U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

March 6, 2023

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Washington, DC 20230

Re: Request for Comment, National Telecommunications and Information Administration, Department of Commerce; Privacy, Equity, and Civil Rights; 88 Fed. Reg. 3714-3720 (January 20, 2023)

To Whom It May Concern:

The U.S. Chamber of Commerce's Technology Engagement Center ("C_TEC") appreciates the opportunity to submit feedback to the National Telecommunications and Information Administration in response to its request for comment on addressing issues at the intersection of privacy, equity, and civil rights.

C_TEC appreciates NTIA's ongoing work to bring together individuals, organizations, and associations who understand the importance of working together to discuss and address these critical matters. Furthermore, we appreciate the opportunity to provide input to help further inform the agency on how technology provides better outcomes for all, specifically those who live in marginalized or disadvantaged communities.

C_TEC continues to be concerned with the growing patchwork of state privacy laws. A complex state privacy patchwork of 50 laws could cost companies over $1 trillion—and $200 billion[1] for small businesses. With costs like these, the United States would have difficulty competing internationally if its companies have multiple sets of privacy rules to follow while other countries take a more unitary approach. This is why the U.S. Chamber continues to advocate for Congress to pass a preemptive comprehensive national data privacy bill. Consumers deserve strong privacy protections and innovative products and services. Businesses need certainty, uniformity, and protection against abusive litigation. It is for this reason that the Chamber supports national privacy legislation that does all these things.

C_TEC looks to provide the following feedback on the request for comment on "Privacy, Equity and Civil Rights"

[1] https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws/

Framing:

1. *How should regulators, legislators, and other stakeholders approach the civil rights and equity implications of commercial data collection and processing?*

a. *Is "privacy" the right term for discussing these issues? Is it under-inclusive? Are there more comprehensive terms or conceptual frameworks to consider?*

Naming the civil rights and equity implications of commercial data collection and processing as a "privacy issue" only is under-inclusive as it extends beyond privacy, cutting across consumer protection, truth in advertising, and the potential for discriminatory impact of personalized marketing practices. To effectively build a framework that can evolve along with the uses of commercial data, stakeholders will need to look not only at the potential harms and implement protections against those harms but also at the benefits that many consumers gain from the very uses of data that legislators and regulators might undercut by restricting uses of data without taking a thoughtful (and inclusive) approach.

b. *To what degree are individuals sufficiently capable of assessing and mitigating the potential harms that can arise from commercial data practices, given current information and privacy tools? What value could additional transparency requirements or additional privacy controls provide; what are examples of such requirements or controls; and what are some examples of their limitations?*

As privacy legislation and regulatory enforcement activity have proliferated and evolved, so have the transparency practices of companies who leverage commercial data to provide the right product to their audience. These newly developed transparency requirements and privacy controls result in a more educated consumer base. For example, the average consumer now understands that information is being gleaned from online activity.

While the "new wave" of state privacy legislation, such as Virginia, does hold companies to a better transparency standard in their data practices and privacy controls, there is a delicate balance between providing the right amount of openness and over-informing consumers which leads to engagement exhaustion or "notice fatigue." In reaction to this fatigue and exhaustion, consumers are prone to assent without any aforethought by clicking on the consent button or simply abandoning their consumer journey. Policymakers should understand that imposing more transparency

requirements and privacy controls could exacerbate this fatigue and exhaustion, causing consumers to engage less. Accordingly, the disclosure must be targeted and meaningful. Policymakers should look for ways to empower consumers, such as providing them with the right to access their data and requesting a copy of the personal information that an organization collects about them so they can make informed decisions about their privacy. Technical mandates that restrict how this information is shared often are too restrictive and can lead to poor design. Still, companies should be incentivized to make this information readable, accessible, and actionable.

c. *How should discussions of privacy and fairness in automated decision-making approach the concepts of "sensitive" information and "non-sensitive" information, and the different kinds of privacy harms made possible by each?*

As privacy legislation has evolved, there has been a corresponding erosion of the distinction between sensitive and non-sensitive information. This is due to the use of the big data sets that automated decision-making mainly relies on – a company can infer so much sensitive information from the big data sets that are being used.

