CIPL's Response to NTIA Privacy, Equity, and Civil Rights Request for Comment

Docket No. NTIA-2023-0001

Submitted March 6, 2023

I. Executive Summary and Key Recommendations

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to comment on issues at the intersection of privacy, equity, and civil rights as the National Telecommunications and Information Administration (NTIA) gathers information to prepare a report on whether and how commercial data practices can lead to disparate impacts and outcomes for marginalized or disadvantaged communities.

As reflected by the NTIA in its first question—"Is 'privacy' the right term for discussing these issues?"[2]—CIPL views the civil rights implications of commercial data practices as questions focusing more on **data use** than on data privacy. Although privacy concerns are certainly related to data uses, the questions raised are more accurately characterized as ones addressing responsible data practices.

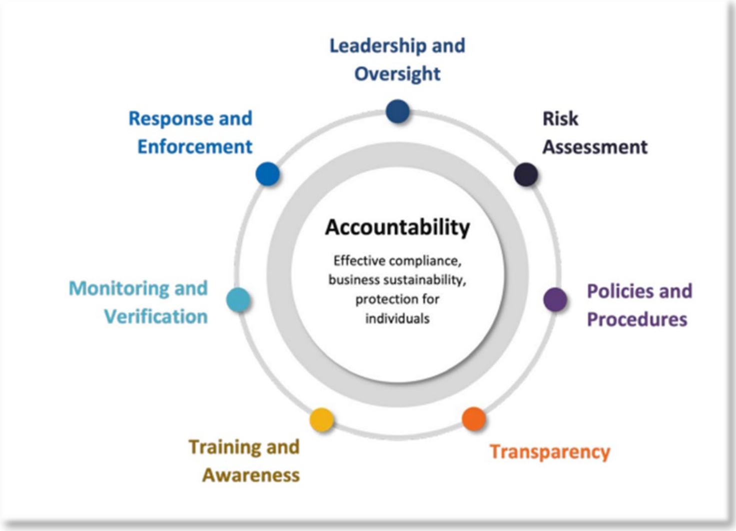
CIPL has a long history of promoting responsible data practices through its efforts regarding organizational accountability. Indeed, CIPL's Accountability Framework,[3] at its core, is a blueprint for responsible data practices. By encouraging organizations to implement and demonstrate accountability, CIPL has sought to ensure not only that organizations comply with applicable legal requirements and best practices but also that organizations improve societal trust in their legitimate and beneficial uses of data.

Figure 1. The CIPL Accountability Framework

[1] CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 85+ member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[2] Privacy, Equity, and Civil Rights Request for Comment, NTIA, 88 FR 3714, at 3718, (January 20, 2023), available at https://www.federalregister.gov/documents/2023/01/20/2023-01088/privacy-equity-and-civil-rights-request-for-comment.

[3] See CIPL resources and papers on organizational accountability: https://www.informationpolicycentre.com/organizational-accountability.html.



Source: CIPL

Among other practices covered by the above framework, accountability expressly requires organizations to perform contextual risk assessments on their data uses that identify not only potential harms to individuals but also appropriate protective measures to minimize the risks. As noted in CIPL's recent response to the Federal Trade Commission's Advance Notice of Proposed Rulemaking on Commercial Surveillance and Data Security,[4] contextual risk assessments can help determine whether a particular use in a given context will adversely affect different groups of consumers in different sectors or in different segments of the economy.

Contextual risk assessments are well suited to identify and address the impact of data uses on marginalized or underserved communities. Given that certain data uses can and do adversely affect those communities, organizations should include such considerations within the scope of their risk assessments. Of course, compliance with legal obligations should already be part of any risk assessment, and civil rights obligations in particular must be addressed to prevent illegal discrimination. Federal law clearly prohibits racial discrimination in employment, housing, and credit opportunities, and risk assessments addressing data uses in those contexts should specifically ensure compliance with those laws.

However, to the extent data is used in other contexts—i.e., in contexts that do not specifically violate civil rights laws—a contextual risk assessment would help identify not only potential harms to members of a particular group, but also appropriate measures to mitigate those harms. Thus, where marginalized or underserved communities are, in NTIA's words, "materially disadvantaged regarding … the effort required to adequately manage privacy controls [and] … at increased risk of privacy losses or data misuse,"[5] a properly calibrated risk assessment would help identify such potential effects or

[4] CIPL Comments on the FTC's ANPR on Commercial Surveillance and Data Security, response to Q12, page 25, Nov. 21, 2022, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_ftc%E2%80%99s_anpr_on_commercial_surveillance_and_data_security__21_nov_2022_.pdf.

