November 21, 2022

Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, District of Columbia 20580

RE: Comments of ACT | The App Association to the Federal Trade Commission on 87 FR 51273, *Trade Regulation Rule on Commercial Surveillance and Data Security*

I. Introduction and Statement of Interest

ACT | The App Association (App Association) appreciates the opportunity to submit views to the Federal Trade Commission (FTC) on whether it should implement new trade regulation rules or other regulatory alternatives concerning the ways companies collect, aggregate, protect, use, analyze, and retain consumer data, as well as transfer, share, sell, or otherwise monetize that data in ways that are unfair or deceptive.[1]

The App Association is a global trade association for small and medium-sized technology companies. Our members are entrepreneurs, innovators, and independent developers within the global app ecosystem that engage with verticals across every industry. We work with and for our members to promote a policy environment that rewards and inspires innovation while providing resources that help them raise capital, create jobs, and continue to build incredible technology. Today, the value of the ecosystem the App Association represents – which we call the app economy – is approximately $1.7 trillion and is responsible for 5.9 million American jobs, while serving as a key driver of the $8 trillion internet of things (IoT) revolution.[2] Consumer trust is fundamental for competitors in the app economy, especially for smaller firms that may not have substantial name recognition. Strong data privacy protections that meet evolving consumer expectations are a key component of developing consumer trust in tech-driven products and services. The App Association helps shape and promote privacy best practices in a variety of contexts, including for apps directed to children and digital health tools, making us well-positioned to provide insight to the FTC regarding this advance notice of proposed rulemaking (ANPR).

[1] 87 FR 51273 https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security

[2] ACT | The App Association, State of the U.S. App Economy: 2020 (7th Edition) (Apr. 2020), available at https://actonline.org/wp-content/uploads/2020-App-economy-Report.pdf

II. General Views of the App Association on the Need for a Comprehensive Cross-Sectoral Privacy Framework, and the Federal Trade Commission's Role

Protection of consumers' data and trust is of the utmost importance to the small business community. Now more than ever, the small businesses and startup innovators we represent rely on a competitive, trustworthy, and secure ecosystem to reach millions of potential users across consumer and enterprise opportunities so they can grow their businesses and create new jobs. Since 1915, the FTC has forged law through adjudicated decisions, consistently taking this action on a case-by-case basis under Section 5 of the FTC Act.[3] While the Commission is authorized to propose "rules which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce"[4] within the meaning of Section 5(a)(1) of the Act, it is far from certain that the FTC has the authority to wield broad rulemaking power.[5] The ANPR raises uncertainties as to FTC's authority to pursue such rulemaking, and appears to be inconsistent with congressional intent of the FTC Act. Section 5 is silent as to whether issuing rules and regulations fall under the purview of the FTC, and when additional powers were allocated to the Commission by amendments to Section 6, the added powers were limited to examining, reporting, and advising.[6] Further, the legislative history does not squarely support the FTC having adequate authority that could have harmful implications across the economy. The App Association strongly urges FTC to carefully consider its authority for pursuing the ANPR, and to fully resolve the many questions related to its authority in consultation with impacted stakeholders, before advancing further.

The App Association is committed to a strong FTC acting to address demonstrated consumer harms and has continuously supported FTC enforcement actions to protect consumers. The American approach to privacy is a work in progress, and the App Association agrees that the time for changes to the U.S. approach to privacy regulation has arrived. Federal sector-specific regulation of privacy, along with a patchwork of state-level laws and regulations, presents a challenging scenario for a small business innovator. The App Association is supportive of a new federal privacy framework that will clarify the obligations of our members and pre-empts the fractured state-by-state privacy compliance environment, and generally urges that the U.S. approach to privacy provide robust privacy protections that correspond to Americans' expectations, as well as leverage competition and innovation. We urge FTC to carefully consider whether its ANPR, while well-intentioned, could derail increasingly promising efforts by Congress to

[3] Federal Trade Commission Act § 5, 38 Stat. at 719-21; and 15 U.S.C. § 45 (2018).

[4] 15 U.S.C. Sec. 57a (2028).

[5] 87 FR 51273; Federal Trade Commission Act Pub. L. No. 63-203, § 6(g), 38 Stat. 717, 722 (1914).

