Centre for Information Policy Leadership
Hunton Andrews Kurth

October 31, 2018

**Response of the Centre for Information Policy Leadership (CIPL)
to the Request for Comment by the National Telecommunications and Information Administration (NTIA) on "Developing the Administration's Approach to Consumer Privacy"**

Docket No. 180821780-8780-01

31 October 2018

Introduction

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to respond to the Request for Comment (RFC) by the National Telecommunications and Information Administration (NTIA) on "Developing the Administration's Approach to Consumer Privacy", published in the Federal Register on September 26, 2018. CIPL commends NTIA for initiating a renewed national debate on updating the US privacy framework in a way that advances both consumer privacy and the ability to innovate and that responds effectively to recent global and domestic privacy law developments. CIPL also welcomes NTIA's approach of beginning this process by focusing on the intended core outcomes and high-level goals of any new US privacy framework. Our comments below address the issues and questions raised in the RFC in the order in which they are presented by NTIA. In various places we refer to a number of recent CIPL white papers that address some of the issues raised in this response in greater detail.

Comments

I. Background (p. 2)

CIPL fully agrees with NTIA's description of the key issues in this section, particularly that any new privacy framework must (1) engender consumer trust in the effective protection of consumer privacy interests and concerns; (2) reduce national regulatory fragmentation; (3) increase national and global interoperability; (4) enable innovation; (5) be risk based (i.e., focus on harm) and be flexible; and (6) be scalable to organizations of all sizes. In addition, we believe it should be future-proof and technology neutral.

We understand that the RFC does not call for the creation of a statutory standard at this stage. However, we would like to register our view that, as further discussed below, the US would be

[1] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 66 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 reflecting the views of any particular CIPL member company or of the law firm of Hunton Andrews Kurth LLP.

best served by a comprehensive baseline privacy law that implements or enables the features mentioned above, applies to all organizations, preempts inconsistent state laws, amends or replaces inconsistent federal privacy laws where appropriate, and otherwise works with or around well-functioning existing sectoral laws, some of which are referenced in the Background section of the RFC. Such baseline privacy legislation could then be complemented by rulemakings, codes of conduct, certifications and other co-regulatory accountability mechanisms that can provide any necessary details that are intentionally not specified in the baseline law. Indeed, NTIA's approach to start with the intended outcomes and goals of any privacy regime is appropriate and well suited to lay the foundation for a well-thought-out legislative proposal in the future. As further discussed below, as a next step, we recommend preparing draft legislative language capturing the proposed outcomes and goals with greater specificity to facilitate a more granular discussion about what a new US privacy law should look like.

II. Privacy Outcomes (p. 5)

CIPL strongly agrees with NTIA's assessment that, to date, the principles-based approach to privacy has resulted in problems by conflating or confusing desired outcomes with the means of achieving these outcomes. As an example, NTIA points to informed consent as a traditionally desired outcome and to notice and choice as the means for achieving this outcome, which has not worked. NTIA correctly cites to the example of long and legalistic privacy policies (notice and choice) that only few people read, understand or can effectively act upon, and which, therefore, do not enable informed consent.

Apart from the fact that informed consent should be a desired outcome only in limited contexts where consent is actually still necessary, desirable and practicable (see discussion below), CIPL agrees with NTIA's general critique of this approach and with NTIA's proposal to replace this approach with one that focuses on the outcomes of organizational practices rather than on the means by which these outcomes are to be accomplished. Thus, according to the RFC, examples of desired outcomes include the following:

- a reasonably informed user, empowered to meaningfully express privacy preferences (and we would add: "where expression of preferences is appropriate") (see further discussion below);
- products and services that are inherently designed with appropriate privacy protections particularly in contexts where user intervention may be insufficient to manage privacy risks;
- the collection, use, storage and sharing of personal data that is reasonable and appropriate to the context; and
- user transparency, control and access that is reasonable and appropriate.

These outcomes would then be operationalized through a risk management approach and accountability measures, which give organizations both flexibility and the ability to innovate in how to achieve these outcomes. CIPL strongly agrees with this approach as we have been advocating for a risk-based approach to privacy protection, regulation and oversight for a long time.[2] This would also bring privacy protection more clearly in line with the prevailing approach to information security and cybersecurity, which is mostly risk based. However, it is important to note that this approach does not obviate the need for high-level and principle-based parameters in any new law and through other formal guidelines from regulators or co-regulatory mechanisms that provide businesses with sufficient legal certainty (see discussion below). It is also important to ensure that any obligation to meet these outcomes must be consistent with the ability of organizations to (1) prevent or detect fraud; (2) protect the security of people, devices, networks or facilities; (3) protect the health, safety, rights or property of the covered entity or other persons; (4) respond in good faith to valid legal process or provide information as otherwise required or authorized by law; or (5) monitor or enforce agreements between the covered entity and an individual, including terms of service, terms of use, user agreements or agreements concerning monitoring criminal activity.

This risk management approach envisioned by the RFC essentially enables organizations to calibrate privacy compliance measures and requirements based on the likelihood and severity of risks to individuals. It would require organizations to conduct risk assessments with respect to their data processing operations. (However, in cases of commonly agreed "low-risk" uses (e.g., handling business contact information), such assessments should not be required). The risk assessments would identify the relevant risks to individuals and the benefits of processing and enable context-appropriate controls and mitigations to eliminate or reduce any identified risks to a reasonable level, taking into account the intended purpose and benefits of the processing. Organizations would also have to be able to demonstrate and explain their risk assessment and decision-making processes to privacy enforcement authorities in the event of a legal challenge. As suggested by NTIA, a more prescriptive approach that specifies the necessary controls and mitigations or otherwise prescribes specific requirements about when and how to process certain personal data would result in compliance checklists that may undermine the very essence of organizational accountability and innovation in privacy solutions and would waste resources without necessarily advancing consumer privacy.