[5] Privacy, Equity, and Civil Rights Request for Comment, NTIA, 88 FR 3714, at 3715, (January 20, 2023), available a`t https://www.federalregister.gov/documents/2023/01/20/2023-01088/privacy-equity-and-civil-rights-request-for-comment.

harms in the context of a given data use as well as enable appropriate safeguards to prevent or mitigate them.

An accountability-based framework for data use can enable full compliance with hard legal requirements, including those grounded in civil rights, as well as enable contextual prioritization of compliance measures and safeguards that are tailored to the specific degree of risk. It also enables mitigations that are consistent with preserving as much as possible the intended benefits of the intended data uses. Thus, organizational accountability focuses on the mitigation of *actual* risks to individuals and helps avoid unnecessary safeguards that undermine legitimate uses while facilitating strong safeguards in high-risk cases. As such, it is an indispensable tool for enabling responsible and beneficial data uses. While CIPL's Accountability Framework was initially developed to help mitigate risks related to privacy harms, our framework and the risk assessments it entails can have broader application and can help address risks associated with any data use, including harms impacting marginalized or underserved communities. CIPL's forthcoming report on the adoption of a holistic data strategy by corporate boards will explore this topic in greater detail.[6]

Any regulatory framework designed to prevent the wide range of potentially harmful impacts of data uses should enable and require organizations to conduct such risk assessments for their relevant data processing operations. Moreover, it should require organizations to be able to **demonstrate** to the regulatory authority upon request how those risk assessments were conducted and to **explain** and **validate** their processing decisions based on those assessments.

A risk assessment does not address whether **certain types of data should be used generally or at all**, but rather whether **the data can be used responsibly and with appropriately tailored protections in a specific context and for a specific purpose.**

Recent scholarship by Professor Daniel Solove stresses this point in the context of a discussion regarding the classification of certain data types as "sensitive."[7] Professor Solove states that instead of focusing on the **nature** of data—i.e., providing heightened protections for data deemed sensitive (such as racial or ethnic origin, religious beliefs, or sexual orientation)—laws should focus on **use**, **harm**, and **risk**:

> This Article argues that the problems with the sensitive data approach make it unworkable and counterproductive—as well as expose a deeper flaw at the root of many privacy laws. These laws make a fundamental conceptual mistake—they embrace the idea that the nature of personal data is a sufficiently useful focal point for the law. But nothing meaningful for regulation can be determined solely by looking at the data itself. **Data is what data does. Personal data is harmful when its use causes harm or creates a risk of harm. It is not harmful if it is not used in a way to cause harm or risk of harm.**[8]

By emphasizing that it is the **use** of data that matters, not whether it is sensitive or non-sensitive, Professor Solove recognizes that there may be appropriate and beneficial uses of data commonly

[6] Provisionally titled "Leveraging Data Responsibly: Why Boards and the C-Suite Need to Embrace a Holistic Data Strategy." Upon its anticipated publication in April 2023, CIPL will share this report with the NTIA.

[7] Solove, Daniel J., *Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data* (January 11, 2023), available at https://ssrn.com/abstract=4322198.

[8] *Id.* p. 4 (emphasis added).

regarded as sensitive: "If privacy laws fail to focus on use, harm, and risk, then they can perversely impede beneficial uses of data."[9]

Citing an article published by the International Association of Privacy Professionals (IAPP),[10] Professor Solove notes that restrictions on data about race, for example, may threaten the ability of marginalized groups to access digital content. "[E]ven though businesses may collect and share sensitive personal information for reasons beneficial for underrepresented communities, they may make a financial decision to stop doing so to avoid creating new compliance obligations implicated by collecting and disclosing sensitive information."[11] If online publishers avoid creating, selling and/or using audience segments composed of individuals interested in issues impacting people of color and other historically underrepresented groups, "economically disadvantaged communities will lose access to, among other things, valuable educational content regarding identity and ideologies, information regarding how they can get involved in social justice causes, and a medium to express their thoughts on these issues."[12]

