THE BETTER IDENTITY COALITION

Comments to the National Institute of Standards and Technology (NIST)

RFI on Developing a Privacy Framework

January 2019

The Better Identity Coalition appreciates the opportunity to provide comments to the National Institute of Standards and Technology (NIST) on its Request for Information (RFI) on Developing a Privacy Framework.

As background, the Better Identity Coalition is an organization focused on developing and advancing consensus-driven, cross-sector policy solutions that promote the development and adoption of better solutions for identity verification and authentication. Our members – 18 companies in total – are recognized leaders from different sectors of the economy, encompassing firms in financial services, health care, technology, telecommunications, fintech, payments, and security.

The coalition was launched in February 2018 as an initiative of the Center for Cybersecurity Policy & Law, a non-profit dedicated to promoting education and collaboration with policymakers on policies related to cybersecurity. More on the Coalition is available at https://www.betteridentity.org/.

Last summer, we published "Better Identity in America: A Blueprint for Policymakers" – a document that outlined a comprehensive action plan for the U.S. government to take to improve the state of digital identity in the U.S. Privacy is a significant focus: the Blueprint detailed new policies and initiatives that can help both government and industry deliver next-generation identity solutions that are not only more secure, but also better for privacy and customer experiences.

At the outset, we appreciate the decision by NIST to seek public input as it embarks on developing a privacy framework. The value of leveraging a public-private collaborative model to reduce risk in the digital world was demonstrated in NIST's efforts leading development of the Cybersecurity Framework several years ago, and it's one that we believe makes sense to replicate here.

Given our focus on identity, we are especially encouraged to see NIST taking a leadership role on this topic. The roots of NIST's privacy engineering program were in NIST's work leading the National Strategy for Trusted Identities in Cyberspace (NSTIC) – driven by a need to more concretely define how digital identity systems could be architected to enhance privacy and address potential privacy risks created by new identity systems. As we detail in this response, we continue to believe the intersection of identity and privacy is highly relevant.

We offer the following comments:

1. **The Coalition is highly supportive of the focus on ensuring good privacy outcomes, rather than prescribing how those outcomes should be achieved.**

   Technology is constantly evolving, and an overly prescriptive approach may fail to anticipate new innovations that might allow privacy to be protected in ways better than what is generally available today.

   NIST's call for a Framework that delivers a *"prioritized, flexible, risk-based, outcome-based, and cost-effective approach"* is the right one.

2. **Industry is already working to address privacy risk in identity systems.**

   The RFI noted that one goal was *"to gain a greater awareness about the extent to which organizations are identifying and communicating privacy risks or have incorporated privacy risk management standards, guidelines and best practices into their policies and practices."*

   As a Coalition, we highlighted the concept of privacy as it relates to identity in our Policy Blueprint, noting:

   > *The privacy implications of existing identity tools – specifically the ways in which the inadequacy of some identity systems has placed consumers at risk – have made clear that consumers need better identity solutions that empower them to decide what information they share, when they share it, and in what context.*
   >
   > *Accordingly, new identity proofing solutions should be crafted with a "privacy by design" approach. That means:*
   >
   > - *Privacy implications are considered up front at the start of the design cycle – and protections are embedded in the solution architecture*
   > - *Identity data is shared only when consumers request it*
   > - *Identity data that is shared is only used for the purpose specified*
   > - *Consumers can request release of information about themselves at a granular level – allowing them to choose to share or validate only certain attributes about themselves without sharing all their identifying data*

   Our embrace as a Coalition of the need to 1) address privacy risk in identity systems up front and 2) call for common approaches in addressing these risks, demonstrates one aspect of how the private sector is working together to address these issues.

3. **As part of crafting a Privacy Framework, NIST should consider what sorts of digital identity solutions will be needed by implementing organizations to properly address privacy risk and ensure good outcomes.**

   As we noted in our response last year to NTIA's Privacy RFC, several of the proposed privacy outcomes that NTIA hopes to achieve are dependent on the existence of well-designed, robust, digital identity systems.

   When properly designed, Identity becomes the "great enabler" of better privacy.