Instead of categorizing certain data sets as sensitive or not, discussions of privacy and fairness in automated decision-making should focus on regulating harms rather than regulating the types of data that are being used. Policymakers should understand that information characterized as sensitive may be necessary to measure or identify approaches to mitigating issues (e.g., to monitor algorithms for bias) even if an underlying system is not collecting or processing sensitive data. An overinclusion of types of data of what is considered sensitive –paired with prohibitions on the use of "sensitive data" could make it more difficult for technology developers to train and test applications for fairness.

It is important to highlight that there are already applicable sector-specific laws on the books around using "sensitive" information. For example, in the healthcare sector, health data must follow the requirement of the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. It's vital that policymakers understand that there are many of these primary legal frameworks already in place that protect the use of sensitive information.

d. *Some privacy experts have argued that the collective implications of privacy protections and invasions are under-appreciated.[28] Strong privacy protections for individuals benefit communities by enabling a creative and innovative democratic society, and privacy invasions can damage*

communities as well as individuals. What's more, many categories of extractive and profitable processing rely on inferences about populations and demographic groups, making a collective understanding of privacy highly relevant.[29] How should the individual and collective natures of privacy be understood, both in terms of the value of privacy protections; the harms of privacy invasions; and the implications of those values and harms for underserved or marginalized communities?

The collective implications for privacy protections and potential invasions are not under-appreciated. Recent rhetoric only highlighting negative implications of data use has harmed policymakers' and society's ability to engage in meaningful discourse on the matter. This is why it is essential to encourage a discourse also highlighting the benefits to consumers and businesses derived from the commercial use of large data sets. For example, a small business that has a social media presence can grow its local presence to a receptive audience in a new and meaningful way because of the audience segmentation and advertisement personalization.[2] Consumers receive ads relevant to their interests. Businesses get consumers to buy their products.

Rather than assigning negative connotations to all commercial uses of data, legislators and regulators should focus on creating legislation or taking regulatory enforcement action aimed at reducing the harms to consumers including underserved or marginalized communities. For example, instead of prohibiting the use of commercial data to determine creditworthiness, policymakers should create frameworks that ensure entities using commercial data to determine creditworthiness will not do so in a way that unfairly harms underserved or marginalized communities while enabling them to retain the benefits of data analysis like inclusivity scores that help target solutions to societal problems. [3]

e. *How should proposals designed to improve privacy protections and mitigate the disproportionate harms of privacy invasions on marginalized communities address the privacy implications of publicly accessible information?*

Policymakers should incentivize the development of frameworks that entities can use to build governance into their uses of commercial data to ensure that the resulting outputs of such commercial data will not result in disparate impact or treatment of a protected class rather than prohibiting the use of commercial data wholesale. At the same time, policies related to publicly-available data should respect First Amendment protections.

---

[2] https://americaninnovators.com/wp-content/uploads/2022/08/Empowering-Small-Business-The-Impact-of-Technology-on-U.S.-Small-Business.pdf

[3] https://americaninnovators.com/wp-content/uploads/2020/01/CTEC_DataForGood_v4-DIGITAL.pdf

f. *What is the interplay between privacy harms and other harms that can result from automated decision-making, such as discriminatory or arbitrary outcomes? How should these two issues be understood in relation to one another in the context of equity and civil rights concerns?*

There is no denying that there is a direct relationship between data and the outcomes of automated decision systems. For this reason, it is critical that these systems are trained on robust and sound data. It is essential that policymakers look for opportunities to open up data sets to assist in helping to mitigate any negative impacts.

g. *Civil rights experts and automated decision-making experts have raised concerns 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. How should regulators, legislators, and other stakeholders think about the differences between intentional discrimination and unintentional discrimination on the basis of protected characteristics, such as race or gender? How do data practices and privacy practices affect each?*

The Chamber recommends that policymakers take into account frameworks and tools that already exist when thinking about how to mitigate possible discrimination. Policymakers should also not conflate the concepts of disparate impact and disparate treatment.[4] The business community does recommend policymakers advance the following:

- Open Data: Regulators and legislators can address potential harm regarding automated decision-making systems by making government data that does not contain PII available for training. Rich and diverse data sets which represent the consumer base can help improve systems.