---

[2] See "A Risk-based Approach to Privacy: Improving Effectiveness in Practice," 19 June 2014, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_1-a_risk_based_approach_to_privacy_improving_effectiveness_in_practice.pdf; "The Role of Risk Management in Data Protection," 23 November 2014, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_2-the_role_of_risk_management_in_data_protection-c.pdf; "Protecting Privacy in a World of Big Data, The Role of Risk Management," 16 February 2016, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/protecting_privacy_in_a_world_of_big_data_paper_2_the_role_of_risk_management_16_february_2016.pdf; and "Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR," 21 December 2016, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf.

NTIA rightfully raises the need for legal clarity in the context of such a more flexible risk management approach, suggesting that clarity can be achieved within the context of this approach. As stated, to have legal clarity, organizations must be given some parameters as well as be able to rely on privacy enforcement authorities accepting the outcomes of reasonably conducted risk assessments and decisions around appropriate mitigations and controls. If privacy enforcement authorities can readily invalidate the risk assessments and other privacy protection measures with which organizations are implementing the desired "outcomes" of a privacy framework, organizations will not have the requisite legal certainty, thus potentially stifling their willingness to innovate or to generally engage in beneficial business operations.

There are several ways to ensure a sufficient degree of legal certainty in this context:

a) There should be a common understanding of the types of risks and potential harms that organizations must consider in a risk assessment (e.g., financial and economic harms, physical harms and nonmaterial harms such as reputational harms, etc.).

b) It is important that there be a common understanding and approach as to how to evaluate these risks and harms and how to determine whether the mitigations, controls and other implementation measures that come out of the risk assessment process are appropriate.

c) Relevant risks and harms as well as other key parameters of this approach could be set forth at a high level in a comprehensive privacy law. This would still leave the option for additional regulatory guidance where appropriate and sufficient flexibility and discretion for industry to implement context-appropriate risk assessments and mitigations.

d) Another way to align the risk management practices of organizations with the approaches of regulators when evaluating them is for the practices to be framed within universally recognized "organizational accountability" frameworks. These include (i) comprehensive internal privacy programs that implement the key elements of accountability (see discussion below) or (ii) formally recognized and scalable accountability frameworks, such as codes of conduct or privacy certifications, or similar schemes implementing a global standard, such as the APEC Cross-Border Privacy Rules (CBPR) or the ISO Cloud Privacy and Security Standard, as CIPL has previously discussed in detail.[3]

[3] See CIPL papers on "The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society," 23 July 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf; and "Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability," 23 July 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-

e) Finally, enterprise risk management tools and risk assessment methodologies developed in multistakeholder processes, such as by the National Institute of Standards and Technology (NIST), can significantly contribute to legal certainty through the use of commonly accepted approaches.

The RFC seeks comment on seven suggested outcomes: Transparency, Control, Reasonable Minimization, Security, Access and Correction, Risk Management, and Accountability. In the section below, we address each in turn. In addition, we suggest an additional outcome of Complaint-handling and Redress.

Since the RFC specifically asked for comments on clarity, we note that the distinction between the labels "outcomes" and "goals" is not intuitive. (The "goals" section comes after the "outcomes" section in the RFC.) It would be helpful to clarify the distinction at the next opportunity. It appears that the "outcomes" respond to the question of "What direct benefits, impacts or industry behaviors can consumers expect from the envisioned privacy framework?" They can expect transparency around how their data is processed; reasonable control over their data; no unnecessary over-collection of their data; that their data will be secured; that they get reasonable access and opportunities to correct their data; that the risks of harm associated with processing their data will be effectively managed, reduced or eliminated; and that the organization will be accountable. In contrast, the "goals" describe the nonconsumer-facing features of the privacy framework that have a direct impact primarily on regulated organizations or enforcement authorities, such as harmonization, legal clarity, comprehensive application, taking a risk-based and outcome-based approach, interoperability, incentivizing research, FTC enforcement and scalability, i.e., the overall ambition of the privacy framework in respect of its domestic and global policies and commitments.

Specific Outcomes (p. 9)

1. Transparency

CIPL agrees that transparency should be a key outcome of any privacy framework. Much of effective privacy regulation depends on all stakeholders being able to understand the uses of personal data. It also is a prerequisite for consumers to be able to make choices regarding the use of their personal data where such choice is appropriate (see discussion below). Transparency is also part of organizational accountability—there cannot be accountability without transparency. Further, appropriate transparency at the correct level of detail is key to creating and maintaining consumer trust in the digital economy, as well as the necessary trust with regulators. This also implies that transparency cannot and should not be absolute but must vary depending on context and audience.

_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf.

CIPL has done extensive work on reframing the concepts of notice and privacy policies to develop more user-centric and actionable data transparency that, for example, enables effective and genuinely informed consent in contexts where consent remains appropriate. Our 2016 paper on "Reframing data transparency"[4] describes in detail specific and necessary action items for organizations, data privacy regulators and policymakers to collaborate on in developing this new user-centric approach to transparency.

Fundamentally, we believe that transparency must be contextual and tailored toward the specific audience and purpose. For example, a privacy framework or law should enable organizations to frame their privacy-related disclosures in terms of questions such as: Is the disclosure meant to enable a general awareness and basic understanding by consumers about the data uses at issue to enable their trust that the information will be handled accountably and in a way that will not harm them? Is it meant to enable a specific informed choice or consent in a context where such choice and consent would be appropriate? Is it meant for so-called "opt-in" consent, or is it to enable consumers to knowingly indicate their approval of certain data uses without having to take affirmative action to provide consent (i.e., is it designed to enable "opt-out" consent)? Is the disclosure meant for consumers or for a more expert audience, such as data protection regulators? Is it intended to be a comprehensive legal disclosure?

These questions are particularly important in the context of AI, machine learning and algorithmic transparency, which is a topic CIPL addresses in one of its recent white papers on "AI and Data Protection: Delivering Sustainable AI Accountability in Practice."[5] To ensure that organizations implement a user-centric transparency mandate effectively, they must be able to demonstrate to privacy enforcement authorities repeatable and credible processes for devising different transparency tools and disclosures. Implementing companywide data protection privacy management and accountability frameworks (as discussed in CIPL's recent white papers on the role of accountability mentioned above and further discussed below) will ensure that companies will be able to do so.

