Before the
National Telecommunications and Information Administration
United States Department of Commerce
Washington, D.C.

In re	Docket No. 230103-0001
Privacy, Equity, and Civil Rights	

COMMENTS OF
THE COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION (CCIA)

In response to the Request for Comment published January 20, 2023, at 88 Fed. Reg. 3714 (the "RFC") the Computer & Communications Industry Association ("CCIA")[1] submits the following comments.

I. Introduction

CCIA is pleased to participate in this effort by the National Telecommunications and Information Administration ("NTIA" or the "Agency") to examine issues at the intersection of privacy, equity, and civil rights. We provide comments herein on several of the topics raised in the RFC, highlighting the benefits and opportunities created by processing data, the applicability of existing privacy and civil rights laws, and ongoing efforts to prevent, deter, and remedy potential harms.

Vulnerable communities warrant protection from all forms of discrimination. CCIA and its members commend the Agency for conducting this Comment process and for seeking broad engagement and input from stakeholders and the public on ways to approach the civil rights and equity implications of modern data collection and processing. NTIA has a unique ability to address this issue due to its leading role in telecommunications and information policy issues, its extensive experience with these issues, and its ability to effectively engage with outside groups.

[1] CCIA is an international, not-for-profit trade association representing a broad cross section of communications and technology firms. For 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. A list of CCIA members is available at https://www.ccianet.org/members.

Algorithmic fairness is context-dependent and best practices are still evolving; in examining these issues it will be important for NTIA to recognize the need for flexibility in different circumstances. CCIA encourages NTIA and the Commerce Department to recognize the importance of collaboration between industry, regulators, civil society, and other stakeholders in addressing novel policy contexts like issues related to algorithmic fairness.

II. Privacy and Civil Rights Laws

A. Question 1. Framing

Innovation brings new opportunities with improvements to existing technologies and the creation of new tools. Despite these rapid advancements, the decisions and activities driven by artificial intelligence, automated systems, and related technologies are still largely subject to Title VII of the Civil Rights Act of 1964, the Americans with Disabilities Act, and other existing civil rights laws. The Department of Justice and other enforcers have utilized existing frameworks that have developed around these laws to protect individuals against discrimination and uphold civil rights. If two entirely separate bodies of federal law – civil rights law and privacy law – become simultaneously enforceable to address identical violations and harms, the legal system would be troubled with confusion and repetitive legal claims.

Further, while any new technology brings with it speculation about its potential for negative unintended consequences, not every possible risk requires mitigation. Regulators should continue to weigh perception against reality before taking premature and possibly needless action. Developing "Trustworthy AI" will require a comprehensive approach and extensive collaboration between all stakeholders. To that end, we encourage the Agency and lawmakers to reach out to companies to learn more about how they are employing responsible and trustworthy AI,[2] including by adopting forward-looking principles to enable transparency as automated systems evolve.[3] The entire ecosystem could benefit from increased guidance and sharing of best practices, as well as learning about important risks and considerations in using AI tools.

---

[2] Christophe Dupuy et al., *Advance in Trustworthy Machine Learning at Alexa AI*, Amazon Science (Apr. 28, 2022) https://www.amazon.science/blog/advances-in-trustworthy-machine-learning-at-alexa-ai.

[3] Report, *Policy Principles for Enabling Transparency of AI Systems*, Information Technology Industry Council (Sept. 2022), https://www.itic.org/documents/artificial-intelligence/ITIsPolicyPrinciplesforEnablingTransparencyofAISystems2022.pdf

The RFC asks about how to approach this discussion in the context of automated decision making, suggesting the use of "sensitive" and "non-sensitive" information. But this is too restrictive. "Sensitive" information should not be conceived only as a source of harm. Sometimes information that tends to be characterized as "sensitive" may be necessary for measuring or identifying approaches to mitigate issues that may arise even if an underlying system is not collecting or processing sensitive data.

The RFC asks about the "incongruity between intent requirements" in civil rights laws and how automated systems can produce discriminatory outcomes without the intentional guidance of a programmer. As previously mentioned, civil rights laws are well suited to combat discrimination in the digital space, particularly given that they do not only focus on intent. Existing civil rights legal frameworks consider whether certain outcomes are inappropriate in the context of established laws, and include well-established processes to contest allegations that observed outcomes are per se indicative of unlawful bias. Rather than coming up with new ways to conceive of unfair outcomes, CCIA strongly urges policymakers to focus on differentiating between reasonable and unreasonable sources of outcome disparities and to clarify what empirical evidence is required by whom to make or defend against allegations of discrimination.

Moreover, in the context of machine learning, there are frequently explicit tensions between avoiding unfair, differential treatment and addressing unfair outcomes. Policymakers should provide guidance for how to address concerns about achieving this tradeoff.