As stated by CIPL in its response to a U.K. government proposal on the regulation of artificial intelligence (AI),[13] data based on race, ethnicity, and gender is necessary to prevent and detect bias in algorithms. Denying access to, or preventing retention of, such data will only make it harder to detect and remedy bias while also denying all segments of society the full potential of AI's benefits.[14]

Thus, it is important to remember that not all collection and uses of data related to race, religion, or sexual orientation are bad or harmful. While CIPL agrees that certain uses of data may have an adverse impact on marginalized or underserved communities, an accountability-based risk assessment will be able to identify such impacts and distinguish appropriate uses from inappropriate ones and will enable appropriate safeguards.

In sum, CIPL endorses the adoption of organizational accountability measures that include **contextual risk assessments** to help companies:

- evaluate the sensitivity of data and data uses in context, along with the attendant level of risk;
- identify high-risk processing and tailor compliance and mitigation measures to such risk;
- identify legitimate and beneficial uses of data;
- evaluate individual, organizational, and societal benefits of data uses, especially those affecting marginalized or underserved communities; and

[9] *Id.* p. 46.

[10] Dominique S. Leipzig, Arsen Kourinian, David Biderman & Tommy Tobin, Ambiguity in CPRA Imperils Content Intended for Underrepresented Communities, IAPP (Feb. 17, 2021), https://iapp.org/news/a/ambiguity-over-california-privacy-law-imperils-content-intendedfor-underrepresented-communities/.

[11] *Id.*

[12] *Id.*

[13] CIPL's Response to UK Department for Digital, Culture, Media and Sport (DCMS) Policy Paper on Establishing a Pro-innovation Approach to Regulating AI (September 23, 2022) available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_uk_dcms_proposed_approach_to_regulating_ai_23_09_22.pdf.

[14] *Id.*, p. 2.

- document their risk assessments and compliance and mitigation measures and be able to explain their processing decisions under relevant legal standards.

II. Specific Questions

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

1a. Is "privacy" the right term for discussing these issues? Is it under-inclusive? Are there more comprehensive terms or conceptual frameworks to consider?

As mentioned above, CIPL views the civil rights implications of commercial data practices as questions focusing more on **data use** than on data privacy. Although privacy concerns are certainly related to data uses, the questions raised are more accurately characterized as ones addressing responsible data practices.

1b. 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?

In the modern digital society, individuals generally may not be the best placed to protect themselves against harmful data uses. That responsibility must lie primarily with organizations. CIPL's Accountability Framework requires organizations to take concrete steps to operationalize data governance and compliance with privacy and other data-related laws to protect individuals in all contexts independent of consent requirements.

That said, the fact that individuals should not have primary responsibility to protect themselves from harm in the digital society and economy does not mean that their agency and ability to choose should not be enabled where it is meaningful, appropriate, and possible. Indeed, where choice is appropriate, requirements and controls focusing on transparency to enable it are important components of a privacy and data management program. Thus, in addition to the risk assessment and mitigation measures mentioned above, the accountability framework requires organizations to provide transparency to stakeholders internally and externally about the organization's data privacy program, procedures, and protections; the rights of individuals in relation to their data; and the benefits and/or potential risks of data processing. This may include providing actionable transparency for specific situations where asking for consent or giving choices may be appropriate, such as deciding with whom to share social media posts, or responding to a market research survey or to an employee engagement survey that seeks data in protected categories. In cases where consent could be effective, it may not have to be affirmative or express consent; consent may be deemed or implied in situations where processing is low risk and within the reasonable expectations of individuals.

CIPL also stresses that even where it would be practicable to obtain, consent may not always be the best or only way to empower individuals.[15] Other ways to empower individuals include

[15] See *Empowering Individuals Beyond Consent*, by Bojana Bellamy and Markus Heyder, July 2, 2015, available at https://iapp.org/news/a/empowering-individuals-beyond-consent/.

providing user-centric transparency about relevant data practices and providing access and correction rights with respect to consumers' personal data. Access and correction and related individual rights are common in global privacy laws, and they should be considered in the U.S. as well. Most importantly, however, placing the onus on organizations to be accountable in their data privacy management practices—especially through the use of risk assessments and risk mitigation measures—is key to protecting individuals from substantial harms.