Finally, as noted above, transparency includes transparency not only to consumers but also to privacy enforcement authorities, both proactively, as part of ongoing constructive engagement between regulated entities and regulators, and reactively, in case of an actionable complaint, investigation and enforcement procedure. We also believe that various limitations of transparency that are inherent in modern technology (e.g., AI) may be compensated by enhanced transparency to regulators or other bodies that may act as proxies (such as oversight or review boards or third-party certifiers).

---

[4] See CIPL and Telefónica paper on "Reframing Data Transparency," October 2016, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/reframing_data_transparency.pdf.

[5] See CIPL white paper on "Delivering Sustainable AI Accountability in Practice: Artificial Intelligence and Data Protection in Tension," 10 October 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_ai_first_report_-_artificial_intelligence_and_data_protection_in_te....pdf.

2. Control

NTIA posits "reasonable control over the collection, use, storage, and disclosure of personal information" as a desired outcome of a privacy framework. Assuming the emphasis is on "reasonable" and that "appropriate" is added as a qualification (i.e., "reasonable and appropriate control"), CIPL agrees with NTIA that the decision of *which* controls to offer, and *when* and *how* to enable such controls, must be contextual. Additionally, while it is both implied in, and consistent with, NTIA's characterization of this outcome, it should be made explicit that the question of *whether* to make such control available is also a relevant contextual consideration. Clearly, there are contexts where it is infeasible to offer consumer control, choice or consent with respect to certain data processing, or where additional control, choice or consent may not be appropriate because a particular use of data is already expected given the context. CIPL has discussed this issue extensively in various white papers, public consultations and articles.[6]

For example, in the modern digital economy of big data, AI, machine learning and the IoT, in which data processing is ubiquitous, increasingly complex and with many legitimate processing activities several layers removed from the user or the original purpose for which the information was collected, there are many scenarios where it is not possible to provide actionable choice to consumers.

Additionally, there are many cases where such notice and choice are not necessary or desirable, even if they were possible. For example, reasonable secondary use of publicly available information should not be subject to unfettered consumer control. Firms routinely compile information used by companies and governments to meet obligations with respect to "know your customer" (KYC), anti-money laundering, anti-terrorism, export control laws and sanctions lists, etc. Such reasonable and beneficial uses of publicly available information should be preserved. Further, in the context of using data for medical research or other analytics purposes, it would be preferable to protect such information through other means (such as anonymization and data security measures) rather than enabling the unnecessary and potentially arbitrary removal of valuable data from legitimate research through consent mechanisms. Of course, this does not preclude the need for transparency to individuals explaining that such research may occur and now it is protected.

---

[6] See CIPL white paper on "The Role of Enhanced Accountability in Creating a Sustainable Data-driven Economy and Information Society," 21 October 2015, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/protecting_privacy_in_a_world_of_big_data_paper_1_the_role_of_enhanced_accountability_21_october_2015.pdf; CIPL white paper on "Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR," 19 May 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf; and "Empowering Individuals Beyond Consent," Bojana Bellamy and Markus Heyder, IAPP Perspectives, 2 July 2015, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/empowering_individuals_beyond_consent.pdf.

As outlined in CIPL's earlier work on organizational accountability[7] as well as on consent and its alternatives, there are a range of mechanisms better suited than consent for protecting consumers from harm in the modern digital economy. These mechanisms include implementing the full range of elements of organizational accountability—effective leadership and oversight; risk assessment; internal policies and procedures (that include fair processing and ethics); transparency; training and awareness; monitoring and verification; and internal complaint handling, response and enforcement.[8] Consumers may neither be able to, nor be interested in, taking on the difficult job of having primary responsibility for protecting themselves in this complex data economy, a fact amply illustrated by the problem of consent fatigue. Thus, a well-considered and comprehensive privacy framework will include a range of safeguards and back-up measures to ensure individuals are meaningfully protected even where they did not exercise "control" through consent. As noted, these include the transparency requirement, the ability to demand access to data, to correct or delete inaccurate or obsolete data and the ability to complain to organizations or privacy enforcement agency.

On the other hand, there are contexts where consumers do expect and deserve control and clear choices, such as (i) with respect to how they want their personal data and postings to be visible and shared on social media; (ii) sharing medical data with third parties for marketing purposes; or (iii) in connection with sharing personal data that is considered more sensitive and private, such as health, religion, race, sexual orientation data or other high-risk contexts, when such information cannot otherwise be appropriately protected through other accountability measures.

Thus, where other protections are not possible or sufficient, CIPL agrees with the RFC that mechanisms enabling control should be developed keeping in mind intuitiveness of use, affordability and accessibility. Moreover, it should also be made clear that for the sake of general efficiency and minimizing consent fatigue that opt-out or implicit consent mechanisms remain valid where it is clear from the context that inaction by consumers indicates agreement with the proposed data use.

In short, "control" should be a component of a new privacy framework to a limited extent in contexts where it is appropriate, and should also include reference to mechanisms that empower consumers, other than individual choice or consent. However, the general focus of the framework should be putting the onus on organizations to use data responsibly and accountably and to protect consumers from harm regardless of their individual level of engagement. This approach will be essential in the vast majority of information use contexts where individuals cannot realistically be expected to engage and to exercise control over the use of their data.

[7] *Supra* note 3.
[8] *Id*. at page 5.

3. Reasonable Minimization

CIPL agrees with NTIA's inclusion of "reasonable minimization" as an outcome of a new data protection framework. Significantly, NTIA correctly notes that such minimization should be "reasonable" and "appropriate to the context and risk of privacy harm." These qualifiers are very important given the enormous potential of personal data for driving economic growth and societal benefits in the digital economy.