[6] 15 U.S.C. § 46 (2018).

advance a new cross-sectoral privacy framework.[7] The App Association recommends that the FTC instead consider providing guidance, which it has the ability under its existing authority to, on consumer privacy while Congress' work on new legislation continues.

The recent settlement between FTC and fertility and period tracking app Flo is indicative of the FTC's limitations, as well as the need for federal legislation to address privacy risks, especially within the health sector. The FTC's complaint alleges that Flo shared the "health information of users with outside data analytics providers after promising that such information would be kept private."[8] According to FTC, not only did Flo mislead consumers about its data sharing practices, but it also allowed third parties to use the data it shared for their own purposes.[9] In some cases, this occurred in violation of the terms of service of those third parties, the data having been shared via software development kits (SDKs) they provided to Flo.[10] A federal law more intentionally focused on curbing privacy harms should empower consumers to exert more control over their sensitive personal information, including the rights to access, correction, and deletion of such information. Sensitive personal information should also be subject to some flexible limits on processing activities that pose too great a risk to consumers. Although Flo's core deceptive statements in this case enabled the FTC to enjoin further harmful conduct, the recurrence of these privacy harms involving health information highlight the need for risk-based privacy regulation at the federal level. Unlocking the innovative potential for life-saving technologies requires the establishment of a single set of strong, national privacy requirements based on a clear delegation from Congress.

The App Association notes its general concern with the ANPR's framing, which does not appear to acknowledge the many different ways that small businesses go far above and beyond minimum legal requirements. Today, privacy protection is a means of market differentiation, and we caution the FTC from altering this digital economy dynamic. Further, we urge FTC to ensure that its claims of harms are based on a strong and data-driven evidence base, and that its policy actions are not driven by rare edge use cases and/or hypotheticals.

III. The App Association's Views and Questions on Various Topics Raised in the Advance Notice of Proposed Rulemaking

[7] Graham Dufault, "The 4 Ps of Privacy: What Small Businesses Need in a Privacy Bill" (September 13, 2022), available at https://actonline.org/2022/09/13/the-4-ps-of-privacy-what-small-businesses-need-in-a-privacy-bill/.

[8] Press release, "Developer of Popular Women's Fertility-Tracking App Settles FTC Allegations that It Misled Consumers About the Disclosure of their Health Data," Fed. Trade Comm'n (Jan. 13, 2021), available at https://www.ftc.gov/news-events/press-releases/2021/01/developer-popular-womens-fertility-tracking-appsettles-ftc.

[9] Fed. Trade Comm'n, Flo Health, Inc., complaint (published Jan. 13, 2021), available at https://www.ftc.gov/system/files/documents/cases/flo_health_complaint.pdf.

[10] *Id.*

Notwithstanding our views on the FTC's authority to advance its ANPR and our strong preference for a preemptive federal privacy law, the App Association shares the following views and questions on particular topics raised in the ANPR.

a. Children's Privacy

The App Association supports legislation to strengthen privacy protections for children and adolescents beyond the Children's Online Privacy Protection Act (COPPA), as well as revisions to the COPPA Rule that would reduce the incentive to exploit the General Audience (GA) loophole. From our perspective, many harms in the children's privacy space can be traced to the ineffective verifiable parental consent (VPC) regime under COPPA, which could be remedied through the Commission's ongoing COPPA Rule review.

In response to *Question 13,* according to the App Association's research, 85 percent of parents have concerns about their children's digital privacy.[11] Prior to the pandemic, PricewaterhouseCoopers (PwC) estimated that children 12 to 15 years old consumed 20 hours of screen time each week,[12] with other data suggesting that kids seven to 18 years old consumed seven hours of screen time per day.[13] Given these statistics surrounding children's use of online services and parents' growing concern about their children's privacy, some parents have taken more active steps to monitor their children's time online. These steps include enabling parental control settings on their children's devices to make sure they do not have access to inappropriate information and reading privacy policies that the child likely does not understand due to their age. However, research shows that fewer than one in three parents use parental settings on their children's devices[14] and the Pew Research Center also says that 81 percent of parents knowingly let their children use GA services, such as YouTube, without parental restrictions.[15]

---

[11] Morgan Reed, *Developers and COPPA: Their Real-World Experience*, F.T.C. COPPA WORKSHOP, https://www.ftc.gov/system/files/documents/public_events/1535372/slides-coppa-workshop-10-7-19.pdf (October 7, 2019) (F.T.C. COPPA Workshop Slides).

