National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899
PrivacyFramework@NIST.gov

5 July 2019

Re: NIST Privacy Framework Draft

To Whom It May Concern,

Access Now continues to support NIST's development of a privacy risk management framework.[1] While we maintain our firm belief that there is an urgent need for a federal data protection law that provides meaningful protections and rights for individuals,[2] we believe the NIST framework can assist in developing the processes and procedures to operationalize better privacy protections. It can also help develop a common vocabulary for individuals, technologists, and policy experts to productively discuss privacy-related topics.

In December 2018, Access Now submitted comments with specific recommendations for this project.[3] In our comments we emphasized the need for a user-centric process that explicitly recognizes that there are some activities that are inherently inconsistent with protecting and respecting privacy. We then submitted further comments in April 2019 in response to the draft outline.[4] Those comments included four broad recommendations, including a further emphasis on transparency and establishment of a broader conception of privacy. NIST released the full draft of the privacy framework in May 2019, shortly prior to its second workshop held in Atlanta, GA. Additionally, supplemental information was released in June 2019.

In order to re-emphasize the points raised previously, we include our previous submissions as appendices here. In addition, we discuss two new recommendations below in specific answer to the draft framework, the Atlanta workshop, and the supplementary materials.

About Access Now

Access Now is an international organization that defends and extends the digital rights of users at risk around the world.[5] By combining innovative policy, user engagement, and direct technical support, we fight for a free and open internet that fosters human rights. As part of this mission we operate a global helpline for users at risk to mitigate specific threats. Additionally,

[1] *See* https://www.nist.gov/privacy-framework.
[2] *See* https://www.accessnow.org/data-protection-in-the-united-states-heres-what-we-need-to-protect-the-users/.
[3] *See,* appendix 1.
[4] *See*, appendix 2.
[5] *See* https://www.accessnow.org/.

we work directly with lawmakers at national and international forums to ensure policy decisions are focused on users and vulnerable populations.

Comments and Recommendations

At the outset, we recognize several positive aspects of the draft Framework. Perhaps most importantly, we laud NIST in its emphasis of trust, including the explicit recognition that implementation of the Framework must take into consideration more than legal compliance.[6] Not only does this approach ensure the Framework remains relevant in a shifting statutory landscape, but it promotes a vision of privacy that, as Access Now has recommended, focuses on real risks to individuals rather than data processors, which may often manifest as fees or penalties for legal or regulatory non-compliance. This approach may still be improved by providing a clear recognition that people from different communities may face different levels of risk in the processing of their data. The Framework should clearly establish and provide for the risks faced by vulnerable or marginalized populations, lest entities default to a more limited assessment of risk. One solution to assure this happens is for NIST to add a new step for identifying the individuals who may be impacted by a system, product, or service directly into the inventory and mapping phase, so that the different levels of information sensitivity may be considered in the assessment phase and throughout the process.

Additionally, we also appreciate NIST's clear recognition of a broader concept of privacy rights, including privacy risks felt not only by the individual but by society at large, though we take note that while this approach is introduced, it fails to find grounding throughout the Framework. Ensuring societal privacy risks are included throughout the Framework is one way NIST could improve further drafts.

Finally, we continue to favor NIST's approach to the Framework, including as an iterative and non-prescriptive document that can be easily adapted to a variety of different contexts and environments.

While the draft Framework is a considerable accomplishment, we believe there are also areas where future iterations could be substantially improved:

[6] While we applaud trust as an area of emphasis, we note that trust is distinct from trustworthiness and urge the NIST Privacy Framework to push toward the latter. As we explained in comments to the National Telecommunications and Information Administration, "NTIA's proposal states, "[u]sers must therefore trust that organizations will respect their interests, understand what is happening with their personal data, and decide whether they are comfortable with this exchange." Counter-intuitively, this framing puts the obligation to act to ensure data privacy on people instead of on the companies themselves. However, rather than people needing to blindly offer trust to companies, it is the companies that must demonstrate that they are worth[y] of receiving and processing user data. It is also the responsibility of companies to provide people with sufficient information in a manner that facilitates their understanding of the scope and purpose of that processing."
https://www.ntia.doc.gov/files/ntia/publications/access_now_-_ntia_consumer_privacy_comments.pdf.