In particular, the quality, accuracy, effectiveness and ultimately the fairness of AI and machine learning applications frequently depend on the analysis of large amounts of personal data.[9] In fact, minimizing data use in the context of machine learning can increase the risk of unintended discrimination. Thus, in the context of implementing a "reasonable minimization" outcome, organizations must be allowed to define the purposes of the proposed data uses broadly, potentially encompassing as yet unknown or unexpected purposes of data analytics. This will be necessary to enable the collection and retention of the amount and types of personal information necessary for developing AI and machine learning applications to their fullest potential, both in their training and implementation phases.

As in the context of notice, choice and consent, the appropriate safeguards here include, in addition to the ones mentioned by NTIA (additional security safeguards or privacy-enhancing techniques), the full range of requirements encompassed by organizational accountability, as set forth above on page 8.[10] Thus, to ensure credible compliance with the "reasonable minimization" outcome, organizations must implement these elements of accountability with respect to the volume and nature of personal information they collect and retain and must be able to demonstrate and justify their decisions and implementation measures in that regard to regulators.

4. Security

CIPL fully agrees with NTIA's inclusion of "security" in the list of outcomes. In addition to the characterization provided in the RFC, CIPL notes that it is important to allow organizations flexibility in determining the security measures that are reasonable and appropriate to the context at hand. These measures are fluid, as they change over time and are often based on evolving external security standards, rather than being prescribed by law or any regulator in advance. Moreover, adopting appropriate measures in response to data security breaches, such as breach notification requirements, should be included in a security outcome in any new privacy framework (although such a requirement may also be encompassed within the Risk Management outcome below). Finally, the security outcome must allow organizations to use personal data for the development and implementation of data security tools and related legitimate purposes, such as incident prevention, detection and monitoring measures,

[9] *Supra* note 5.
[10] *Supra* note 8.

reasonable and proportionate monitoring of communications and activities of employees, users of services and other relevant individuals, and monitoring of devices operated and owned by individuals.

5. Access and Correction

CIPL agrees with how NTIA has characterized the outcome of "access and correction" (and "deletion"). It should be reasonable, context-specific and appropriate to the risk of privacy harm. The ability of individuals to access, correct and delete personal data in certain circumstances is an important part of the balance of the privacy framework and enables individuals to exercise control over their data regardless of whether they consented to any processing at the outset.

However, access, correction and deletion rights cannot be absolute. Individuals should not be allowed to access, correct or delete data if doing so would: (1) undermine privacy or data security interests; (2) enable fraud or other unlawful activity; (3) interfere with law enforcement or judicial proceedings; (4) be unduly burdensome or excessive in light of the purpose of the processing; or (5) require the collection or processing of additional personal information about the individual. For example, it is critical for functions such as Know-Your-Customer, anti-money laundering, anti-terrorism, credit scoring, and export control requirements and sanctions lists that individuals are not permitted to game the system by suppressing relevant information or by opting out, or having their personal data deleted from databases that provide an important public service. Thus, the access and correction outcome should not interfere with relevant obligations of the organization, other societal goals or legal rights of consumers and other third parties.

Whether, when and how to correct or delete data is a particularly sensitive issue in the context of AI and blockchain. As discussed above, AI and machine learning, including training the algorithms for these purposes, generally rely on complete and accurate data sets and any infringement upon the completeness or accuracy can undermine the analysis and decisions made by these algorithms.[11] In the context of blockchain technology, correcting or deleting personal data may also be inherently impossible and in conflict with how the technology works. Also, there can be legal reasons, including First Amendment concerns, as well as administrative reasons, not to allow correction. These issues should be further clarified and addressed in any future articulation of this outcome. Of course, given the general reliance of AI and machine learning on as much accurate data as possible, the outcome of "access and correction" will likely be significantly driven by that fact alone. In other words, there may be strong inherent incentives to allow for access and correction.

In sum, access, correction and deletion is an important outcome. It is also already widely practiced as it generally aligns with the interest of organizations to engender trust as well as

[11] *Supra* note 5.

have correct information. Where access, correction or deletion would be inappropriate or impose unreasonable burdens and expenses on the organization that are disproportionate to the risks to the individual's privacy, part of the solution lies in providing assurances to consumers that their personal information is reasonably protected by way of the full range of available accountability measures and will not be used for harmful purposes, as discussed in CIPL's white papers on accountability.[12]

6. Risk Management

CIPL welcomes NTIA's characterization of risk management as the "core" of its approach to privacy protection. According to the RFC, risk management "provides the flexibility to encourage innovation in business models and privacy tools, while focusing on potential consumer harm and maximizing privacy outcomes." Indeed, as discussed above, this outcome addresses the expectation of consumers that the risks of harm associated with processing their data will be effectively managed, reduced or eliminated. Thus, it signifies a harms-based approach to data protection and privacy, which is also exemplified by the APEC Privacy Framework, which includes as its first privacy principle that of "preventing harm." CIPL strongly supports this focus on harms as a key component of any modern and scalable data privacy framework.

Also, as discussed above, CIPL has consistently advocated for an approach to privacy compliance that is based on contextual risk/benefit assessments, coupled with all the other elements of organizational accountability, which we already listed above.[13] This focus on identifying harms and addressing them specifically has the advantage of enabling organizations to prioritize their compliance measures and focus resources on what is most important, thereby strengthening both consumer privacy and organizations' ability to engage in legitimate and accountable uses of personal information. When applied across the board to all information processing operations (with some low-risk exceptions where it may be agreed not to be necessary), it also means that we do not need to establish set categories of so-called sensitive information or certain predetermined high-risk processing activities, as any actual sensitivity or high-risk character will be determined and addressed in each risk assessment process. The result of this approach would be more accurate identification of sensitivity and levels of risk in a given context and more appropriate and targeted mitigations and controls, including consent, to address such risks.

