consumer choice and autonomy. The regulations should focus on those situations that present the greatest likelihood of concrete and substantial injury that does not have countervailing benefits for consumers or competition.

ESA appreciates the FTC's consideration of these comments, and we look forward to continuing to work with the FTC on these important issues.

Sincerely,

Michael Warnecke
Chief Counsel, Tech Policy
Entertainment Software Association

---

[47] *See, e.g.*, Aranzaes, Hugo. "Using Player-Avatar Relations to Make More Engaging and Successful Games | GamesIndustry.Biz." *GamesIndustry.Biz*, Jan. 22, 2021, https://www.gamesindustry.biz/using-player-avatar-relations-to-make-more-engaging-and-successful-games.

[48] FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (2012), at 36-45, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.