1. ***The NIST Framework must place a renewed emphasis on broad understanding and outreach for non-technical audiences.***

Ultimately, the NIST Framework must serve a wide array of audiences with highly variant levels of expertise. While the current draft may speak well to engineers or other sophisticated audiences, it falls short in its ability to speak to any non-expert. People across the country, as well as around the world, may be impacted by the implementation of the Framework, and deserve to have a chance to contribute to its development. However, to do that it is necessary to ensure that materials, including the draft Framework itself, are written in an approachable and easily understandable format.

We recognize that it is important to balance accessibility with accuracy and the details necessary for entities to consider the nuances related to operationalization. However, this may behoove the inclusion of more, not fewer, materials, tailored to a variety of audiences and backgrounds. For example, we applaud the inclusion of an Executive Summary in the supplemental materials that NIST released in June 2019. However, even the Executive Summary is several pages long and full of terms of art and complicated references. Instead, a summary is necessary that accurately portrays the top level ideas and concepts but does so clearly and concisely. Additionally, it would be useful to have future drafts include specific, directed questions for individual response, each of which could be preceded by a shortened description of how the issue is handled in the draft.

The need for greater clarity can also assist the development of the Framework more broadly. The current format of the draft introduces numerous ambiguities that may be difficult for readers to resolve without substantial exposure to the document. A more streamlined and simplified version of the draft could act as an entry point for new readers as well as a place to introduce more complicated vocabulary and topics. This could be a useful tool for stakeholders to make the case for the Framework's implementation to colleagues, executives, and board members.

Finally, NIST should invest in translations of the Framework into other languages. Not only would this increase its potential positive impact, but the process of providing translations may provide insight into places where the Framework creates ambiguities by raising questions about word use and choice. The potential conversations created by translations into languages other than English could substantially improve the final products.

2. ***Education and awareness raising must be placed more centrally into the Framework's core.***

Another place where the draft Framework could be improved is by incorporating education as part of the proposed core. If the goal of the Framework is, as described, to increase the confidence and trust of individuals in the organizations that implement it, then a central part of

that implementation must include communicating its use to those impacted. However, because the very nature of the Framework is to allow it to be adapted differently by entities according to their needs, it becomes important to not only communicate that the Framework is being used, but how and to what ends.

Education can also be a two-way street. When people know more about how the entities they interact with consider their information and communications, they can better provide feedback on personal risk they face, which may be able to be incorporated into future iterations of the organization's implementation. This may be particularly useful with certain vulnerable or marginalized communities who may not have their interests represented adequately within the organization or entity. NIST should consider the best ways for entities to communicate with and educate all impacted individuals, particularly those from different backgrounds and across different communities, and including those with whom the entity does not maintain a direct relationship. The Framework then should be updated in order to provide guidance on these communications.

Conclusion

Thank you again for continuing to engage with the public and for the opportunity to provide comments. We look forward to attending future events and reviewing forthcoming materials.

Thank you,

Amie Stepanovich U.S. Policy Manager	Estelle Massé Global Data Protection Lead	Jennifer Brody Legislative Manager

Appendix 1 - Access Now Comments on "Developing a Privacy Framework (Docket No. 181 101 997-8997-01)" (1 December 2018)

Katie MacFarland
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899
PrivacyFramework@NIST.gov

1 December 2018

Re: Developing a Privacy Framework (Docket No. 181101997-8997-01)

Dear Ms. MacFarland,

Access Now thanks the National Institute of Standards and Technology ("NIST") for its work to develop a privacy framework to help "identify, assess, manage, and communicate privacy risks."[1] Earlier this year we warmly welcomed NIST's report on "An Introduction to Privacy Engineering and Risk Management in Federal Systems," and we encouraged private entities to adopt its approach.[2] As such, we are heartened by NIST's "consensus-driven, open, and collaborative process" and optimistic that NIST can help provide practical paths toward the implementation of meaningful privacy protections.

Protecting privacy is vital in the digital age, where data can be used to manipulate, discriminate against, and harm people. NIST has published a request for information ("RFI"), which grants an opportunity to provide feedback on the goals, framing, and path of the agency's process. Our comments provide both general observations about NIST's process to develop the Privacy Framework as well as feedback on specific questions NIST has posed.

About Access Now:

Access Now is an international organization that defends and extends the digital rights of users at risk around the world.[3] By combining innovative policy, user engagement, and direct technical support, we fight for a free and open internet that fosters human rights. As part of this mission we operate a global helpline for users at risk to mitigate specific threats. Additionally, we work directly with lawmakers at national and international forums to ensure policy decisions are focused on users and those most at risk.

