THE BETTER IDENTITY COALITION

Comments to the National Telecommunications and Information Administration (NTIA)

RFC on Developing the Administration's Approach to Consumer Privacy

November 2018

Introduction

The Better Identity Coalition appreciates the opportunity to provide comments to the National Telecommunications and Information Administration (NTIA) on its Request for Comment (RFC) on Developing the Administration's Approach to Consumer Privacy.

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/.

This 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.

To that point, we are excited to see the release of NTIA's RFC. "Privacy" is a term that often means different things to different people – to the extent that government efforts 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 tackled 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*

Comments

At the outset, we appreciate the decision by NTIA to put its draft out for public comment. While the document is a solid draft, it will no doubt be improved through the comment process.

Given the focus of the Better Identity Coalition on consumer-facing identity, we have chosen not to comment on many of the issues raised in the draft – choosing to focus our comments on issues of direct relevance to the work of the Coalition. 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.

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

   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"* 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. Organizations holding data must thus have an efficient way 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.

     Organizations lacking a way to do this may fail to deliver access and correction, and/or may also open up the door for hackers and criminals to exploit inadequate identity systems to steal or delete personal data. Robust identity systems are needed to get a user back to his or her information.

   - 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"* are identity solutions that allow them to assert who they are – or in many cases, select certain things about themselves to reveal at a granular level. Yet some organizations take an all-or-nothing approach in terms of data that they request – providing consumers with a

"false choice" in some cases, or making it difficult for them to make choices in a way that is navigate.

Identity solutions that allow consumers to easily 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 – are essential to enabling user control and data minimization. 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. So long as organizations storing data are protecting it with weak identity solutions such as passwords or other phishable authentication tools, security will not be achieved.

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. A Federally-driven privacy effort should thus focus at least in part on addressing shortcomings in current digital identity solutions.

3. **A risk-based approach makes sense – but more work is needed determining what privacy risks or harms might arise from certain systems or applications.**

One challenge to date has been identifying what actual risks are in privacy – 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.

To that end, we are supportive of the language that calls for a risk and outcome-based approach in any Federal action – as well as the call for the government to incentivize privacy research. The latter is important to better understanding where privacy risks or harms may arise.

Here we would go further to say that not only should government look to incentivize research – government can also help by directly funding research.

4. **Any new privacy rules will require appropriate carve-outs for security and fraud prevention.**

An important consideration for policymakers when crafting new legislation or regulation on privacy and security is to make sure that new rules are not written so broadly that they 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.

To that point:

> Recital 47 of GDPR states: "The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned."
>
> Recital 49 of GDPR states: "The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned.
>
> "This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopped 'denial of service' attacks and damage to computer and electronic communication systems."

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 technologies and place consumers at risk. While this seems to have been a drafting error, it provides an example of the potential consequences of overly prescriptive or poorly drafted policy.

We greatly appreciate NTIA's willingness to consider our comments and suggestions, and welcome the opportunity to have further discussions. Should you have any questions on our feedback, please contact the Better Identity Coalition's coordinator, Jeremy Grant, at jeremy.grant@venable.com.