- Best-Practices: There are clear tensions between avoiding unfair or differential treatment and tackling unfair outcomes in the context of machine learning. Considering these tensions, policymakers should rely on industry best practices (existing and the development thereof) to develop on how to address these concerns.

- Riskbased-Approach : Regulators and legislators should not treat every instance of potential bias the same. Risk-based assessments of automated decision systems are critical to governance. The stakes of someone applying for

[4] https://americaninnovators.com/wp-content/uploads/2020/01/CTEC_DataForGood_v4-DIGITAL.pdf

a mortgage are much higher than a customized playlist. By having companies assign risk and have policies that respond to the level of risk, we can better capture and mitigate harmful systems.

- Encourage Flexibility in Testing: Regulators must provide flexibility to organizations to test their systems in ways that allow them to proactively look at new ways to reduce potential discrimination within these systems. Organizations should also be given a safe harbor that incentivizes testing and allows for mitigation and correction.

That said, it is essential to highlight the importance of policymakers not treating unintentional bias in the same way as intentional discrimination. Because of the subtlety around automated decision systems and bias, laws that treat these different types of discrimination as the same incentivize organizations deploying automated decision systems not to try to discover potential bias as they may be at risk of being legally liable. Treating unintentional bias as intentional discrimination would dramatically reduce industry's willingness to use automated decision systems, denying society the immense benefits that many of these technologies hold.

Impact of Data Collection and Processing on Marginalized Groups

2. *Are there specific examples of how commercial data collection and processing practices may negatively affect underserved or marginalized communities more frequently or more severely than other populations?*

C_TEC would urge NTIA to consider how data collection can help marginalized and underserved communities. It plays an essential role for identifying and addressing health disparities, and for ensuring that AI models can be trained on representative data sets. Data has a great opportunity to help highlight cycles or patterns which may be negatively affecting these communities. For example, in the case of the COVID-19 pandemic, data collection has been critical for understanding healthcare disparities. Furthermore, there are cases where the lack of representation in datasets leads to systems underperforming for those populations.

c. *How do specific data collection and use practices potentially create or reinforce discriminatory obstacles for marginalized groups regarding access to key opportunities, such as employment, housing, education, healthcare, and access to credit?*

Data should not be used to discriminate or to have adverse impacts on a person or community. However, it's important to highlight that consumer data about protected classes—like race and gender for example—are essential for organizations to identify

and mitigate if disparities are present, and to improve equitable outcomes. This is why we stress the importance of government entities opening up government data sets that can assist with this work. Through the government opening up demographic information, we can help support systems looking at reducing disparities and helping improve outcomes such as the use of public health initiatives.

3. Are there any contexts in which commercial data collection and processing occur that warrant particularly rigorous scrutiny for their potential to cause disproportionate harm or enable discrimination?

a. In what ways can disproportionate harm occur due to data collected or processed in the context of evaluation for credit; healthcare; employment or evaluation for potential employment (please include consideration of temporary employment contexts such as so-called "gig" or contract workers); education, or in connection with evaluation for educational opportunities; housing, or evaluation for housing; insurance, or evaluation for insurance; or usage of or payment for utilities?

The context of how the data is being used is necessary to answer whether the data could cause harm. For example, using sensitive or demographic data to improve organizational diversity is widely considered a best practice. Using that same data to drive untested evaluation processes that could negatively affect an individual's access to employment, credit, and healthcare can create long-lasting harm.

Regarding the temporary worker context, workers who pursue this type of career do so partially because it allows them to have other work as well, which must be considered when assessing harm. Data processing done on gig work platforms is also limited in impact because that data only impacts the experience on the platform. Insurance, home loans, and credit scoring data are all shared and used for other decisions that can follow and further impact the user.