[12] *Kids Digital Media Report 2019*, PRICEWATERHOUSECOOPERS, 4, https://cdn2.hubspot.net/hubfs/5009836/PwC%202019/Kids%20Digital%20Media%20Report%202019%20.pdf? (May 2019).

[13] *New tools, old rules: limit screen-based recreational media at home*, AMERICAN HEART ASSOCIATION SCIENTIFIC ADVISORY, https://newsroom.heart.org/news/new-tools-old-rules-limit-screen-based-recreational-media-at-home (Aug. 6, 2018).

[14] F.T.C. COPPA Workshop Slides.

[15] Aaron Smith, et. al, *Many Turn to YouTube for Children's Content, News, How-To Lessons*, PEW RESEARCH CENTER, https://www.pewresearch.org/internet/2018/11/07/many-turn-to-youtube-for-childrens-content-news-how-to-lessons/ (Nov. 7, 2018).

With children spending a growing amount of time on online platforms and services, the resulting consent burden on parents creates challenges for the current COPPA framework, as referenced in *Question 14.* Engaged parents in the modern age are expected to manage an avalanche of VPC documentation, which adds yet another onerous task for them to manage as they attempt to guide their children through complexities of the digital world, often while trying to keep up themselves. Knowing this, many creators of children-oriented websites and services have abandoned the sector or tinkered with their marketing to appear as a GA service ostensibly patronized by non-child users and thus not subject to COPPA (notably producing the opposite practices to the ones referenced in *Questions 15 and 16)*. Such practices are fairly widespread and often brazen; companies such as YouTube and TikTok, which profit from popular accounts populated and watched by users clearly under the age of 13, claim general audience status, flouting COPPA and the FTC by ignoring their responsibility to obtain VPC. Though the FTC recently reached[16] settlements[17] with both companies, the fines they are required to pay pale in comparison from the benefits they accrued from ignoring the law.[18]

To help close this loophole and improve overall COPPA compliance, the App Association encourages the FTC to allow platforms to innovate around tools and mechanisms for app developers to utilize as they implement the three steps to obtain VPC. A potential innovation could include a mechanism to verify that a person is an adult and able to consent to an app's privacy policy on behalf of a child. Additionally, the platform can provide the consenting adult with a notification of the collection, use, or disclosure of the child's personal information. Finally, a platform may provide implementation methods that allow individual app developers to obtain verifiable parental consent from the parent based on the platform-level age verification. This type of collaborative effort between platforms and app developer would allow parents to make informed decisions about the apps their children use in an exponentially more streamlined and transparent fashion.

---

[16] Federal Trade Commission, "Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law," https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law

[17] Federal Trade Commission, "Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That it Violated Children's Privacy Law." https://www.ftc.gov/news-events/news/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc-allegations-it-violated-childrens-privacy

[18]Federal Trade Commission, "DISSENTING STATEMENT OF COMMISSIONER ROHIT CHOPRA In the Matter of Google LLC and YouTube, LLC" https://www.ftc.gov/system/files/documents/public_statements/1542957/chopra_google_youtube_dissent.pdf

The App Association notes that some platforms already implement similar procedures by offering family plans to sign up and use a platform along with providing parents optional settings for their children such as "asking to buy," rejecting or approving a purchase, monitoring content, or placing limits on screen time from the parent's device. This allows a parent a simplified process to see what their kids are doing on their devices and decide what limits they want to set for their children, ensuring that parents have meaningful notice of and control over how an app collects, uses, and discloses their children's personal information without imposing unnecessary burdens and costs on app developers

Relative to *Question 21,* we have also broached the need for lawmakers to address targeted advertising to minors in testimony to Congress.[19] However, as we instructed Congress, there may be constitutional implications of an outright ban on certain kinds of advertising. Experience has shown that bans on advertising, even to minors, have had difficulty standing up to First Amendment scrutiny, and there may be less constitutionally fraught ways of dealing with the issues lawmakers seek to address.[20]

b. Data Security

The Commission asks whether it should commence a Section 18 rulemaking on data security (*Question 31*), as well as several questions about the standards such a rulemaking should adopt (*Questions 32-36*). As with our comments on a general privacy rulemaking, the App Association prefers and supports strong federal privacy legislation inclusive of requirements that covered companies to take certain steps to detect, prevent, and remediate unauthorized access to personal information. We support the inclusion of data security requirements that preempt most state laws that would otherwise impose conflicting or substantially different data security obligations. Strong federal data security provisions would raise the average readiness of American companies to defend against cyberthreats of all kinds, from state-sponsored ransomware campaigns to social engineering and phishing attacks.