Importantly, policymakers, lawmakers and regulators could still provide guidelines on the types of personal information or processing operations that are potentially sensitive or high risk (such as medical data). Such guidance will be important to businesses. However, those guidelines

[12] *Supra* note 3.
[13] *Supra* note 8.

should be rebuttable presumptions that can be negated by an actual risk assessment that takes the context of the proposed uses into account.[14]

Also, to avoid unnecessary risk assessments, regulators could identify categories of information uses that are generally accepted to be "low-risk" activities (such as handling business contact information) and that would not require risk assessments under normal circumstances. This is particularly important for purposes of making the risk-based approach scalable for SMEs and for generally increasing legal certainty where it is possible to do so. Of course, even here, organizations must always consider whether such low-risk classification is accurate in their particular context.

In that connection, the RFC mentions the work of the National Institute of Standards and Technology (NIST) in developing a voluntary risk-based risk management tool. Risk management tools that operationalize the risk-based approach and risk management for organizations will be a crucial component of any future privacy framework with risk management at its core. Tools and risk assessment methodologies such as this, particularly when they are the result of multistakeholder processes that have the buy-in from relevant privacy enforcement authorities, will help ensure the necessary alignment between organizations and enforcers that the results of properly conducted risk assessments will be upheld. This aspect of the risk-based approach to privacy is essential for creating the necessary legal certainty for organizations to innovate and engage in new and beneficial economic activity.

7. Accountability

CIPL strongly agrees with including "accountability" in the essential outcomes of a privacy framework. In fact, in our recent white papers on the role of organizational accountability and the need for privacy enforcement authorities and policymakers to specifically incentivize accountability, we argued that accountability is a key building block of modern data protection.[15] Accountability is also essential for the future of the digital society where laws alone cannot deliver timely, flexible and innovative solutions. It is the combination of a baseline privacy framework and co-regulatory accountability frameworks that is best suited for the fast pace of the digital society.

As discussed in detail in these papers, the concept of organizational accountability provides the framework for organizations to implement comprehensive internal privacy programs that are designed to ensure that organizations have the processes and systems in place, including for risk assessment, to enable maximum compliance with relevant requirements as well as the ability to demonstrate it on request.

[14] *Supra* note 2 ("Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR") at pages 8, 30 and 31.
[15] *Supra* note 3.

In its paragraph on accountability, NTIA refers to its subsequent discussion in the section on "High-Level Goals for Federal Action" relating to incentivizing risk and outcome-based approaches within organizations "that enable flexibility, encourage privacy-by-design, and focus on privacy outcomes." In CIPL's recent white paper on "Incentivizing Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability,"[16] CIPL argued that given its many benefits to all stakeholders, organizational accountability should be specifically incentivized through a range of measures that regulators and policymakers could provide. We discuss this issue in the relevant section below.

In short, we strongly encourage including accountability as an essential outcome. We would further recommend that NTIA clarify and elaborate upon this important concept in line with its globally accepted meaning, including in the APEC Privacy Framework, the EU General Data Protection Regulation, as well as other relevant international privacy regimes that incorporate this concept. To that end, we refer you to the above-referenced recent CIPL white papers on this topic.

Suggestions for additional outcomes:

8. Complaint-handling and Redress

In addition to the above outcomes, CIPL recommends the additional outcome of complaint-handling and redress. Consumers should be able to expect that organizations are able to reliably, quickly and effectively respond to actionable complaints and provide redress where appropriate in light of the nature of the services at issue, the nature of the complaints and other relevant variables. This is a key element of organizational accountability. Because it is consumer-facing, it should be a separately stated outcome that consumers can expect from a privacy framework.

A new privacy framework should require organizations to have internal processes and structures in place that accomplish this outcome. To the extent organizations participate in formal accountability schemes like codes of conduct, certifications or APEC CBPR, this outcome will likely be required within the context of these mechanisms, often in conjunction with or through third-party dispute resolution and/or "enforcement" of these mechanisms by third-party certifiers or Accountability Agents. Of course, this outcome is in addition to and not in lieu of complaining to and enforcement by appropriate government authorities.

III. <u>High-Level Goals for Federal Action (p. 9)</u>

As discussed above, the "goals" set forth in the RFC describe the non-consumer-facing features of the privacy framework that have a direct impact primarily on regulated organizations or

[16] *Id*.

enforcement authorities. They include: harmonizing the legal landscape; having legal clarity while maintaining the flexibility to innovate; ensuring comprehensive application; employing a risk- and outcome-based approach; maintaining interoperability; incentivizing privacy research; FTC enforcement; and scalability.

CIPL agrees with each of these goals and believes they can be accomplished. CIPL also recommends adding an additional goal of enabling "effective use of personal information."

1. Harmonizing the legal landscape

We support the effort on the federal level to harmonize the US privacy framework, including through federal privacy legislation that preempts inconsistent privacy laws at the states level, amends or replaces inconsistent federal privacy laws where appropriate, and works with or around well-functioning existing federal sectoral privacy laws.

The RFC refers to "consumer privacy" and "users." It is not entirely clear whether the proposed framework intends to cover employees. NTIA should clarify that; given the complexity of US employment laws and the burden that a privacy law affording access and correction rights would put on small and medium-size businesses, the new framework should be focused on data privacy in the consumer and commercial context, recognizing that many existing federal sectoral laws cover other situations. We note that the RFC does not define the term "consumer," so this may already be intended. When limiting the framework to consumers, it would be useful to provide clarification of what the term encompasses, to avoid legal uncertainty and gaps in coverage.

2. Having legal clarity while maintaining the flexibility to innovate

Legal clarity and flexibility are frequently seen as in conflict. However, as described above and in our cited materials, a privacy framework based on organizational accountability and the risk-based approach can provide both legal clarity and the flexibility for organizations to innovate and implement appropriate privacy protections based on their specific business models and operational structures. It is up to accountable organizations to operationalize privacy principles included in the privacy framework, as it best suits their organizational culture, processing context and risks. Organizations may also have to be prepared to sacrifice some degree of legal certainty in return for greater flexibility and technologically neutral, and thus more general, standards. It is a price worth paying for the sake of delivering the most effective privacy framework that can deliver the right outcomes for consumers and organizations.