Privacy is best secured through anonymization, but it comes with a trade-off as full anonymity would strip data of all utility. Privacy-enhancing technologies (PETs), most notably differential privacy (DP), are key tools to minimize data processing. Rather than attempt data de-identification, which is increasingly difficult and susceptible to reverse engineering, PETs offer an array of tools to enable data minimization. PETs have significantly lowered the baseline of risk associated with handing over one's data and have made incremental increases in risk much smaller. Apple and Google already use DP in their respective mobile operating systems. Apple built DP into iOS 10 for all data collection and uses it for improving pre-installed applications like Notes and the keyboard.[4] Google, credited with developing federated learning, uses it for

[4] Andrea Scripa Els, *Artificial Intelligence as a Digital Privacy Protector,* 31 HARV. J.L. & TECH. 217, 221 (2017); Fang Liu, Ph.D., *A Statistical Overview on Data Privacy*, 34 Notre Dame J.L. Ethics & Pub. Pol'y 477, 478 (2020).

word recommendations on the Android keyboard.[5] The Agency should also account for the specific tradeoffs between privacy and security with the upcoming report, especially given how adversely impactful some technical mandates like rushed interoperability can be.[6]

B. Question 4. Existing Laws and Regulations

Although PETs enhance privacy by reducing the risk of identifiability, they come with a tradeoff that can sometimes be in tension with fairness. Applying PETs might make analyses of data less accurate with regard to components that represent smaller, historically-marginalized communities. This was a primary concern with the U.S. Government's decision to apply differential privacy to Census data.[7] At the same time, however, there may be instances in which PETs can enable privacy-protective insights into equity.

Absent federal comprehensive privacy legislation, states continue to take the lead in the privacy debate. Virginia's comprehensive privacy law may provide a helpful model[8] that represents an emerging consensus framework in the states, with Colorado, Connecticut, and Utah having passed laws with similar concepts. Virginia's law is characterized by key consumer privacy rights, like access, deletion, and correction, and includes foundational privacy concepts, like controller/processor designations.

The Agency can look to the National Institute of Standards and Technology (NIST) Special Publication 1270 – "Towards a Standard for Identifying and Managing Bias in Artificial Intelligence" – as a helpful resource to consult when attempting to address marginalized or underserved communities. PETs can play an important role in reducing the risk of identifiability in datasets, an important privacy protection. Privacy laws can help encourage and incentivize

---

[5] *Id.*

[6] *See* Mikołaj Barczentewicz, *Privacy and Security Implications of Regulation of Digital Services in the EU and in the US*, TTLF Working Paper No. 84, STANFORD-VIENNA TRANSATLANTIC TECH. L. FORUM (2022), http://law.stanford.edu/wp-content/uploads/2022/01/TTLF-WP-84_Barczentewicz.pdf ("A crude interoperability mandate could make it much more difficult for service providers to keep up with the fast- evolving threat landscape... Even today, email continues to be a source of security concerns due to its prioritization of interoperability").

[7] Fact Sheet, US Census Bureau, *Comparing Differential Privacy With Older Disclosure Avoidance Methods* (Aug. 12, 2021) https://www.census.gov/library/fact-sheets/2021/comparing-differential-privacy-with-older-disclosure-avoidance-methods.html.

[8] The Data Minimization principle helped Virginia achieve a balance that promotes innovation through its reasonably necessary standard. This would limit enforcement to data collection and uses that are unambiguously outside the bounds of this standard. *See* Virginia Consumer Data Protection Act, S.B. 1392 § 59.1-574. ("A controller limits the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer").

using PETs by exempting risk-reduced data from obligations that would otherwise apply. Various data protection schemes accomplish this by exempting anonymized data from definitions of personal data, but often those laws lack sufficient clarity around what anonymization actually means. Given the technical diversity of PETs – and the complexities and costs of using them – laws should seek to adopt a flexible approach to anonymization. Anonymization does not require reducing the risk of identifiability to absolute zero, but rather to a sufficiently remote level. The UK Information Commissioner's Office has begun to embrace such a flexible approach in their draft guidance on anonymization, and this could serve as a useful source of inspiration for other policymakers around the world.[9]

III. Impact of Data Collection and Processing of Personal Information

The internet is a revolutionary engine of economic growth and opportunity. This catalyst for innovation has empowered individuals with access to previously unreachable markets, creating agents for change in all sectors of society. Organizations across the digital ecosystem have used personal data to provide innovative services, and responsible data use can be beneficial for people, businesses, and society. But as the digital economy expands, more attention is rightfully being paid to the impact of data processing on consumers and how to maintain responsible and trustworthy treatment of personal information. Although companies continue to develop new data transparency tools and controls, CCIA urges Congress to adopt a baseline consumer privacy law to ensure that consumers' personal information is handled responsibly no matter where it is collected or who is processing it.