We also urge the Commission against continuing along the path of expanding its interpretation of *data security* rules in order to mitigate *privacy* issues observed in the marketplace. For example, the Commission voted last year to approve a policy statement affirming that health apps and connected devices that collect or use consumers' health information must comply with the Health Breach Notification Rule. In our view, the policy statement went to great lengths to elide the difference between a breach of security and a privacy violation in hopes of expanding the rule's reach. Whereas the Health Breach Notification Rule plainly states that it exists simply to

[19] Testimony of Morgan Reed, ACT | The App Association, Senate Commerce Committee Hearing, "Protecting Consumer Privacy," September 29, 2021. https://www.commerce.senate.gov/services/files/19181833-E747-4D4E-8548-C8FF9CDCA54D

[20] See Reno v. ACLU, 521 U.S. 844 (1997)

ensure that PHR providers and their service providers notify consumers "when the security of their individually identifiable health information has been breached,"[21] the policy statement asserts that whenever a health app discloses sensitive health information without users' authorization, this is a "breach of security" under the rule.[22] Notably, the Final Rule included several examples to elucidate what exactly a data breach means, all of which reference instances where information is taken or stolen without the provider's knowledge (i.e., unauthorized access).[23]

While we are sympathetic to the goal of preventing the unanticipated disclosure of users' sensitive information and agree that there should be punishment when a company violates consumer trust, the fact remains a data breach notification law is not the ideal vessel by which to accomplish that goal and may create unnecessary confusion for both businesses and consumers. To the extent that the Commission ultimately proffers new rules on both data security and privacy with this new rulemaking activity, we hope those will be duly separated such that each rule or set of rules addresses market practices that correspond accordingly.

c. Collection and Processing of Consumer Data

In *Question 43*, the Commission asks if it should impose limitations on companies' collection, use, and retention of consumer data. The principle of data minimization is a crucial element of the federal privacy legislation that the App Association prefers to a broad Commission privacy rulemaking. For example, the App Association has supported federal privacy legislation that would prohibit collections, processing, or transfer beyond what is reasonably necessary, proportionate, and limited to products and services requested by the individual or communications anticipated within the context of the relationship. We note that this approach is more likely to stand up to legal scrutiny in the Untied States as opposed to in the European method of barring all processing unless a lawful basis exists. We have supported that such legislation could require the FTC to issue nonbinding guidance, which will help inform covered entities without subjecting them to more complex forms of liability.

---

[21] Health Breach Notification Rule, 74 Fed. Reg. 42962 (Aug. 25, 2009), *available at*

https://www.ftc.gov/system/files/documents/federal_register_notices/2009/08/healthbreachnotificationrulefinal.pdf

[22] Federal Trade Commission, Statement of the Commission on Breaches by Health Apps and Other Connected Devices (September 15, 2021), *available at*

https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf

[23] Health Breach Notification Rule, 74 Fed. Reg. 42966, §318.2 (August 25, 2009), *available at*

https://www.ftc.gov/system/files/documents/federal_register_notices/2009/08/healthbreachnotificationrulefinal.pdf

The Commission also asks how a data minimization rule could be scoped to prevent the personal data from being used for purposes other than what is necessary to perform the requested service or specified at the time of collection (*Questions 44-47).* To the extent that the Commission pursues such a minimization rule, we urge it to stay away from language that revolves around *unexpected* uses of information. In the experience of many App Association member companies, consumers may not always *expect* specific improvements to products and services, even if they ultimately benefit from them. While we agree that using personal information to create high-risk products and services without consumer consent, such as a facial recognition algorithm, is unacceptable, not all unexpected improvements are objectionable. A risk-based approach to incompatible processing purposes may be preferable in order to preserve businesses' ability to create innovative products that consumers may not anticipate but are unlikely to bring them harm.