The business community agrees that all organizations using data in these contexts should conduct rigorous internal privacy assessments to determine potential inadvertent disparate impact caused by their products and services.

Existing Privacy and Civil Rights Laws

4. How do existing laws and regulations address the privacy harms experienced by underserved or marginalized groups? How should such laws and regulations address these harms?

d. Are there situations where privacy law conflicts with efforts to ensure equity and protect civil rights for these communities? If so, how should those conflicts be addressed?

One of the major conflicting issues in addressing equity is having good and accurate data to help test the systems to eliminate and mitigate any potential bias. Testing algorithms for bias by protected classes requires having data on protected classes. Many privacy laws block companies' ability to identify, monitor, and rectify disparities. The solution to this conflict is straightforward. Companies should not be banned from collecting demographics for the purpose of discrimination testing.

Furthermore, it's important to highlight that the use of things such as privacy-enhancing technologies (PETs) can enhance privacy by reducing the risk of identifiability but simultaneously can sometimes be in tension with fairness. Applying PETs might make data analyses less accurate for smaller, historically marginalized communities represented in it. This was a primary concern with the U.S. Government's decision to apply differential privacy to Census data. At the same time, though, there may be instances in which PETs can enable privacy-protective insights into equity.

f. Legislators around the country and across the globe have enacted or amended a number of laws intended to deter, prevent, and remedy privacy harms. Which, if any, of these laws might serve as useful models, either in whole or in part? Are there approaches to be avoided? How, if at all, do these laws address the privacy needs and vulnerabilities of underserved or marginalized communities?

The U.S. Chamber has long advocated for a comprehensive national data privacy law that provides strong preemption to eliminate a potential patchwork of state laws. There is a pressing need for clear and comprehensive horizontal privacy rules that protect all consumers and businesses. However, if Congress were to look at existing state models, we highly encourage them to look at Virginia's comprehensive privacy law. This framework– which has influenced other states including Utah, Colorado, and Connecticut– is characterized by crucial consumer privacy rights, like access, deletion, and correction, and includes foundational privacy concepts, like controller/processor designations.

It's also important to highlight that agencies that have been provided congressional authority to regulate specific sectors should be the specific regulating agency when it comes to AI. Industries such as the financial services sector already have extensive regulatory requirements that help them to appropriately manage the implementation of AI (e.g., GLBA, ECOA, Reg B, etc.). In addition, the "Model Risk Management Guidance" released by the OCC, Fed, and the FDIC requires banks to develop effective model risk management frameworks, including robust model

development, implementation, and use; effective validation; and sound governance. This required (and carefully implemented) use of AI in banking results in higher efficiencies from automating banks' internal processes and increases and accelerates innovation, thus enhancing the customer experience (e.g., providing customers with instant credit application decisions). AI is a critical resource in the financial services industry.

Regardless of sector, approaches to regulating data-driven technologies, including AI, should focus on principles-based frameworks which define a flexible approach that can evolve as AI evolves. To ensure consistency and legal certainty with respect to existing laws, any new AI framework or policy should not contradict or duplicate existing legislation but rather build upon it.

g. Are there any privacy or civil rights laws, regulations, or guidance documents that demonstrate an exemplary approach to preventing or remedying privacy harms, particularly the harms that disproportionately impact marginalized or underserved communities? What are those laws, regulations, or guidance documents, and how might their approach be emulated more broadly?

C_TEC would like to highlight the following guidance documents, which can help remedy any potential harm.

- NIST's Special Publication 1270 ("Towards a Standard for Identifying and Managing Bias in Artificial Intelligence") can be a helpful resource to consult.

