March 6, 2023

National Telecommunications and Information Administration
1401 Constitution Ave NW
Washington, District of Columbia 20230

RE: Comments of ACT | The App Association to NTIA on Privacy, Equity, and Civil Rights [Docket No. 230103-0001]

I. Introduction and Statement of Interest

ACT | The App Association (App Association) appreciates the opportunity to submit views to the National Telecommunications and Information Administration (NTIA) on the intersection of privacy, equity, and civil rights and how the processing of personal information by private entities generates, worsens, or improves disproportionate harms for marginalized and historically excluded communities. We align with NTIA's goal to identify gaps in applicable privacy and civil right laws and find ways to prevent and deter harmful behavior and impacts, while rectifying existing gaps.

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.[1] 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 NTIA regarding this request for comment on privacy, equity, and civil rights.

II. General Views of the App Association on the Need for a Comprehensive Cross-Sectoral Privacy Framework

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. Today, the "tech sector" no longer exists as a separate, unique vertical. Rather, it has expanded and taken root as part of other industries, and in the process, it has been democratized into a startup economy that thrives across the nation, mostly outside of Silicon Valley. As cars begin to drive themselves and physicians adopt clinical decision tools that utilize artificial intelligence (AI), the United States is fast evolving into a "tech economy." Moreover,

[1] 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

companies thought of as tech heavyweights often have more in common with traditional economy players from a business model standpoint; the former just happens to use newer technologies and find ways to make them useful for people.

As regulators from across key markets abroad continue to rush to utilize approaches to regulation of the digital economy which are often heavy handed, the United States has remained the greatest market in the world for building a startup due to its evidence-based and light-touch approach to regulating new industries. Across the world, other governments struggle to incent and sustain the digital economy growth seen only in this country because companies elsewhere often face great barriers to bringing novel products and services to market, slowing technological innovations to the pace of government approval.

The American approach to privacy remains 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 believe a comprehensive federal privacy legislation can address some of the issues raised by NTIA in this request for comment (RFC). 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, especially in the context of businesses using personal data to discriminate based on nationality, race, gender, religion, or disability. As online risks continue to expand, federal privacy legislation could constitute an expansion of Americans' civil rights in the digital age.

As the RFC points out, substantive amounts of research have demonstrated that marginalized or underserved communities are at heightened risk of privacy violations and data loss or misuse. We agree with NTIA that all communities must be able to trust and safely access digital services to realize their full potential and increase adoption of beneficial digital services. Enabling all Americans to enjoy robust privacy protections will help to accomplish that goal and increase trust in the digital economy. Trust is the linchpin of App Association members' economic viability. Even as more and more of our member companies take advantage of opportunities in the enterprise space, trust is just as—if not more—important as it is for companies that serve consumers directly.

III. Responses of ACT | The App Association to Specific Questions Raised in NTIA's Request for Comment

Below, we offer responses to various outcomes and high-level goals NTIA raises in its RFC.

1. Framing

Considering the framing questions, and especially how regulators, legislators, and other stakeholders should approach the civil rights and equity implications of commercial data collection and other processing, we reiterate our position from the previous section. We strongly believe the best approach to the civil rights and equity implications of commercial data collection and other processing is a federal privacy law that would give individuals more control over their information and prohibit businesses and

non-profits from utilizing personal data to discriminate users based on their race, religion, national origin, gender, or disability status.

Without a federal privacy law, it becomes increasingly hard for individuals to navigate the rules around commercial data processing and the remedies and rights available to them. Similarly, the lack of a federal privacy law increases the potential harms that can arise from data processing, especially considering the ever-expanding landscape of information and privacy tools with which users interact. 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. 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 could remedy these issues. 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. Such a requirement would protect all Americans, especially those who are disproportionality impacted by data theft and data loss. We further support the inclusion of data security requirements that preempt most state laws that would otherwise impose conflicting or substantially different data security obligations, so there is only one set of rules for both consumers and businesses to follow. 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, which would ultimately benefit consumers.

Concerning privacy and fairness in automated decision making in the context of sensitive and non-sensitive information, we note that the usership of technologies that can pull biometrics and infer cognitive or emotional states (which is sensitive data) will only continue to increase, especially as efficacy improves and the potential benefits become clearer to users. The App Association is keenly aware of the need to create appropriate guardrails to protect sensitive data and keep up with the growth of the industry to ensure that companies that collect sensitive biometric data do so responsibly. Automated decision making can discriminate against marginalized communities and exacerbate hidden biases in data that is used to run the tools in question. Aside from advocating federal privacy legislation, the App Association continues to lead in advocating for the development of frameworks that will responsibly support the development, availability, and use of AI innovations that are safe for everyone, including by developing Good Machine Learning Practices specifically for AI development and risk management of AI, resources that may help NTIA as it contemplates questions relating to automated decision-making systems.[2]

In building trust with marginalized communities, NTIA 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.