In responding to *Question 37,* the App Association notes that its members currently leverage numerous innovative biometric-assisted technologies in order to provide services consumers need and demand in the digital economy. Here, we will share two key uses cases: facial verification and wearable devices.

i. Facial Verification

Facial verification technologies are most often used for security purposes, i.e., to verify whether a person really is who they say they are. For example, our members currently use facial verification technologies embedded at the platform level, such as Apple's Face ID, to allow users to log in to apps using a scan of their face from the camera app. An app developer can choose to integrate Apple's Face ID as an option for users to select as one of the factors in a two-factor authentication scheme. For example, users often opt for two-factor authentication to improve device security in cases where an application stores sensitive personal information, such as bank account information. The mathematical representation of the individual's face (the gallery image) used to validate the comparison image is stored within Apple's Secure Enclave on the device and is not available to the developer, Apple, or any other third party.[24]

As the underlying technology continues to improve, app developers are likely to implement a greater variety of facial recognition use cases. Therefore, by way of responding to *Question 38*, it will become increasingly important that emerging standards of regulation ensure that appropriate governance and accountability structures attach to each use case commensurate with its risk. For example, in existing risk frameworks created by academics, targeted use of facial verification algorithms on

[24] Apple, "About Face ID advanced technology," September 14, 2021, https://support.apple.com/en-us/HT208108

a one-to-one basis typically represents a lower risk deployment, whereas real-time deployment of facial identification in public spaces is among the highest.[25]

The App Association currently supports legislation to limit particularly risky uses of facial recognition technology and consistently advocates for a federal privacy law that would limit how companies can process consumer data without their consent.[26] To the extent that the Commission seeks to create rules in this area, differentiating between targeted, consent-based uses of biometrics versus drag-net applications will be an important task going forward.

ii. Wearables

Through our Connected Health Initiative (CHI), the App Association seeks to advance responsible pro-digital health policies and laws that can harness the great potential of connected healthcare devices and tools, some of which may leverage biometric inputs, to unlock a higher standard of care for patients while minimizing potential harms. The remote collection of health data through wearables can help ameliorate some of the long-standing disparities in healthcare access by allowing personalized diagnostics to occur outside of traditional healthcare institutions. For example, fitness trackers that collect valuable data, such as sleep patterns, activity, and stress levels, can automatically share relevant information with clinicians, therapists, or coaches so that they can use granularized data to create more personalized care routines without requiring an in-person visit.

In light of the COIVD-19 pandemic, many have turned to digital health platforms, tools, and services to consult with caregivers in greater numbers in an effort to avoid the risk of exposing themselves or others to the virus. Wearable ownership and use increased in 2020, with 43 percent of respondents using wearables in 2020, compared to 33 percent in the year prior.[27] Additionally, during COVID-19, more than half of all owners and users of wearables reported using them to manage a diagnosed health condition.[28] Sixty-two percent of physicians reported in a recent study that they believe wearable devices would increase the overall quality of care for their patients.[29]

---

[25] Claire Garvie, Alvaro Bedoya, and Jonathan Frankle, "The Perpetual Lineup: Risk Framework," Georgetown Center Privacy & Technology, October 18, 2016, https://www.perpetuallineup.org/risk-framework

[26] ACT | The App Association, "Testimony of Morgan Reed, President at ACT | The App Association Before the U.S. Senate Committee on Commerce, Science, and Transportation on Protecting Consumer Privacy," September 19, 2021, https://actonline.org/wp-content/uploads/Reed-Testimony.pdf

[27]Rock Health, "Digital Health Consumer Adoption Report 2020," February 26, 2021, https://rockhealth.com/insights/digital-health-consumer-adoption-report-2020/

[28] Ibid.

[29] Nersi Nazari, "5 Key Attributes For Medical Wearables Seeking Adoption By Hospitals," Vital Connect, October 20, 2017: https://vitalconnect.com/5-key-attributes-medical-wearables-seeking-adoption-hospitals/