NTIA is correct that compromise and creative thinking will be required. This is true particularly regarding the issue of how organizations can rely on privacy enforcement authorities to honor the outcomes of their risk assessments and implementation decisions where these were made within a "flexible" framework that does not prescribe clear rules for all contexts. As discussed above, CIPL believes that the processes inherent in organizational accountability and the risk-

based approach, coupled with the requirement that organizations must be able to demonstrate how these processes have been implemented, will address that issue effectively. Moreover, general agreement around the methodologies for privacy assessments, what potential risks to take into account and what potential risks may be "high risks," as well as clear guidance on what is "low risk" that under normal circumstances would not require a risk assessment, can also significantly contribute to legal clarity without undermining the flexibility to innovate. The NIST Privacy Framework and risk assessment methodology can significantly contribute to this objective.

Finally, over time and with the development and sharing of best practices, organizations of all sizes will be able to benefit from the accumulated collective know-how and experiences on how to implement a principles-based and risk-based privacy framework through their own organizational practices. Industry associations will also play an important role, as well as associations of privacy professionals, such as the IAPP, and industry standards bodies. Of course, ultimately, privacy enforcement agencies and courts will be able to provide additional legal clarity in specific cases.

3. Ensuring comprehensive application

CIPL agrees that a new US privacy framework should, at a minimum, cover all organizations or data use practices that are not covered by an existing adequate sectoral privacy law. To the extent different industries, business models and technologies require different approaches, the comprehensive framework should be high level enough to cover all of them (such as through a "risk and outcome-based approach," as the RFC correctly states).

Moreover, existing sectoral laws must be somehow brought into alignment with respect to each other and the new privacy framework in terms of levels of protection and other key features to enable smooth and seamless data flows and legal certainty when data keeps moving between sectors. This is necessary in an environment in which clear delineations among sectors is no longer the norm. Thus, as stated above, we support a comprehensive baseline privacy law that applies to all organizations, preempts inconsistent state laws, amends or replaces inconsistent federal privacy laws where appropriate, and otherwise works with or around well-functioning existing sectoral laws.

Further, in its next iteration, the proposed framework might add the clarification that this approach should allow for more granular guidance and/or regulation through enforceable codes of conduct and certifications where useful and appropriate. These mechanisms could address the specific needs of particular sectors, technologies, processes, products or services, or enable more detailed comprehensive organizational privacy programs that implement the full range of general requirements of any new privacy legislation.

With respect to potentially overlapping sectoral regulations, a new comprehensive privacy framework should clearly define the new responsibilities of the primary privacy enforcement authority (presumably the FTC) vis-à-vis the responsibilities of other regulators.

4. Employing a risk- and outcome-based approach

CIPL fully supports the goal of creating a risk- and outcome-based approach to privacy regulation for the reasons set forth in the RFC and as already discussed above. In addition to the features of this approach already discussed above, such an approach places the burden of protecting consumers directly where it belongs—on the businesses that use personal data, rather than on consumers, who, in an increasing number of contexts, should not and realistically cannot be tasked with understanding in detail and managing for themselves complex data uses or constantly making choices about them.

5. Creating interoperability

Maximizing the interoperability between different legal and privacy regimes should be a top priority goal for the United States. Most major businesses act globally and rely on the ability of data to flow across borders freely, and, indeed, many SMEs do as well. Any new privacy framework for the United States should therefore continue to enable the free, but responsible and accountable, flow of data across borders.

For transfers of data from the United States to other countries, the system should be based on the traditional US accountability-based approach. The entity that has collected and transferred the data is held accountable for the continued protection of the data at the level at which it is protected in the United States regardless of where it flows.

However, given that a growing number of countries are imposing cross-border transfer restrictions for data exports from their countries (albeit, coupled with cross-border transfer mechanisms that nevertheless enable such transfers in defined circumstances), any new US approach must be able to interoperate and work with these restrictions and transfer mechanisms. Hence, to enable free and responsible data flows into the United States, the US regime should enable its companies to demonstrate adequate privacy protections to receive non-US data, for example, by participating in the APEC CBPR. Indeed, the United States already participates in the APEC CBPR, at least with respect to companies within the FTC's jurisdiction. That participation can and should be broadened to all US industry sectors. The fact that the new United States-Mexico-Canada Agreement (USMCA) explicitly validates the CBPR as a cross-border transfer mechanism and encourages the parties to promote and develop this and similar interoperability mechanisms, supports this point. Indeed, a new US privacy framework should also explicitly refer to CBPR and similar mechanisms, including the APEC Privacy Recognition for Processors (PRP) system now in effect, which allows personal information processors to

demonstrate their ability to assist personal information controllers in complying with relevant privacy obligations.[17]

Advancing global interoperability, accountability schemes and cross-border transfer mechanisms like the APEC CBPR is essential. Many of the global privacy regimes share common privacy requirements. To the extent these common requirements are reflected in mechanisms like the CBPR, EU Binding Corporate Rules, ISO standards or future GDPR certifications or other codes and certifications, these schemes can be made interoperable with each other to reduce the administrative burden for companies associated with having to begin from scratch each time they seek certification or approval in these various overlapping and similar systems. Organizations should be able to leverage their existing certifications and approvals to be certified or approved in another system. Apart from schemes like the APEC CBPR, there is no path toward global interoperability (short of having one global privacy standard). As such, given the importance of global data flows in enabling productive economies and innovation, the goal of interoperability is of utmost importance.

Last but not least, the EU GDPR makes data transfers from the EU to third countries significantly easier if these third countries are deemed "adequate" in terms of their data protection framework. Thus, while meeting EU adequacy should not be the main driving factor in devising a new US privacy framework, the elements necessary to meet the EU's (and other countries') adequacy requirements should be seriously considered and implemented in the United States where appropriate and consistent with the overarching goals of enabling effective consumer privacy and innovation. This may be in the interest of US multinational companies, as well as SMEs.