2. Impact of Data Collection and Processing on Marginalized Groups

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

In response to question 2(a), according to the App Association's research, 85 percent of parents have concerns about their children's digital privacy. Prior to the pandemic, PricewaterhouseCoopers (PwC) estimated that children 12 to 15 years old consumed 20 hours of screen time each week, with other data suggesting that kids seven to 18 years old consumed seven hours of screen time per day. 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 and the Pew Research Center also says that 81 percent of parents knowingly let their children use general audience (GA) services, such as YouTube, without parental restrictions. Due to their underdeveloped digital literacy, lack of analytical skills and judgment (compared to adults), children are especially vulnerable to commercial data collection and processing practices that may affect them negatively (sometimes later in life). Additionally, with children spending a growing amount of time on online platforms and services, the resulting consent burden on parents also creates challenges for the current Children's Online Privacy Protection Act (COPPA) framework. Engaged parents in the modern age are expected to manage an avalanche of verifiable parental consent (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. VPC can be particularly burdensome for parents who do not have government-issued forms of identification, a credit or debit card, or have learned English as their second language.

Recognizing the difficulties parents and businesses may face in providing and obtaining VPC, many creators of child-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. Such practices are widespread and often brazen; companies such as YouTube, Epic Games, and TikTok, which profit from popular accounts populated and watched by users clearly under the age of 13, claim general audience status, and ignore their responsibility to obtain VPC. Though the Federal Trade Commission (FTC) recently reached settlements with those companies, the fines they are required to pay pale in comparison from the benefits they accrued from ignoring the law.

Regarding the remaining questions under section 2, on the impact of data collection and processing on marginalized groups, we note that the principle of data minimization would be a preferable approach to broad limitations on companies' ability to collect, use, and retain consumer data. 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 believe that this approach is more likely to stand up to legal scrutiny in the United States as opposed to in the European method of barring all processing unless a lawful basis exists. Further, we suggest that data minimization language stay away from revolving 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 to preserve businesses' ability to create innovative products that consumers may not anticipate but are unlikely to bring them harm.

That said, we acknowledge that the current data collection and processing practices of some businesses currently enable things like discriminatory policing,[3] digital redlining,[4] voter suppression,[5] digital health inequities,[6] identity theft,[7] retail discrimination[8], employment discrimination[9], housing discrimination[10], increased surveillance[11] and certain dangers to physical safety.[12] Numerically these trends impact more White Americans, but looking at the percentages, it becomes clear that Black and Indigenous people face disproportionate harms.[13] Additionally, there are constantly new tools that collect and use data in ways that enable companies to leverage it for surveillance, racial profiling, and discrimination.

Concerning contexts in which commercial data collection and processing occur that warrant particularly rigorous scrutiny for their potential to cause disproportionate harm or enable discrimination, we note that AI, facial recognition and processing of biometric data via, e.g., wearables all simultaneously promise significant rewards while also posing notable risks. These technologies warrant scrutiny because they hold the potential to invade privacy and enable discriminations.

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.

---

[3] "U.N. Panel: Technology in Policing Can Reinforce Bias," The New York Times, https://www.nytimes.com/2020/11/26/us/un-panel-technology-in-policing-can-reinforce-racial-bias.html

[4] Zack Quaintance, "What Is Digital Redlining? Experts Explain the Nuances," Government Technology (Mar. 28, 2022), https://www.govtech.com/network/what-is-digital-redlining-experts-explain-the-nuances

[5] Ian Vandewalker, "Digital Disinformation and Vote Suppression," NPR (Sep. 2, 2020), https://www.brennancenter.org/our-work/research-reports/digital-disinformation-and-vote-suppression

[6] Sara Heath, "Is the Digital Divide the Newest Social Determinant of Health?" Patient Data Access News (Mar. 10, 2021) https://patientengagementhit.com/news/is-the-digital-divide-the-newest-social-determinant-of-health

[7] Sarah Dranoff, "Identity Theft: A Low–Income Issue," American Bar Association (Sep. 15, 2014) https://www.americanbar.org/groups/legal_services/publications/dialogue/volume/17/winter-2014/identity-theft--a-lowincome-issue/

8 Ray Fisman and Michael Luca, "Fixing Discrimination in Online Marketplaces," Harvard Business Review (Dec. 2016), https://hbr.org/2016/12/fixing-discrimination-in-online-marketplaces

9 Miranda Bogen, "All the Ways Hiring Algorithms Can Introduce Bias," Harvard Business Review (May 6, 2019) https://hbr.org/2019/05/all-the-ways-hiring-algorithms-can-introduce-bias

10 Valerie Schneider, "Locked Out by Big Data: How Big Data, Algorithms, and Machine Learning May Undermine Housing Justice," Columbia Human Rights Law Review https://hrlr.law.columbia.edu/hrlr/locked-out-by-big-data-how-big-data-algorithms-and-machine-learning-may-undermine-housing-justice/

11 Drew Harwell, "Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding," The Washington Post (Dec 19, 2019) https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/

[12] Aarti Shahani, "Smartphones Are Used To Stalk, Control Domestic Abuse Victims," NPR (Sep. 15, 2014), https://www.npr.org/sections/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims

[13] Michele Gilman and Rebecca Green, "The Surveillance Gap: The Harms of Extreme Privacy and Data Marginalization," NYU Review of Law and Social Change 42 (2018): 253-307, https://socialchangenyu.com/review/the-surveillance-gap-the-harms-of-extreme-privacy-and-data-marginalization/

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.[14]

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

[14] 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.