   Conversely, a lack of robust, privacy-protecting identity solutions may make it difficult to practically achieve several of the proposed outcomes. For example:

   - Access and Correction. The ability of a user to have *"qualified access to personal data that they have provided, and to rectify, complete, amend or delete this data"* (per the

NTIA RFC) is largely dependent on the ability of the organization holding that data to easily know whether the person demanding access to that data is actually who he or she claims to be. Any privacy framework must enable organizations to 1) validate the identity of a consumer making a request to access or correct their information, 2) securely authenticate them into the system – while keeping others out and 3) quickly connect them to their information.

Secure identity systems are essential for the practical implementation of any effective privacy framework. Digital identity proofing and authentication support an individual's ability to securely access and manage personal data held by organizations. Organizations can utilize effective digital identity solutions to better protect personal data from hackers and criminals looking to exploit privacy-related obligations to steal or delete personal data and commit fraud or theft.

- Control and Reasonable Minimization. An essential element of allowing consumers to *"exercise reasonable control over the collection, use, storage, and disclosure of the personal information they provide to organizations"* (per the NTIA RFC) are identity solutions that allow them to assert who they are – or in many cases, select certain identifying information about themselves to reveal at a granular level. Many current identity solutions create an all-or-nothing dynamic in terms of requesting data – providing consumers with a "false choice," or making it difficult for them to make choices.

  Robust identity solutions allow consumers to easily request release of information about themselves at a granular level and minimize data exposure through a choice – to share or validate only certain attributes about themselves without sharing all their identifying data. To be clear, however, this approach may not be appropriate in every circumstance, such as when a consumer's credit report is requested in accordance with the Fair Credit Reporting Act.

  Robust identity solutions also provide an effective way for organizations to authenticate that a consumer has provided consent to data collection, or a specific use of data.

- Security. Identity is far and away the most commonly exploited attack vector in cyberspace; 81% of 2016 breaches leveraged compromised credentials to get into systems. Strong identity solutions help mitigate the most common security risks.

A driving force behind the creation of the Better Identity Coalition was the realization that the U.S. lacks the robust identity infrastructure that is needed to deliver on these three outcomes today. Whether through NIST's work or elsewhere, any Federally-driven privacy effort should thus focus at least in part on addressing shortcomings in current digital identity solutions.

In a world where commerce is increasingly digital, well-designed identity solutions are becoming increasingly important in achieving good privacy outcomes.

4. **As part of crafting a Privacy Framework, NIST should also take care to not be overly prescriptive – lest it inadvertently preclude the use of tools that can protect consumers.**

   An important consideration for policymakers when crafting new rules or guidance on privacy and security is to make sure that language is not written so broadly that it might preclude use of promising technologies for risk-based authentication. For example, while Europe's General Data Protection Regulation (GDPR) limits the collection of data in many circumstances, it also highlights that when it comes to protecting security and preventing fraud, there are cases where an entity may have a "legitimate interest" in processing personal data – including in cases where such data can be used to deliver secure authentication or verification capabilities. This "carve out" has allowed the use of data-based security and consumer protection solutions to flourish.

   In contrast, California's recently passed California Consumer Privacy Act has more ambiguous language that some experts have interpreted as potentially allowing consumers to opt out of having their data used to protect against malicious, deceptive, fraudulent, or illegal activity. This could inhibit the deployment of new, innovative authentication and verification technologies and place consumers at risk – and provides an example of the potential consequences of overly prescriptive or poorly drafted policies or frameworks.

5. **Better tools are needed to determine what privacy risks or harms might arise from certain systems or applications.**

   Today, privacy is defined differently by many stakeholders, and there is a divide between compliance exercises and those solutions that actually help reduce privacy risk – the former does not always fully address the latter.

   One challenge to date has been identifying what actual privacy risks are – specifically, outlining the kinds of harms that might occur based on the design choices made. Many compliance-focused models fail to anticipate broader issues that may arise.

   The opportunity presented by this new NIST effort for government to collaborate with industry stakeholders on the development of new tools to identify and address privacy risk is one that our members appreciate. To the extent that NIST efforts to work in partnership with industry can help to further define the privacy outcomes that are most important, it can help to guide the private sector on where it should invest and focus.

We greatly appreciate NIST's willingness to consider our comments and suggestions, and welcome the opportunity to have further discussions.