- NIST's AI Risk Management Framework

- PETs can play an essential role in reducing the risk of identifiability in datasets, which is important for privacy protection. Privacy laws can help encourage and incentivize using PETs by exempting risk-reduced data from obligations that would otherwise apply. Many existing data protection schemes exempt anonymized data from definitions of personal data, but often those laws lack clarity around precisely what anonymization means. Because of the technical diversity of PETs—and the complexities and costs of using them—laws should adopt a flexible approach to anonymization. They should recognize that 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.

h. What is the best way to collect and use information about race, sex, or other protected characteristics to identify and prevent potential bias or discrimination, or to specifically benefit marginalized communities? When should this occur, and what safeguards are necessary to prevent misuse?

There are various approaches to collecting demographics to test for discrimination. In general, such collection should be broadly allowed for the purpose of discrimination testing. Companies should also be encouraged to collect demographics in different ways – by geography, by inference, by self-report, in conjunction with non-profits. A recent AHRQ study on "Impact of Healthcare Algorithms on Racial and Ethnic Disparities in Health and Healthcare" found that "disparities were reduced when race and ethnicity were incorporated in an intentional effort to tackle known racial and ethnic disparities in resource allocation."

Furthermore, it's important to highlight that each approach has limitations. For example, self-reporting suffers from non-response bias that may systematically underreport the discrimination faced by marginalized groups. By using several approaches, discrimination testing can be most robust.

Finally, we believe it is important for the use of data to be transparent and that consumers have an understanding of the following.

- why they are being asked to share personal information related to protected characteristics
- how that information is collected, used, and stored
- how the data sharing benefits them as a user
- what happens if they do not share their data. If the answer to 'what happens if I do not share my data' includes factors that impact access, cost, or disparate customization, then a company has not created meaningful choice, and therefore may be demanding a privacy compromise as a tradeoff for receiving a service that should be a right. Companies should build meaningful choice into their products in such a way that the sharing of personal information benefits the user and the company, and does not require the user to sacrifice access or autonomy if they choose not to agree to data collection.

Solutions

5. What are the principles that should guide the Administration in addressing disproportionate harms experienced by underserved or marginalized groups due to commercial data collection, processing, and sharing?

a. Are these principles reflected in any legislative proposals? If so, what are those proposals, and how might they be improved?

We would like to highlight that both Virginia's comprehensive privacy law and GDPR are instructive with respect to the need for limiting obligations for profiling/automated decision systems to cases where the automated decision system produces a legal or similarly significant effect on an individual.

d*. In considering equity-focused approaches to privacy reforms, how should legislators, regulators, and other stakeholders approach purpose limitations, data minimization, and data retention and deletion practices?*

It is often the case that fairness and equity-focused measures that policymakers contemplate actually run counter to data minimization principles. Those sometimes conflicting approaches ought to be considered in any policy framework to ensure a balance between both objectives.

Regulators should also take a risk-based, non-prescriptive approach to strike the appropriate balance. When considering the risks AI systems pose, regulators should focus on the activities (or outcomes) of the AI, as opposed to blanket regulations on the technology (e.g., facial recognition used to surveil a crowd poses a different risk than facial verification used to authenticate an individual opening a mobile application).

e. Considering resources, strategic prioritization, legal capacities and constraints, and other factors, what can federal agencies currently do to better address harmful data collection and practices, particularly the impact of those practices on underserved or marginalized groups? What other executive actions might be taken, such as issuing executive orders?

The Administration – through its federal agencies – should encourage the public and private sector to test for discrimination by creating a safe harbor from enforcement actions, as has been done in other jurisdictions (*see* MASS. GEN. LAWS ch. 149, § 105A(d)). This safe harbor will encourage companies and state and local government agencies to test and mitigate disparities proactively. This is especially important because the collection of demographic data and the execution of disparate impact testing can create legal risks for a company.