Clearly, usership of technologies that can pull biometrics and infer cognitive or emotional states will continue to increase, especially as efficacy improves and the benefits become clearer to users. The App Association is keenly aware of the need to create appropriate guardrails to keep up with the growth of the industry and to ensure that mobile health players that collect sensitive biometric data continue to do so responsibly. Aside from advocating federal privacy legislation, as mentioned earlier, the App Association continues to lead in advocating for the development of frameworks that will responsibly support the development, availability, and use of such AI innovations, including by developing Good Machine Learning Practices specifically for AI development and risk management of AI, resources that may help the Commission as it contemplates *Questions 53-57,* regarding automated decision-making systems.[30]

d. Artificial Intelligence

In *Question 60*, the ANPR requests comment on whether the FTC should "forbid or limit the development, design, and use of automated decision-making systems that generate or otherwise facilitate outcomes that violate Section 5."[31] The App Association continues to work proactively to advance the use of artificial intelligence (AI) in key use cases in ways that prioritize consumer safety and while well-intentioned, the ANPR stands to stifle American innovation. As just one example, the App Association's Connected Health Initiative[32] (CHI) assembled a Health AI Task Force in the summer of 2018 consisting of a range of innovators and thought leaders. CHI unveiled its AI Task Force's deliverables during a public-private multistakeholder dialogue in Washington, DC, which include a position piece supporting AI's role in healthcare, policy principles addressing how policy should approach the role of AI in healthcare, and a terminology document targeted at policymakers.[33] Since then, CHI has also developed Good Machine Learning Practices specifically for AI development and risk management of AI meeting the Food and Drug Administration's definition of a medical device.[34] More generally, the App Association continues to lead in advocating for a pragmatic approach to consumer protection that responsibly supports the development, availability, and use of AI innovations.

[30] The CHI's Good Machine Learning Practices are available at https://bit.ly/3gcar1e.

[31] See ANPR at section IV, Q.60.

[32] *See* www.connectedhi.com.

[33] The CHI Health AI Task Force's deliverables are accessible at https://actonline.org/2019/02/06/why-does-healthcare-need-ai-connected-health-initiative-aims-to-answer-why/.

[34] The CHI's Good Machine Learning Practices are available at https://bit.ly/3gcar1e.

AI is an evolving constellation of technologies that enable computers to simulate elements of human thinking – learning and reasoning among them. An encompassing term, AI entails a range of approaches and technologies, such as Machine Learning (ML) and deep learning, where an algorithm based on the way neurons and synapses in the brain change due to exposure to new inputs, allowing independent or assisted decision making. AI-driven algorithmic decision tools and predictive analytics are having, and will continue to have, substantial direct and indirect effects on Americans. Some forms of AI are already being used to improve American consumers' lives today – for example, AI is used to detect financial and identity theft and to protect the communications networks upon which Americans rely against cybersecurity threats.

Today, Americans encounter AI in their lives incrementally through the improvements they have seen in computer-based services they use, typically in the form of streamlined processes, image analysis, and voice recognition (we urge consideration of these forms of AI as "narrow" AI). The App Association notes that this "narrow" AI already provides great societal benefit. For example, AI-driven software products and services revolutionized the ability of countless Americans with disabilities to achieve experiences in their lives far closer to the experiences of those without disabilities.

Moving forward, across use cases and sectors, AI has incredible potential to improve American consumers' lives through faster and better-informed decision making, enabled by cutting-edge distributed cloud computing. As an example, healthcare treatments and patient outcomes stand poised to improve disease prevention and conditions, as well as efficiently and effectively treat diseases through automated analysis of x-rays and other medical imaging. From a governance perspective, AI solutions will derive greater insights from infrastructure and support efficient budgeting decisions. It is estimated that AI technological breakthroughs will represent a $126 billion market by 2025.[35]

Nonetheless, AI also has the potential to raise a variety of unique considerations for policymakers. The App Association appreciates the FTC's efforts to develop a policy approach to AI that will bring its benefits to all, balanced with necessary safeguards to protect consumers. To assist the Commission, we offer a comprehensive set of AI policy principles below for consideration with which that we strongly encourage alignment:

1. **AI Strategy:** Many of the policy issues raised below involve significant work and changes that will impact a range of stakeholders. The cultural, workforce training and education, data access, and technology-related changes associated with AI will require strong guidance and coordination. A strategy incorporating guidance on the issues below will be vital to achieving the promise that AI offers to consumers and our economies. We believe it is critical to take this opportunity to

[35] McKinsey Global Institute, *Artificial Intelligence: The Next Digital Frontier?* (June 2017), available at https://www.mckinsey.com/~/media/McKinsey/Industries/Advanced%20Electronics/Our%20Insights/How%20artificial%20intelligence%20can%20deliver%20real%20value%20to%20companies/MGI-Artificial-Intelligence-Discussion-paper.ashx.

encourage civil society organizations and private sector stakeholders to begin similar work.