1c. 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 noted above, an accountability-based framework does not focus on particular **types** of data—e.g., whether it is "sensitive" or "non-sensitive"—but rather on the **use** of the data in a specific context. Indeed, even uses of so-called "non-sensitive" data could have "sensitive" effects. By focusing on the **use**—and whether that use creates adverse, unjustifiable, or unfair effects on individuals—potential harms can be identified and mitigated. The risk assessment addresses whether **the data can be used responsibly and with appropriately tailored protections in a specific context and for a specific purpose.** Indeed, in some contexts, data categorized as "sensitive" may be used for beneficial purposes, such as actively countering discrimination and advancing equity.

1e. 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?

Whether data is publicly accessible or not, the focus should be on the **specific use case** and potential harms therein, including potential harms that could result from a combination with other sources of data.

1g. 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?

An accountability-based framework requires not only the identification of potential harms (including unintended harms) associated with a specific use case, but also the implementation of appropriate mitigation measures. By requiring organizations, private or governmental, to be able to explain their risk assessments and processing decisions based on those assessments, an accountability-based framework should greatly reduce any harms deemed "unintentional." That said, government policy should offer organizations guidance to help distinguish harmful from harmless outcome disparities and to help clarify what empirical evidence is required by whom to make or defend against allegations of discrimination.

Theme 2. Impact of Data Collection and Processing on Marginalized Groups

3b. Are there particular technologies or classes of technologies that warrant particularly rigorous scrutiny for their potential to invade privacy and/or enable discrimination?

While a proper risk assessment should be able to identify whether a particular technology or use would warrant heightened scrutiny in a particular context, it would be helpful for government policy to provide guidance on types of uses that may be considered particularly harmful (or presumptively harmful), which can be rebutted in particular contexts through contextual risk assessments.

3c. When should particular types of data be considered proxies for constitutionally-protected traits? For example, location data is frequently collected and used, but where someone lives can also closely align with race and ethnicity. In what circumstances should use of location data be considered intertwined with protected characteristics? Are there other types of data that present similar risks?

Again, an accountability-based framework does not focus on particular **types** of data—e.g., whether it is "sensitive," "non-sensitive," or even a "proxy for constitutionally-protected traits"—but rather focuses on the impact of the **use** of the data in a specific context. As noted in our response to Q1c, even uses of so-called "non-sensitive" data could have "sensitive" effects. By focusing on the **use**—and whether that use creates adverse, unjustifiable, or unfair effects on individuals—potential harms can be identified and mitigated. The risk assessment addresses whether **the data can be used responsibly and with appropriately tailored protections in a specific context and for a specific purpose.** A proper risk assessment would screen for harms associated with proxies as much as it would for so-called sensitive data.

3d. Does the internet offer new economic or social sectors that may raise novel discrimination concerns not directly analogous to brick-and-mortar commerce? For example, how should policymakers, users, companies, and other stakeholders think about civil rights, privacy, and equity in the context of online dating apps, streaming services, and online gaming communities?

A proper risk assessment would identify any novel concerns associated with new products, services, technologies, and business models, and it would help craft the necessary safeguards to protect against any novel harms.

Theme 3. Existing Privacy and Civil Rights Laws

4f. 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?

CIPL supports laws that implement an accountability-based framework that requires organizations to conduct a contextual risk assessment addressing whether data can be used responsibly and with appropriately tailored protections in a specific context and for a specific purpose. See also CIPL's papers on "Ten Principles for a Revised US Privacy Framework"[16] and "Learning from the GDPR: What Elements Should the US Adopt?"[17]

4g. 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?

See our response to Question 4f.

Theme 4. 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?

5b. What kinds of protections might be appropriate to protect children and teens from data abuses? How might such protections appropriately address the differing developmental and informational needs of younger and older children? Are there any existing proposals that merit particular attention?

As a follow-up to the publication of our recent policy paper "Protecting Children's Data Privacy, International Issues and Compliance Challenges,"[18] CIPL is currently exploring best practices and emerging options to address the issues and challenges raised in the paper. Applying a risk based-approach will feature prominently in this context. CIPL will provide a copy of its findings once published.

5c. What kinds of protections might be appropriate to protect older adults from exploitative uses of their data?