[1] https://www.federalregister.gov/documents/2018/11/14/2018-24714/developing-a-privacy-framework.
[2] https://www.accessnow.org/new-report-helps-u-s-federal-agencies-protect-privacy-companies-use/.
[3] https://www.accessnow.org/.

Access Now has also provided comments to the U.S. National Telecommunications and Information Administration ("NTIA") on its development of the Administration's approach to data privacy.[4] As the RFI indicates, this process is happening in parallel to NIST's own. We encourage these processes to complement one another and our submissions to both processes are intended to be mutually-reinforcing. For ease of reference, we also are attaching the full text of that submission here as Appendix A.

In addition, as Appendix B we are attaching "Creating a Data Protection Framework: a Do's and Don'ts Guide for Lawmakers," a report written about our experiences working on and supporting the passage and implementation of the General Data Protection Regulation ("GDPR") of the European Union. Finally, Appendix C contains "A User Guide to Data Protection in the European Union," a practical guide on rights in the GDPR and how they can be exercised. We hope these resources will provide valuable information about international data privacy standards and practices that will be useful in NIST's development of a Privacy Framework.

General Observations

A. NIST's approach must continue to center on the user

In "An Introduction to Privacy Engineering and Risk Management in Federal Systems," NIST observed, "[a]n effective privacy risk model must capture the potential cost of problems to individuals."[5] This was a great victory for user-centric privacy. As we observed at the time:

> *"Focusing on the user seems like common sense, but the norm has been to focus exclusively on the entity collecting data, not the person whose data was being collected. This meant considering the users only by proxy, in the form of legal or reputational costs. That approach has been wholly inadequate for taking into account the wide range of threats that we face when our data are collected and processed, and the damage breaches can cause (such as the emotional impact of having our personal photos revealed to the world)."*[6]

We encourage NIST to commit to carry this principle into the development of the Privacy Framework.

It is important to note, however, that there is no model we are currently aware of to assess individual privacy risks, either on average or specific to a person. Accordingly, more research is necessary in order to determine metrics for evaluating impact before this principle can be

[4] https://www.accessnow.org/cms/assets/uploads/2018/11/NTIA-Consumer-Privacy-Comments.pdf.
[5] https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf.
[6] https://www.accessnow.org/new-report-helps-u-s-federal-agencies-protect-privacy-companies-use/.

properly implemented. NIST should invest in and incentivize this research, which must be expansive and not limited to financial harms. Instead, it must also include emotional, psychological, physiological, human rights, and other impacts that individuals may face on account of a privacy event. It should also include a probe of possibilities for individual and collective remedies, including the options people may have to respond to or mitigate those impacts.

Finally, when it comes to the assessment, it should also be noted that risk is often wrongly only considered in relation to the volume of data at risk. Entities processing large amount of data shall indeed have stringent security and privacy obligations, however, this does not necessarily mean small data sets or data processing activities are without risks. Beyond volume, risks must also take into account the type of data, including particularly sensitive data types such as health and biometric, and the amount of information it reveals about a single individual.

B. A risk-based approach to privacy must recognize that some risks are too high to mitigate

As noted in the RFI, NIST held an initial workshop on the Privacy Framework in October 2018 in Austin, Texas.[7] At that event, speakers appeared to reach consensus that the goal of the NIST process should be to find ways to mitigate privacy risk, but not to get rid of it.[8] While it may be true, as the speakers agreed, that risk can never be totally eliminated, it is important that the Privacy Framework recognize that some risks are too significant to be properly mitigated and advise that in these cases the activity giving rise to the risk should be forfeited by the entity. NIST should research a method for entities to determine where that threshold exists and identify when a proposed activity reaches it.

Additionally, the principle that the model should assess risks for the individual rather than the entity means that the threshold of acceptable risk should be communicated adequately to the individual, who should be able to exercise a choice about whether to accept that risk, along with steps that can be taken by the individual to mitigate that risk on top of what steps the entity has taken. For choice to be meaningful, alternative solutions shall be provided to individuals who decide that a risk is too high. In today's online environment, individuals encounter many "take it or leave it" approaches whereby they are required to agree to uninformative, complex, or misleading terms and conditions or tracking walls that require consent to tracking in order to use a service. If individuals do not agree to these unilaterally decided conditions, they simply cannot use the service. Such a model fails to both adequately inform the individual and provide meaningful choice. Privacy cannot exist on a "take it or leave it" approach.