In this context, it is important to stress that adequacy does not require the privacy regimes to be identical. As noted in the case of the recent EU-Japan adequacy decision, the Japan privacy regime was deemed adequate despite not having all the requirements of the GDPR. This demonstrates that in devising appropriate privacy regimes, countries should not be blindly copying the GDPR without having a regard to their own constitutional and legal culture and heritage. Any future US privacy framework may be able to benefit from adequacy findings in other jurisdictions in the long run, especially as the United States would have already had some exposure to the EU considerations in the context of the negotiations and reviews of the Privacy Shield mechanism. It is in the elements of this mechanism that NTIA should be seeking starting points for ensuring interoperability with the EU.

6. Incentivizing privacy research

CIPL fully agrees with the goal of having the US government encourage and incentivize research into and development of products and services that improve privacy protections. However, this

[17] See "APEC Privacy Recognition for Processors ('PRP') Purpose and Background," available at https://cbprs.blob.core.windows.net/files/PRP%20-%20Purpose%20and%20Background.pdf.

goal should be broadened and amplified along the lines of the argument for incentivizing organizational accountability generally, as discussed in the above-mentioned CIPL white paper on this topic.[18] The following table taken from this paper sets forth some of the specific incentives regulators and/policymakers could provide to organizations to encourage active implementation of accountability. Some of these overlap with the "incentivizing" goal described in the RFC; others could be included in this goal going forward:

Using demonstrated accountability[19] as a differentiating or mitigating factor in investigation or enforcement contexts
For example: • As one of the discretionary factors in considering whether to initiate an investigation or enforcement action. • As a mitigating factor in assessing the type of penalties and levels of fines. • As a mitigating factor in case of an individual failure/human error, where the organization is able to demonstrate that it took reasonable precautions to prevent the failure or error. DPAs should communicate this policy regularly and refer to it in specific enforcement cases.
Using demonstrated accountability as a "license to operate" and use data responsibly, based on organizations' evidenced commitment to data protection
As one of the bases for: • Facilitating responsible AI, machine learning, automated decision-making and other big data applications because of the risk assessment, mitigations and other controls in the accountability program. • Allowing broader use of data for social good and research. • Participation in relevant "regulatory sandbox" initiatives.[20]

[18] *Supra* note 3.

[19] "Demonstrated accountability" includes all the essential elements of accountability (i.e., leadership and oversight, risk assessment, policies and procedures, transparency, training and awareness, monitoring and verification, and response and enforcement). Thus, the degree to which each of the accountability elements are demonstrably implemented within an organization will impact the degree to which such implementation can serve as a mitigating factor.

[20] CIPL would like to draw NTIA's attention to an interesting "regulatory sandbox" initiative at the UK Information Commissioner's Office (ICO), which recently sought public comment on this initiative to create a supervised safe space for piloting and testing innovative products, services and business models in the real market, using the personal data of real individuals. See ICO call for views on creating a regulatory sandbox, available at https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-call-for-views-on-creating-a-regulatory-sandbox/ and CIPL's response to the call for views, 11 October 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_ico_call_for_views_on_creating_a_regulatory_sandbox__11_october_2018_.pdf. Such initiatives could, among many other benefits, help establish legal certainty for organizations that are uncertain about the legal and regulatory implications of proposed new data uses.

Publicly recognizing best-in-class organizations and showcasing accountable "best practices" (including those that may be an aggregation of such best practices compiled and generalized by regulators)
• To promote reputation and trust of accountable organizations. • To promote healthy peer pressure and competition in the marketplace.
Supporting and guiding organizations (particularly small and emerging companies) on a path toward accountability, either individually or through association bodies
For example: • Compliance agreements used by the Canadian Office of the Privacy Commissioner.
Co-funding between DPAs and industry for research into novel accountability tools
• Similar to proposals contained in the Privacy Bridges Report of 37th International Privacy Conference, Amsterdam 2015[21] (See Bridge 10 on Collaborating on and Funding for Privacy Research Programs). • Specific grants by regulators such as the UK ICO and Canadian federal and provincial regulators to fund research projects in accountability.
Offer to play proactive advisory role to organizations seeking to implement accountability
• In context of novel technology or business models. • Offer specific resources, including documentation and dedicated contact persons, to support the implementation of heightened accountability.
Using accountability as evidence of due diligence
For example: • In a selection process for processors and other vendors. • In M&A transactions.
Using formal accountability schemes as evidence of uniform and high-level privacy protection to enable cross-border data transfers within the company group and to third parties
• APEC CBPR and PRP; EU BCR; GDPR certifications.
Articulate proactively the elements and levels of accountability to be expected
• For instance, at what point would expecting accountability measures constitute undue hardship to organizations?[22] • Based on the concept of proportionality and a risk-based approach to accountability measures.

Table 1 – Incentives for Implementing Accountability

[21] "Privacy Bridges: EU and US Privacy Experts in Search of Transatlantic Privacy Solutions," 37th International Privacy Conference, Amsterdam, 2015, at page 40, available at https://privacybridges.mit.edu/sites/default/files/documents/PrivacyBridges-FINAL.pdf.

[22] Some regulators, as a matter of their statutory duty, already consider the impact on organizations of adopting regulator recommendations as to best practices. Making these impact determinations for more of their recommendations and suggested best practices will include conducting more detailed impact assessments to measure the costs and benefits to organizations of adopting such practices.

In addition to providing specific incentives to organizations, regulators and law- and policymakers should also consider how to incentivize and encourage third-party certification bodies and "Accountability Agents" to become involved in facilitating organizational accountability through formal accountability schemes such as certifications. The success of accountability through formal accountability schemes depends on the willingness of competent certification bodies and Accountability Agents of all sizes to enter the market.