A contextual risk assessment would help identify not only potential harms to members of a particular group (such as the elderly), but also the appropriate mitigation measures for a given context and a given use.

In addition, organizations are increasingly looking to **Privacy Enhancing Technologies (PETs)** and **Privacy Preserving Technologies (PPTs)** to protect consumer data. PETs and PPTs can play an extremely important role in mitigating privacy risks while enabling beneficial data uses. Of course, PETs/PPTs are not a silver bullet and will always have to be considered in combination

[16] *Ten Principles for a Revised US Privacy Framework*, CIPL White Paper (March 21, 2019), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_principles_for_a_revised_us_privacy_framework__21_march_2019_.pdf.

[17] *Learning from the GDPR: What Elements Should the US Adopt?*, CIPL White Paper (January 25, 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_paper_-_learning_from_the_eu_gdpr_-_what_elements_should_the_us_ado....pdf.

[18] *Protecting Children's Data Privacy Policy Paper I: International Issues and Compliance Challenges*, CIPL White Paper (October 20, 2022), available at https://www.informationpolicycentre.com/policy-paper-i-international-issues--compliance-challenges.html.

with other mitigation measures. Moreover, proper regulatory incentives to develop and deploy PETs, could greatly increase their use in appropriate contexts. As with other technologies and uses of data, organizations should be held accountable for their use of PETs/PPTs. Thus, companies must deploy technical and organizational measures to ensure and demonstrate the appropriateness of these methodologies. CIPL's forthcoming report on PETs and PPTs will explore this topic in greater detail.[19]

5d. 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?

As noted in CIPL's recent response to the Federal Trade Commission's Advance Notice of Proposed Rulemaking on Commercial Surveillance and Data Security,[20] CIPL believes that the principles of purpose specification and use limitation must be balanced with the need to allow organizations the flexibility to react to new inferences from old or different data sets and to generally use data for new and beneficial purposes that do not increase the risk of harm to individuals. One way of doing this is by enabling further processing where the new use is "compatible" or "not-incompatible" with the original purpose,[21] which would include all uses that are consistent with, can co-exist with, and do not undermine, conflict with, or negate the original purpose, and where any new risk of harm can be appropriately addressed through targeted mitigations and controls based on risk assessments.

CIPL notes that access to large amounts of data potentially collected for a different purpose is critical to building analytics models, AI systems, and machine learning algorithms. AI systems in particular need diverse data sets, including data commonly regarded as sensitive, to understand and subsequently limit biased and discriminatory outputs. Notwithstanding the data minimization and purpose limitation principles, it can be difficult to know ahead of time what is "necessary" in the AI context, since the processing of more and more data may lead to new discoveries and correlations, may maximize the accuracy of results, and may improve bias detection and prevention. Furthermore, AI technology has the capability of finding new and beneficial uses for old data (e.g., in the financial industry, old data can reveal patterns and identify trends that were unknown at the time of collection, which can be helpful for fraud prevention).

Finally, data minimization, contrary to some views, does not mean data deletion. Rather, it means that data should be adequate and appropriate for the specified purpose. In other words, as long as there is a specified purpose for the processing, data can be retained for that specific purpose; data minimization does not come into play.

[19] Upon its anticipated publication in later in 2023, CIPL will share this report with the NTIA.

[20] *Supra*, note 4, response to Q46.

[21] See, for example, the GDPR Art. 5(1)(b), which permits the processing of data for purposes other than those for which the personal data was initially collected where the processing is compatible with the purposes for which the personal data was initially collected. See also GDPR Recital 50.

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

6c. 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 noted in CIPL's recent response to the FTC's Advance Notice of Proposed Rulemaking,[22] organizational accountability frameworks require organizations to implement comprehensive privacy management programs and to be able to demonstrate the existence and effectiveness of these programs and all their component parts on request, both internally (to their boards and senior management) and externally (to privacy enforcement authorities, business partners, and increasingly, shareholders and investors). This includes being able to demonstrate the risk assessments that the organization has conducted with respect to its data practices. Monitoring and auditing of privacy management programs are among the requirements of CIPL's Accountability Framework; companies must ensure that they adhere to their own data processing and protection policies, rules, and standards. Given the demonstrability requirement, we do not believe it is necessary to impose additional and routine self-reporting requirements or audits. However, we do believe that voluntary external audits may be a helpful tool for organizations to use in assessing and demonstrating the effectiveness of their privacy management programs.