[7] https://www.nist.gov/news-events/events/2018/10/kicking-nist-privacy-framework-workshop-1.
[8] https://www.nist.gov/news-events/events/2018/10/kicking-nist-privacy-framework-workshop-1.

A post-hoc example of how this may operate can be evaluated by its absence in the recent data breach at Facebook.[9] In that instance, to its credit, Facebook quickly notified (albeit inadequately) the population of potentially impacted users after the breach was discovered. However, as we noted at the time:

> *"[N]either [Facebook's] notice nor the blog post that it links to gives you any information for figuring out whether you specifically have suffered any damage from the breach. Even if Facebook isn't sure yet what, if any, of an individual's information has been compromised, it might have been helpful to advise people to review the information they have in their accounts. As the old adage says, it's smart to "hope for the best but prepare for the worst." That should be applied here from the perspective of the impacted users."*[10]

In the end, no matter what steps a data processing entity may take to mitigate risk, it is the individual who is best placed to understand the extent of a risk and make a decision based on their own context and risk threshold. This is not to say that notification is enough. Notice and choice, as experts have noted at length, is a failed model for protecting privacy.[11] Users must have rights to effectively control the processing of their data. There must be an obligation on entities to adequately protect that data, including to meaningfully limit when and to what extent data can be processed.[12] However, where entities are making choices regarding risk thresholds, informing individuals of the factors behind those choices and allowing them to weigh the risk for their own lives empowers people to make more informed, reasonable decisions for themselves.

Specific Responses

A. Minimum Attributes for a Privacy Framework

> *Consensus-driven and developed and updated through an open, transparent process* - It is too often true that multi-stakeholder processes get captured by the most powerful and well-resourced voices in the room.[13] NIST must ensure to its fullest capability that all voices are given equal footing in the development of the Privacy Framework. NIST should also recognize that even within a single sector, several groups may disagree about form or substance of a given issue, and take steps to ensure that a multitude of voices are heard and highlighted throughout the process and reflected in the document.

[9] https://www.accessnow.org/the-breachbook-chronicles-faq-on-facebooks-latest-privacy-debacle/.
[10] *Id*.
[11] https://epic.org/2016/07/epic-tells-fcc-to-reject-notic.html.
[12] https://www.accessnow.org/data-protection-in-the-united-states-heres-what-we-need-to-protect-the-users/.
[13] *See*, *e.g.*, https://www.eff.org/document/privacy-advocates-statement-ntia-face-recognition-process.

Common and accessible language - We applaud NIST for its commitment to accessible language, which we have found lacking in other government processes.[14] We encourage NIST to follow this through by ensuring that complicated concepts or documents on which the foundation is based are summarized or simplified for a general audience. For example, in places where NIST's Cybersecurity Framework is referenced, it would be good to provide detail on the overlap between the two processes so that an individual does not have to become well versed in one project to participate in this one.

Risk-based, outcome-based, voluntary, and non-prescriptive - We encourage that, among the outcomes presented here, NIST include "effectively protects privacy," or similar language to indicate action at limiting data processing rather than just encouraging research and innovation.

Compatible with or may be paired with other privacy approaches - The Privacy Framework should aim to take into account the benefits of and learn from the flaws of data protection laws around the world, including the GDPR in the European Union, the Brazilian Internet Law,[15] and other current or soon-to-be passed measures with which entities will have to comply.

B. Goals of the Privacy Framework

The RFI identifies three goals of a Privacy Framework:

I. To better understand common privacy challenges in the design, operation, and use of products and services that might be addressed through a voluntary Privacy Framework;
II. to gain a greater awareness about the extent to which organizations are identifying and communicating privacy risk or have incorporated privacy risk management standards, guidelines, and best practices, into their policies and practices; and
III. to specify high-priority gaps for which privacy guidelines, best practices, and new or revised standards are needed and that could be addressed by the Privacy Framework or a related roadmap.