2. **Research:** The FTC should support research and development of AI by prioritizing and providing sufficient funding while also ensuring adequate incentives (e.g., streamlined availability of data to developers, tax credits) are in place to encourage private and non-profit sector research. Transparency research should be a priority and involve collaboration among all affected stakeholders who must responsibly address the ethical, social, economic, and legal implications that may result from AI applications.

3. **Quality Assurance and Oversight:** In building trust with marginalized communities, FTC should support the advancement of risk-based approaches to ensure that the use of AI aligns with the recognized standards of safety, efficacy, and equity. Providers, technology developers and vendors, and other stakeholders all benefit from understanding the distribution of risk and liability in building, testing, and using AI tools. Policy frameworks addressing liability should ensure the appropriate distribution and mitigation of risk and liability. Specifically, those in the value chain with the ability to minimize risks based on their knowledge and ability to mitigate should have appropriate incentives to do so. Some recommended guidelines include:
    - Ensuring AI is safe, efficacious, and equitable.
    - Supporting that algorithms, datasets, and decisions are auditable.
    - Encouraging AI developers to consistently utilize rigorous procedures and enabling them to document their methods and results.
    - Requiring those developing, offering, or testing AI systems to provide truthful and easy to understand representations regarding intended use and risks that would be reasonably understood by those intended, as well as expected, to use the AI solution.
    - Ensuring that adverse events are timely reported to relevant oversight bodies for appropriate investigation and action.

4. **Thoughtful Design:** FTC should strongly encourage the design of AI systems that are informed by real-world workflows, human-centered design and usability principles, and end-user needs. AI systems solutions should facilitate a transition to changes in the delivery of goods and services that benefit consumers and businesses. The design, development, and success of AI should leverage collaboration and dialogue among users, AI technology developers, and other stakeholders in order to have all perspectives reflected in AI solutions.

5. **Access and Affordability:** FTC should endorse the creation of accessible and affordable AI systems. Significant resources may be required to scale systems and policymakers should take steps to remedy the uneven distribution of resources and access. Policies must be put in place that incentivize investment in building infrastructure, preparing personnel and training, as well as developing, validating, and maintaining AI systems with an eye toward ensuring value.

6. **Ethics:** AI will only succeed if it is used ethically. It will be critical to promote many of the existing and emerging ethical norms for broader adherence by AI technologists, innovators, computer scientists, and those who use such systems. FTC should:
    - Encourage the development of AI solutions that align with all relevant ethical obligations, from design to development to use.
    - Encourage the development of new ethical guidelines to address emerging issues with the use of AI, as needed.
    - Maintain consistency with international conventions on human rights.
    - Ensure that AI is inclusive such that AI solutions beneficial to consumers are developed across socioeconomic, age, gender, geographic origin, and other groupings.
    - Reflect that AI tools may reveal extremely sensitive and private information about a user and ensure that laws protect such information from being used to discriminate against certain consumers.

7. **Modernized Privacy and Security Frameworks:** While the types of data items analyzed by AI and other technologies are not new, this analysis will provide greater potential utility of those data items to other individuals, entities, and machines. Thus, there are many new uses for, and ways to analyze, the collected data. This raises privacy issues and questions surrounding consent to use data in a particular way (e.g., research, commercial product/service development). It also offers the potential for more powerful and granular access controls for consumers. Accordingly, FTC should address the topics of privacy, consent, and modern technological capabilities as a part of the policy development process. Risk management policy frameworks must be scalable and assure that an individual's data is properly protected, while also allowing the flow of information and responsible evolution of AI. With proper protections in place, policy frameworks should also promote data access, including open access to appropriate machine-readable public data, development of a culture of securely sharing data with external partners, and explicit communication of allowable use with periodic review of informed consent.

8. **Collaboration and Interoperability:** FTC should enable eased data access and use through creating a culture of cooperation, trust, and openness among policymakers, AI technology developers and users, and the public.