6e. 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?

As noted in CIPL's recent response to the FTC's Advance Notice of Proposed Rulemaking,[23] given government's considerable demands in relation to its limited resources, co-regulatory schemes such as certifications or codes of conduct can provide some relief to regulatory and enforcement pressures.

Certification schemes and codes of conduct often involve the use of third-party certifiers, monitoring bodies, and dispute resolution providers. These entities can play important front-line enforcement and oversight roles and remediate many issues before the enforcement authority needs to step in. They review organizations' compliance and accountability programs and ensure that companies comply with the relevant standard to which each was certified. When necessary, they can suspend certifications and take other remedial actions against non-compliant organizations. Dispute resolution functions can relieve the enforcement authority from the burden of dealing with large numbers of "easy" cases, allowing it to focus on more important and strategic matters.

The benefits of such schemes to regulators and enforcement authorities are numerous:

[22] *Supra*, note 4, response to Q92.

[23] *Supra*, note 4, response to Q51.

- **Reduce oversight workload**: Where certification bodies take on and share the burdens of supervision and oversight with the enforcement authority, the authority's workload is reduced.
- **Improve compliance**: Certifications may result in improved outcomes and more effective on-the-ground compliance due to mandatory periodic re-certification processes and ongoing monitoring requirements, thereby reducing enforcement burdens of the authority.
- **Reduce complaint handling**: Because certifications may include complaint handling and dispute resolution mechanisms, they can address large numbers of individual complaints. To the extent the enforcement authority does not need to get involved, formal co-regulatory schemes make enforcement easier, freeing the authority to investigate compliance against specific sets of detailed requirements established by certifications and codes of conduct.
- **Transparency**: Certification requires organizations to disclose their data practices in a transparent and organized fashion vis-à-vis the certification bodies and ultimately the enforcement authority in the event of enforcement. This makes it easier for the authority to properly assess these practices as well as possible violations of the relevant requirements. This, in turn, may drive down the costs and burdens of enforcement actions, both for the enforcement authority and organizations.

Co-regulatory schemes can also help companies—particularly small and medium-sized enterprises (SMEs)—to meet relevant legal and accountability requirements by relying on existing standards, without having to devise a custom-made program themselves. They enable organizations to readily demonstrate accountability and their program to enforcement authorities, business partners, clients, and individuals, creating administrative efficiency and building trust.

However, to encourage uptake of certifications by industry, it is crucial for the certification process to be efficient and scalable. Moreover, it is essential that certifications are effectively incentivized, i.e., clearly accompanied by benefits for certified organizations, such as considering certification as a safe harbor or mitigating factor in enforcement. (The EU GDPR recognizes adherence to codes of conduct or certifications or other forms of demonstrated accountability as a mitigating factor in enforcement. GDPR Article 83(2).) Otherwise, organizations will be reluctant to invest time and money in obtaining and maintaining certifications on top of the many other requirements to which they are already subject.

In short, such co-regulatory schemes benefit all stakeholders because they augment the capabilities and reach of the enforcement authority and raise the level of overall privacy protections and compliance.[24]

[24] See CIPL White Paper: *Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanism*, April 12, 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_certifications_discussion_paper_12_april_2017.pdf; filed herewith as Exhibit 16.

III. Conclusion

Because combating racial discrimination and fostering equity are core responsible data practices, CIPL believes that an organizational accountability framework—with a particular focus on contextual risk assessments—can address many of the concerns raised by the NTIA. As highlighted in our recent article "To Combat Data-Intensive Racial Injustice, Prioritize Adoption of Accountability Frameworks,"[25] it is essential for accountability frameworks to incorporate explicitly into their risk assessments screening for fairness and for unjust racial discrimination. CIPL is committed to advancing the quest for solutions to data-intensive racial injustice by participating constructively in ongoing policy debates, sharing our expertise on solutions such as risk-based accountability frameworks, and lifting up diverse perspectives on this challenging but critically important topic.

[25] *To Combat Data-Intensive Racial Injustice, Prioritize Adoption of Accountability Frameworks*, CIPL (February 15, 2023), available at https://www.linkedin.com/pulse/combat-data-intensive-racial-injustice-/.