While we find these to be admirable goals, we also find them to be missing important objectives. As with the outcomes identified above, we don't find that any of the goals

identified will actually address privacy challenges that impact users today. Additionally, while now is a crucial moment to establish uniform standards around data protection, neither the

[14] *See, e.g.*, https://www.ntia.doc.gov/files/ntia/access-04202015.pdf at fn 1 ("For purpose of this comment, we refer to the so called "UAS" as drones throughout, and encourage NTIA to do the same throughout its rulemaking process. In order to adequately involve the public as a stakeholder, it is important to use terms that the public understands and finds accessible. Nondescript acronyms will undermine public involvement and bias respondents toward government, companies, and a small number of civil society groups who understand the issue.").
[15] https://www.pnm.adv.br/wp-content/uploads/2018/08/Brazilian-General-Data-Protection-Law.pdf; *see also* https://www.accessnow.org/brazil-president-approves-data-protection-bill-but-vetoes-key-accountability-measures .

identified outcomes nor goals align with, complement, or even recognize those from the NTIA process.[16] For example, the NTIA process includes as goals to incentivize privacy research and FTC enforcement. We encourage NIST to harmonize the identified goals and outcomes with those of the NTIA proposal, along with any subsequent changes in response to public comments.

C. Specific Privacy Practices

One in the list of practices or services NIST expresses interest in receiving information is "de-identification." Here, we encourage NIST to exercise care in nuance. While information may be de-identified, in that it can be divorced from a specific direct identifier, databases with even a small number of data points are often at risk of re-identification with trivial ease.[17] Machine learning tools make this process even easier.[18] However, de-identification is not the only way to protect data: in fact it's only one within a spectrum of methods, including anonymization, wherein steps are taken to prevent re-identification.[19] NIST's inquiry should look beyond simply de-identification to include anonymization and aggregation techniques that will better protect data as artificial intelligence tools continue to advance.

Additionally, NIST also lists "enabling user preferences." Several academics have recently explored the extent that user interface and design decisions impact the ability of people to exercise meaningful choice regarding the use or distribution of their data.[20] Recently, a coalition of consumer organisations sent a letter to the Federal Trade Commission calling for an investigation into tech giants deceptive design practices that steer users to "agree" to privacy-invasive default settings.[21] Any exploration of the existence of user preferences should also include an element of analyzing the design choices that underlie those preferences, including efficacy, intuitiveness, and degrees of nuance, including within the nuance of differing contexts of use.

Conclusion

---

[16] *See*, https://www.federalregister.gov/documents/2018/09/26/2018-20941/developing-the-administrations-approach-to-consumer-privacy; https://www.federalregister.gov/documents/2018/10/11/2018-22041/developing-the-administrations-approach-to-consumer-privacy (extending deadline for comment).
[17] *See, e.g.*, https://www.zdnet.com/article/re-identification-possible-with-australian-de-identified-medicare-and-pbs-open-data.
[18] *See, e.g.*, https://journals.openedition.org/factsreports/4494.
[19] For the spectrum of ways to protect data, *see* https://fpf.org/2016/04/25/a-visual-guide-to-practical-data-de-identification/.
[20] *See, e.g.*, http://www.hup.harvard.edu/catalog.php?isbn=9780674976009.
[21] *See*, https://thepublicvoice.org/wp-content/uploads/2018/06/FTC-letter-Deceived-by-Design.pdf.

We appreciate NIST's engagement with the privacy community. We look forward to continuing to work with your office throughout this process.

Thank you,

Amie Stepanovich
U.S. Policy Manager
Access Now

Estelle Massé
Global Data Protection Lead
Access Now

Appendix 2 - Access Now Comments on "NIST Privacy Framework Outline" (1 April 2019)

National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899
PrivacyFramework@NIST.gov

1 April 2019

Re: NIST Privacy Framework Working Outline

To Whom It May Concern,

Thank you for your continued engagement on the development of a Privacy Framework.[1] While Access Now strongly believes in the need for a comprehensive data privacy law,[2] we also recognize the benefit of working to develop and implement better processes and approaches for corporate entities and other organizations to protect privacy. As such, we support the work being led by the National Institute of Standards and Technology (NIST).

Last year we submitted comments on NIST's Request for Information, noting "[p]rotecting privacy is vital in the digital age, where data can be used to manipulate, discriminate against, and harm people."[3] We emphasized the need for a user-centric process that explicitly recognizes that there are some activities that are inherently inconsistent with protecting privacy. Additionally, we made several specific recommendations, including for NIST to:

- Conduct comprehensive outreach and ensure materials are accessible for all audiences;
- Emphasize the protection of privacy as a key outcome;
- Provide for compatibility with global laws and policies, including the European Union's General Data Protection Regulation (GDPR);
- Expand upon the goals of the Privacy Framework to address challenges to users, as well as to better align goals with other government efforts;
- Recognize distinctions between de-identified, anonymized, and aggregated data;
- Analyze design choices that may impact the ability of individuals to identify and implement privacy tools and exercise their preferences.