A. Question 2. Specific Examples of Disproportionate Impact

There is a fundamental tension between algorithmic fairness and privacy – pursuing algorithmic fairness measurements often requires having certain information, and data minimization principles often limit the collection of such information. For example, labeled data is often necessary for algorithmic fairness measurements, but research has revealed that across the industry labeled data is often not readily available for race, and is less available for other protected attributes.[10] As organizations work to responsibly navigate this trade-off between

[9] Draft, Information Commissioner's Office, *Chapter 2: How do we ensure anonymisation is effective?*(Oct. 2021) https://ico.org.uk/media/about-the-ico/documents/4018606/chapter-2-anonymisation-draft.pdf.
[10] https://www.bu.edu/articles/2022/race-ethnicity-data-gaps-delaying-antiracism-efforts/; https://www.bifrost.ai/post/its-2022-and-data-labeling-still-sucks.

privacy and fairness, the Agency has the opportunity to provide additional clarity to help organizations responsibly perform the measurements that are envisioned by the questions raised in the RFC.

NTIA should consider how data collection can continue to play a positive role in helping underserved and marginalized populations. The use of AI has helped to alleviate the overworked healthcare sector through data-driven diagnostics, identification of pandemics, and imaging diagnostics. More specifically, data collection has been critical for understanding and addressing healthcare disparities around the COVID-19 pandemic.[11] Unfortunately, however, these efforts remain limited where the lack of representation in datasets leads to systems underperforming for those populations. The Agency should consider how to encourage availability of robust datasets that more accurately reflect the diversity of populations being served.

Even amidst the challenges, these data-driven technologies can proficiently process massive amounts of data to create gains in productivity and accuracy, as well as create various efficiencies and consumer benefits in countless sectors.[12] One example is in the lending marketplace, where the use of AI has increased access to financial credit and lowered interest rates across demographic groups when compared to traditional models. These beneficial tools continue to be improved. For instance, Meta has launched its Variance Reduction System, which seeks to operate more equitably to reduce the risk of algorithmic discrimination, for housing ads and will expand the technology later this year to employment and credit ads.[13]

IV. Efforts to Prevent, Deter, and Remedy Harmful Behavior and Harmful Impacts

A. Question 5. Guiding Principles and Solutions

As the Agency continues to explore potential actions concerning automated decision-making, CCIA urges the focus to remain on securing protections for consumers concerning fully automated decisions that may have legal or other similarly significant effects on people's lives.

---

[11] Report, U.S. Department of Health and Human Services, *CDC Found Ways To Use Data To Understand and Address COVID-19 Health Disparities, Despite Challenges With Existing Data* (July 2022); Strategy, Center for Disease Control and Prevention, *CDC COVID-19 Response Health Equity Strategy: Accelerating Progress Towards Reducing COVID-19 Disparities and Achieving Health Equity* (May 18, 2022).

[12] Arash Aghlara*, Decision Automation Benefit*, FLEXRULE (Sept. 2020), https://www.flexrule.com/archives/decision-automation-benefits/.

[13] Roy L. Austin, *An Update on our Ads Fairness Efforts*, META (Jan. 9, 2023), https://about.fb.com/news/2023/01/an-update-on-our-ads-fairness-efforts/.

Both Virginia's comprehensive privacy law and the GDPR utilize this approach. The Agency should advise against adoption of rules that would unnecessarily restrict low-risk systems and tools that support ordinary business operations and transactions. Even where automated decision-making holds the possibility of producing legal or similarly significant effects on users, it is vital that context be considered. In such cases, consumers may still benefit, and if automated-decision making is turned off the risk of potential harm may accrue. Examples would be where a healthcare system uses an individual's address to select the closest ambulance dispatch location, or where fraud detection is relied upon in making financial or insurance decisions. Accordingly, to the extent certain uses of automated decision systems are restricted, there should be appropriate carve-outs for any processing relating to fraud prevention, anti-money laundering processes, screening, or for another type of security or compliance activities. Failure to do so would, for example, enable bad actors to avoid or opt-out of automated processes that detect and block their fraudulent activities, and limit companies' ability to protect customers' privacy and security.

The RFC asks about protections for children and teens regarding data harms. Children deserve enhanced security and privacy online. CCIA urges a comprehensive approach that draws on industry expertise in meeting the needs of children and parents. Age-specific regulations that require sites to collect and maintain additional sensitive data on all users, including detailed information on children, to comply with the law are counterproductive. Policymakers should recognize the importance of allowing platforms to foster age-appropriate experiences, balancing reasonable safeguards for teens with preserving their right to be online and benefit from access to information, communication, and expression. Civil liberties experts have cautioned against the unintended consequences of age-estimation requirements, including "potentially deterring vulnerable young people from finding online resources on sensitive issues like reproductive health or gender identity."[14] To strike this balance, many data privacy laws and regulations around the world apply the "best interests of the child" standard to how companies should handle young people's data, requiring them to provide age-appropriate experiences.