6. What other actions could be taken in response to the problems outlined in this Request for Comment include?

We would urge NTIA to include policy prototyping as part of its policy recommendations. Policy prototyping provides an opportunity for stakeholders to experiment and test the effectiveness of a potential policy in a controlled environment – helping 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*. What roles should third-party audits and transparency reporting play in public policy responses to harmful data collection and processing, particularly in alleviating harms that are predominantly or disproportionately experienced by marginalized communities? What priorities and constraints should such mechanisms be guided by? What are the limitations of those mechanisms? What are some concrete examples that can demonstrate their efficacy or limits?*

As legislatures and agencies consider the possibility of regulating, they must be aware that technology is continually developing and the current processes to mitigate potential bias or concerns could become obsolete. This risk of obsolescence is why the Chamber discourages the use of one-size fits all solutions such as third-party audits. While outside assistance should never be discouraged, it should be noted that there is a well-documented risk of engaging third-party auditors. Given that there currently are no standards and certifications regarding third-party auditors, there is no guarantee that reviewers can deliver verifiable measurement methods that are valid, reliable, safe, secure, and accountable. Furthermore, there are further additional issues around potential trade secrets being unveiled, as we all as opening data that could open up further privacy concerns.

d*. What role could design choices concerning the function, accessibility, description, and other components of consumer technologies play in creating or enabling privacy harms, particularly as disproportionately experienced by marginalized communities? What role might design play in alleviating harms caused by discriminatory or privacy-invasive data practices?*

To best address discriminatory and privacy-invasive data practices, companies need to voluntarily implement a culture of privacy by design and consider fairness throughout the lifecycle of the product. This cannot be simply written into law as it is highly context specific. Having sector-specific sets of best practices should be encouraged in navigating how to serve various communities.

To better understand (and mitigate) potential disparate impact on systematically excluded communities, it is imperative to have demographic and behavioral data with which to measure. Data, of course, can be used in numerous

ways, so depending on all the ways this collected data is used, some might enable harm. A federal privacy law would provide clear guidance on the collection of data. Any law around this should provide guardrails, as well as safe harbors for using data to measure impact to systemically excluded communities and provide for mitigations.

Expanding the definition of design choices to include the design of user research would be helpful in addressing discriminatory impact. The implicit or explicit exclusion of certain communities in any and all studies, and therefore their perspectives, needs, goals, etc., can be one of the leading causes of harm. The missing perspectives, typically of systemically excluded communities, allows teams to make decisions based on historically overrepresented groups — removing the majority of the world's population from their strategy. This lack of awareness and holistic perspective would inevitably lead to exclusive, inaccessible, unsafe, harmful experiences. In contrast, to alleviate these issues, teams must deeply understand systemic oppression and inequality and that every decision that is made, is likely being made on top of one that is persisting exclusion. Doing this includes, but is not limited to, hiring a diverse team, ensuring diversity of research participants, shifting power from the designers and builders to the customer, seeing each and every individual user as an expert in their own lived experiences, and co-creating solutions alongside them.

e. What role should industry-developed codes of conduct play in public policy responses to harmful data collection and processing and the disproportionate harms experienced by marginalized communities? What are the limitations of such codes?

Creating a code of conduct on an industry basis for use of AI and other data-driven technologies would give participants in the code of conduct flexibility to leverage data through novel technologies while at the same time ensuring that entities leveraging such technologies implement a gold-standard set of principles to protect the data being used. The aim of any such code of conduct would be to make it easier for industries to engage with technologies that tackle some of the biggest issues in our economy. In fact, some industries, such as the financial services sector, has already worked with regulators to create and implement guidance that sets such rules: the "Model Risk management Guidance" released by the OCC, Fed, and the FDIC. The guidance itself acts as a code of conduct that banks can apply to ensure that they are choosing safe, effective, and secure technology to improve the services they provide.

Conclusion

The Chamber stands ready to work with you on ways the federal government can help lift up communities. We believe that this can be done by fostering public trust in technology and assisting in the responsible development, deployment, and use

of trustworthy technology that protects Privacy, Equity, and Civil Rights. The U.S. Chamber has long recognized the importance of the government and private sector working together to address issues of public concern. We stand committed to working to address these challenges, protecting against harmful biases, and respecting human rights.

Sincerely,

Michael Richards
Director
Chamber Technology Engagement Center
U.S. Chamber of Commerce