[1] *See* https://www.nist.gov/privacy-framework.
[2] *See* https://www.accessnow.org/data-protection-in-the-united-states-heres-what-we-need-to-protect-the-users/.
[3] https://www.nist.gov/sites/default/files/documents/2018/12/12/nist_privacy_engineering_comments_from_access_now.pdf.

Access Now commends NIST in the progress made in the Privacy Framework Working Outline, [4] and here we provide further comments in brief.

About Access Now

Access Now is an international organization that defends and extends the digital rights of users at risk around the world.[5] By combining innovative policy, user engagement, and direct technical support, we fight for a free and open internet that fosters human rights. As part of this mission we operate a global helpline for users at risk to mitigate specific threats. Additionally, we work directly with lawmakers at national and international forums to ensure policy decisions are focused on users and those most at risk.

Recommendations

1. In designing and explaining the Functions, one of the elements of the Privacy Framework Core, NIST should add a new Function to provide a place for entities to consider discontinuation of overly-intrusive activities. In the alternative, NIST should expand the description of one of the existing Functions to expressly recognize that this may have to occur where risks that are identified are particularly great and potential safeguards are not adequate.

As explained in our initial response, there are some forms of data processing that should not be engaged in. It is incumbent upon the Privacy Framework to not only recognize that but to assist entities in making determinations about when and how to end projects where that is the case.

2. NIST should emphasize transparency beyond the Function of "Inform," which is related to "understanding about how data is processed." Right now, transparency is only mentioned in the "Inform" Function. Instead, an element of transparency should be included in all Functions, including "Control" (in regard to how safeguards can be understood and exercised) and "Respond" (specifically for nuanced transparency around specific incidents as well as blanket transparency on number of incidents and response pathways).

It is critical to see elements of transparency implemented into all of the Functions performed by an entity. Specifically, there should be detailed reporting on specific incidents, as well as statistical reporting that can help identify trends and patterns. Transparency should include

[4] https://www.nist.gov/privacy-framework/working-drafts.
[5] https://www.accessnow.org/.

steps to help individuals understand the potential impact of any incidents, including emotional or psychological impacts, and to respond where possible.

3. NIST should define and discuss privacy risk as an expansive concept, focusing on its impact on the individual or groups of individuals, including households, local communities, marginalized populations, or even society as a whole. The discussion of privacy risk management should also be elevated into the document itself rather than in an appendix.

In our initial submission we encouraged a user-centric framework, and we are glad to see that the Identify function specifically refers to "privacy risk for individuals." Here we clarify that NIST should include in this framing not only specific individuals, but also groupings and communities of individuals, including those who self-identify based on race, sexual orientation, political ideology, or other characteristics. Notably, we continue to believe the risk itself should be oriented to reflect the risk bore by the individual or group, and not the risk to the entity in terms of potential liability or public relations costs.

Additionally, organizations should be encouraged not only to identify specific risks, but also categorical risks whenever possible. By way of example, Facebook may not have anticipated that its relationships with third parties could result in electoral advertising manipulation (although this is debatable), the use of data received from Facebook to design and serve manipulative or discriminatory ads more generally was foreseeable and should have been addressed.

4. Identifying privacy risk often should include broad consultation with a variety of stakeholders. However, members of civil society, advocates, academics, and experts who may offer insight are often strained for resources. NIST should include the importance of these consultations explicitly and, as an extension of that, consider the responsibilities of entities in pursuing and partaking in these consultations.

Organizations may not be well placed to wholistically identify privacy risks, particularly those risks that are disproportionately faced by marginalized communities. Accordingly, organizations should be actively encouraged to engage in broad consultations to better anticipate those risks. However, since those who may be best suited to provide additional insight are often strained for resources -- both tangible and intangible -- it is necessary to consider how to engage responsibly and respectfully. NIST is well-placed to consider basic parameters for these consultations, which could benefit all actors.

Conclusion

Thank you again for continuing to engage with the public and for the opportunity to provide comments. We look forward to your further events and materials.

Thank you,

Amie Stepanovich
U.S. Policy Manager
Access Now

Estelle Massé
Global Data Protection Lead
Access Now

Drew Mitnick
Policy Counsel
Access Now