The RFC asks how to consider equity-focused approaches to privacy reform. It is often the case that fairness and equity-focused measures that policymakers contemplate tend to run

[14] Natasha Singer, *Children's Groups Want F.T.C. to Ban 'Unfair' Online Manipulation of Kids*, New York Times (Nov. 17, 2022), https://www.nytimes.com/2022/11/17/business/childrens-privacy-games-tom-tiktok.html.

counter to data minimization principles. Those sometimes-conflicting approaches should be considered in any policy framework to ensure a balance between achieving both objectives.

B. Question 6 - Alternative Actions

Industry and the advocacy community continue to collaborate on many of the difficult policy considerations relating to AI, including fairness, transparency, the future of work, and economic impacts.[15] The Agency can look at the National Institute of Standards and Technology's (NIST) AI Risk Management Framework, a voluntary and flexible framework that was the result of significant collaboration between government, industry, civil society, and other stakeholders. Additionally, the NIST AI Playbook helps organizations navigate and incorporate the frameworks' considerations, such as trustworthiness in the design, development, deployment, and use of AI systems.

CCIA recommends NTIA include policy prototyping in its recommendations. Policy prototyping provides an opportunity for stakeholders to experiment and test the effectiveness of a potential policy in a controlled environment – helping in turn to ensure that policies are well-informed and reflective of the needs and concerns of all stakeholders. This allows for iterative improvement, as well as the identification of unintended consequences before implementation.

C. Industry Efforts and Collaborations.

The tech sector continues to support meaningful engagement with all communities to learn and further develop products and services for the benefit of everyone. In particular, the efforts to help address the needs of the disability community have resulted in substantial progress.

Of the many industry initiatives, two broader efforts are particularly notable – the Speech Accessibility Project and Teach Access. Last year, in partnership with the University of Illinois at Urbana-Champaign (UIUC), Meta, Amazon, Apple, Google, Microsoft, the Davis Phinney Foundation, and Team Gleason launched the Speech Accessibility Project. This research initiative seeks to make voice recognition technology more useful for people with a range of diverse speech patterns and disabilities. Unfortunately, many modern speech recognition systems, such as voice assistants and translation tools, do not always recognize people with

[15] *See, e.g.,* Partnership on AI, which includes over 100 industry and advocacy members, conducting research and thought leadership to advance understanding of AI technologies, https://www.partnershiponai.org/.

speech patterns associated with disabilities. Through the Speech Accessibility Project, UIUC researchers will recruit paid volunteers representing a diversity of speech patterns to contribute recorded voice samples. These recordings will be used to create a private, de-identified dataset that can be used to train machine learning models to better understand a variety of speech patterns.

Unfortunately, computer science, design, and user experience degree programs often do not convey the importance of prioritizing accessibility. Teach Access has brought industry, academia, and advocacy stakeholders together to address this issue.[16] The initiative includes, among others, Verizon Media, Microsoft, Google, Meta, Apple, Stanford, Cornell, and Georgia Tech. Key to Teach Access is creating models for teaching and training students in technology-related fields how to create accessible experiences. Notably, Teach Access has launched an online tutorial covering best practices for accessible software design to advance accessibility training in higher education, intending to ensure that future technologies are "born accessible."

Beyond these initiatives, the tech sector continues to make significant progress in the field of captioning. For example, META's Automatic Alt Text (AAT) uses automatic photo description technology to recognize more than 1200 objects and concepts, generating descriptions that can be read aloud to people who are blind or with low vision through a screen reader.[17] More than 80% of images displayed on Facebook and Instagram now contain AAT.

[16] Teach Access has won a Heroes of Accessibility Award from Knowbility and received an Honorable Mention for the FCC Chairman's Award for Advancements in Accessibility.

[17] Newsroom, Meta, *Using AI to Improve Photo Descriptions for People Who Are Blind and Visually Impaired*, (Jan. 19, 2021), https://about.fb.com/news/2021/01/using-ai-to-improve-photo-descriptions-for-blind-and-visually-impaired-people/.

V. Conclusion

CCIA applauds NTIA for conducting this public comment process. CCIA encourages NTIA to continue seeking broad engagement and input from stakeholders and the public on ways to approach the civil rights and equity implications of modern data collection and processing.

Respectfully submitted,

Alvaro Marañon
Policy Counsel
Computer & Communications Industry Association
25 Massachusetts Avenue NW, Suite 300C
Washington, DC 20001
amaranon@ccianet.org

March 6, 2023