We believe that incentivizing accountability is crucial to a successful privacy framework. It enables a race to the top whereby organizations not only strive to comply with the bare minimum of what is legally required but are incentivized, and rewarded for, heightened levels of organizational accountability that benefit all stakeholders. This result is unlikely to be achieved by the mere threat of law enforcement or market pressures. Enforcement and market-based incentives must be augmented by proactive policies and incentives provided by policymakers and privacy regulators, as described in the attached CIPL white papers on this topic.[23]

7. FTC enforcement

CIPL agrees that the FTC should be the principal federal agency to enforce any new comprehensive US privacy legislation and should be appropriately resourced as such. As noted above, however, a new comprehensive privacy framework and a central national privacy enforcement authority should work with and around existing well-functioning sectoral regulations and regulators that already have significant regulatory and enforcement expertise in their respective sectors. It should also be considered whether amending or even replacing inconsistent federal sectoral privacy laws would be appropriate. Exactly how a new privacy framework and the FTC as the principal federal agency should interact with other federal functional regulators and sectoral privacy laws should be carefully considered and worked out with input from all relevant stakeholders.

8. Scalability

CIPL agrees on the goal of "scalability" of enforcement, which should be proportionate to the scale and scope of the information an organization is handling and should be outcome-based in the same way as organizations' privacy protections should be outcome-based rather than uniform. This approach allows the enforcement authority to prioritize its enforcement and other oversight activities according to the significance of the harm at issue and thereby be as effective as possible within the resources it has.

The FTC already practices this approach. However, with increased responsibilities under a broader privacy law, the FTC will have to ensure that its current approach is adapted to the

[23] *Supra* note 3.

changes in the scope and nature of its responsibilities. CIPL's recent discussion paper on strategies for data protection authorities to improve their effectiveness in privacy enforcement and regulatory oversight addresses issues directly relevant in this context. They include strategies for prioritization of regulatory and enforcement activities and alternative approaches to enforcement that ensure compliance by regulated entities through a variety of means grounded in "constructive engagement" between the authority and regulated entities.[24] Some of these directly support and enable the scalability issue identified by NTIA. While the practices described in this paper largely reflect current FTC practice, any new US privacy law should ensure that it, too, is consistent with this approach. It should affirmatively encourage and enable constructive engagement and collaboration between the privacy enforcement authority and industry to achieve effective compliance and should preserve the FTC's ability to reserve legal enforcement actions primarily for willful, intentional, repeated and grossly negligent violations.

Also, in the section on "scalability," NTIA suggests that privacy obligations must be tailored to the nature of the organization's processing activities and that, therefore, there should be a distinction between organizations that control personal data and processors that merely process data on behalf of controllers. CIPL agrees with this notion. The GDPR, the APEC Privacy Framework and many other international privacy regimes include this distinction. We encourage NTIA to define these concepts and their relevant obligations consistent with these global examples to further support global interoperability.

Finally, we believe that the accountability obligations can also be scaled to the size of the organization and the nature of its business—that is a key feature and purpose of accountability. The elements of accountability would still remain the same, but implementation would take into account the particular needs and constraints of SMEs.

Suggestion for additional goals for federal action:

9. **Enabling effective use of personal information**

CIPL encourages consideration of an additional goal: enabling broad and effective uses of personal information for the benefit of economic development and societal progress, as well as for the benefit of individuals, particularly the data subjects. Of course, this goal can be seen as subsumed under the above goal regarding "legal clarity while maintaining the flexibility to innovate." However, this important point might be clearer when separately stated. Modern data protection and privacy enforcement authorities cannot be responsible only for protecting consumer privacy. Due to their supervisory position with respect to personal information, they also have the responsibility to safeguard and facilitate the beneficial potential of such

[24] See CIPL paper on "Regulating for Results: Strategies and Priorities for Leadership and Engagement," 10 October 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_final_draft_-_regulating_for_results_-_strategies_and_priorities_for_leadership_and_engagement_2_.pdf.

information and, therefore, the full range of responsible and accountable data uses. Although it is already implied in the risk-based approach set forth in the RFC, this dual role of a privacy framework and of privacy enforcers should be clearly articulated in any comprehensive privacy framework.

IV. Next Steps (Request for Comment, p. 12)

The RFC also seeks input on next steps and specific measures the administration should take to effectuate the proposed outcomes and goals and whether there are other ways this approach could be implemented, such as through executive action or procurement or other non-regulatory actions. The RFC also asks whether the Department of Commerce should convene people and organizations to explore additional commercial data privacy issues.

In response, CIPL recommends that NTIA take a holistic and deliberate approach toward developing a comprehensive privacy law that accomplishes the items discussed in the RFC, as supplemented by CIPL (and likely many other commenters).

Further, we believe that each of the proposed outcomes and goals should be fleshed out in greater detail. One possible next step could be to actually articulate the outcomes and goals in draft legislative language to provide a clearer basis for further discussion on the precise elements and articulation of each of them. We recommend an iterative process between NTIA and other public and private sector stakeholders toward that goal. We believe that while the process should not be unduly rushed, it should proceed at a pace that reflects the need to sooner rather than later address both the competing state law developments and international developments.

This would also help address another question raised by NTIA: "If all or some of the outcomes or high-level goals described by the RFC were replicated by other countries, do you believe it would be easier for US companies to provide goods or services in those countries?" We believe that it would, because it would improve interoperability and reduce the number of inconsistent requirements that create significant compliance burdens on multinational companies. However, until the United States has a comprehensive and final framework that is easily explainable and replicable, it will be difficult to get other countries to adopt its approach. Instead, other approaches that may not be as well suited to maximize both privacy and innovation are more likely to be widely adopted.

V. Conclusion

We hope the above comments provide useful input into the development of a new US privacy framework. We look forward to further opportunities to comment and provide input into this process. If you have any questions or would like additional information, please contact Bojana Bellamy, bbellamy@huntonAK.com, Markus Heyder, mheyder@huntonAK.com, Nathalie Laneret, nlaneret@huntonAK.com, or Sam Grogan, sgrogan@huntonAK.com.