- 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 incent 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.

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.

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.[15]

As the underlying technology continues to improve, app developers are likely to implement a greater variety of facial recognition use cases. Therefore, 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 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.[16] 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.[17] To the extent that the Commission seeks to create rules in

[15] Apple, "About Face ID advanced technology," (Sep 14, 2021), https://support.apple.com/en-us/HT208108
[16] Claire Garvie, Alvaro Bedoya, and Jonathan Frankle, "The Perpetual Lineup: Risk Framework," Georgetown Center Privacy & Technology, (Oct 18, 2016), https://www.perpetuallineup.org/risk-framework
[17] 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

this area, differentiating between targeted, consent-based uses of biometrics versus drag-net applications will be an important task going forward.

Concerning the remote collection of health data through wearables, this can help ameliorate some of the long-standing disparities in healthcare access marginalized groups face, 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 COVID-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.[18] Additionally, during COVID-19, more than half of all owners and users of wearables reported using them to manage a diagnosed health condition.[19] 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.[20]

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.

Another issue worth mentioning here is the effectiveness and administrability of consumer consent to companies' commercial surveillance and data security practices, including the potential for the existing notice and choice consent framework to leave consumers under-protected in many cases, especially when consent is obtained through manipulative conduct (through so-called dark patterns). The App Association acknowledges 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.[21] 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, including from verticals as diverse as finance, health, media, and sports, and of widely varying sophistication and user design prowess.[22]

---

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

[19] Id.

[20] 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/

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

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

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 recommends focusing legislative attention on examples of consent that clearly deceive and bring harm to a user.

3. Existing Privacy and Civil Rights Laws

Several federal civil rights statutes currently exist to shield individuals from discriminatory treatment by various institutions, including:

- Title VII of the Civil Rights Act of 1964 prohibits discrimination in employment based on race, color, religion, national origin, or sex, and Title II of the Act bars discrimination based on race, color, religion, or national origin in public accommodations.
- The Fair Housing Act, enacted in 1968, prohibits discrimination in the sale or rental of housing based on race, color, religion, national origin, sex, disability, or familial status.
- The Equal Credit Opportunity Act, enacted in 1974, prohibits discrimination against credit applicants based on race, color, religion, national origin, sex, marital status, age, or source of income.

While these laws have been crucial in resolving some of the inequities marginalized communities face, unfortunately enforcing these laws continues to be difficult and historical discrimination has simply transitioned into the digital age, including commercial data collection practices, which continues to translate into real-world harms.

Considering useful models for privacy regulation, the European Union's General Data Protection Regulation (GDPR) explicitly considers race, ethnic origin, religion, sexual orientation, political beliefs, health, and biometric data as sensitive data that is subject to a higher level of protection. Its processing is generally prohibited and only allowed under certain derogations, e.g., when an individual has made the data public or given explicit consent, or when a law governs specific types of data processing for a specific purpose related to public health or public interest or a law contains adequate legal safeguards that provide for the processing of sensitive personal data in areas such as public heath, employment, and social protection. Additionally, GDPR also explicitly requires businesses to implement privacy by design, data minimization, and purpose limitation principles, which overall result in stronger data protection for all

consumers. This approach may be worth modeling in order to increase privacy protection for marginalized groups.

4. Solutions

As stated above in more detail, the App Association prefers and supports strong federal privacy legislation that requires 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.

In response to question 5(b) on how to appropriately protect children and teens from data abuse, the App Association supports legislation to strengthen privacy protections for children and adolescents beyond 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 VPC regime under COPPA, which could be remedied through the FTC's ongoing COPPA Rule review.

To help close the general audience loophole and improve overall COPPA compliance, the App Association believes platforms should be able to innovate around tools and mechanisms for app developers to utilize as they implement the 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.

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 monitor 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. Additionally, expanding the current approach from focusing mainly on parental consent to include concepts like data minimization, privacy by design, and allow children to understand their own rights and choices by drafting policies in easy to understand and intelligible language may be further steps to improve the protection of children's data.

Regarding specifically targeted advertising to children, we believe lawmakers need to address targeted advertising to minors in testimony to Congress.[23] However, as we instructed Congress, there may be constitutional implications of an outright ban on certain kinds of advertising. Experience has shown that

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

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.[24]

IV. Conclusion

The App Association appreciates the opportunity to submit its comments to NTIA. We look forward to assisting the Administration in protecting consumers' privacy during this critical time.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Anna Bosch
Privacy Policy Associate

Leanna Wade
Regulatory Policy Associate

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

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