9. **Bias:** The bias inherent in all data, as well as errors, will remain one of the more pressing issues with AI systems that utilize machine learning techniques in particular. Addressing data provenance and bias issues is a must in developing and using AI solutions. The FTC should:
    - Require the identification, disclosure, and mitigation of bias while encouraging access to databases and promoting inclusion and diversity.
    - Ensure that data bias does not cause harm to users or consumers.

10. **Education:** The FTC should support education for the advancement of AI, promote examples that demonstrate the success of AI, and encourage stakeholder engagements to keep frameworks responsive to emerging opportunities and challenges.
    - Consumers should be educated as to the use of AI in the service they are using.
    - Academic education should include curriculum that will advance the understanding of and ability to use AI solutions.

e. Consent and Dark Patterns

App Association members compete on privacy and work hard every day to develop better ways to communicate with their users about privacy and give them meaningful choices. Consumers should have a clear understanding of the types of personal data they are sharing, and which companies are using that data and how. The App Association has long advocated for a federal privacy law that would require data controllers to maintain accessible and transparent privacy policies and obtain affirmative opt-in consent for the processing of sensitive data.

The ANPR seeks to comment on the effectiveness and administrability of consumer consent to companies' commercial surveillance and data security practices, including the potential for more guardrails around the methods and type of consents presented to consumers (*Questions 73, 74, 76, 78,* and *79)*. At the same time, the ANPR notes that the existing notice and choice consent framework may leave consumers under-protected in many cases, especially when consent us obtained through manipulative conduct. Chairman Khan's statement accompanying the ANPR notes that "the use of dark patterns and other conduct that seeks to manipulate users underscores the limits of treating present market outcomes as reflecting what users desire or value."[36]

The App Association agrees that the notice and choice consent regime may not always work for consumers, even if the concept of "dark pattern" remains a frustratingly elusive concept to define.[37] Contrary to the suggestions of some industry commentators, dark patterns or otherwise manipulative consumer choice architectures are by no means a tactic exclusively leveraged by cutting-edge startups or mobile applications. Dr. Lorrie Cranor's pioneering research into consumer privacy choices has found inconsistent and at times misleading user opt-out controls among a wide swath of industry players,

[36] Federal Trade Commission, Advanced Notice of Proposed Rulemaking, Trade Regulation Rule on Commercial Surveillance and Data Security, August 22, 2022 https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security

[37] Harry Brignull, "What are Dark Patterns." https://www.darkpatterns.org/

including from verticals as diverse as finance, health, media, and sports, and of widely varying sophistication and user design prowess.[38]

It is also important to recognize that dark patterns are often extensions of tactics used in the physical world. For example, thought leaders have defined a "roach motel" dark pattern category as design choices that require users to take exhaustive steps to effectuate a preference that may conflict with the business's preference. Of course, the roach motel model was pioneered and perfected for years before websites and apps even existed. Casino designers, for example, are notorious for constructing floor plans that intentionally disguise exits with the goal of manipulating guests into spending extra time within the facility. Few would call that a dark pattern because it occurs within the physical world, yet it seems equally manipulative to the opt-out practices at the *New York Times,* for example.

Other dark patterns, such as "confirmshaming," are clearly holdovers from longstanding face-to-face sales tactics in which salespeople employ behavioral nudges in order to close a sale or upsell a service. As with such sales tactics, confirmshaming should be understood to encompass a wide range of activities that run from innocuous to outright deceptive, the latter of which should be the main source of attention from regulators. Confirmshaming, as currently understood, could include a prompt as simple as "are you sure you wish to opt out," a necessary piece of developer due diligence that could be construed as guilting a customer. While certainly starker when presented plainly on a website or app than when spoken aloud in a sales context, such a prompt hardly seems out of place in the broader marketplace and surely does not constitute an unfair or deceptive trade practice. The App Association urges the FTC to focus its attention on examples of consent that clearly deceive and bring harm to a user.

[38] Lorrie Cranor and Hannah Habib, “An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites,” *Soups 2019,* August 2019. https://www.usenix.org/system/files/soups2019-habib.pdf

IV. Conclusion

The App Association appreciates the opportunity to submit its comments to FTC. We look forward to assisting the Commission in protecting consumers' privacy during this critical time for our country.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Matt Schwartz
Policy Associate

Leanna Wade
Policy Associate

ACT | The App Association
1401 K St NW (Ste 501)
Washington, DC 20005
202-331-2130