June 2018 FedID Meetup

Educating the Public (and Policymakers) on Identity

Approved for Public Release

Distribution Unlimited

Case Number: 18-2204; MP180376

POC: Duane Blackburn

The author's affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions, or viewpoints expressed by the author.

Introduction

The Federal Identity Forum (FedID) Planning Committee piloted a "meetup" concept on 20 June, in partnership with the National Institute of Standards & Technology (NIST) at the National Cybersecurity Center of Excellence (NCCoE) in Rockville, Maryland. Approximately 80 individuals attended; roughly 30% were federal employees.

While beginning to plan for the annual FedID conference, the Planning Committee decided that federal employees really needed opportunities to engage in informal conversations with the private sector about identity matters important to federal agencies, and the nation. The Planning Committee designed a three-fold approach for 2018:

1. Online resources to enable real-time exchange of information and communication (LinkedIn: bit.ly/FedIDChat and Twitter #FedID);
2. DC-based meetups to allow informal face-to-face conversations, generally focused on a specific topic of interest;
3. Annual FedID conference, where community members can get away from their daily demands and devote a few days to really engaging with each other, focusing on big-picture items, and mapping out the community's future.

The meetup on 20 June was the Planning Committee's initial meetup, with a topic of "Educating the Public (and Policymakers) on Identity." This meetup was structured as a dry-run for the approach the Planning Committee will use for several sessions at the September conference. Future meetups, if any, may or may not use this approach.

Meetup Format

The meetup followed a three-tiered structure. The first half-hour was devoted to having senior federal officials introduce the topic, explain its importance for the federal government now and in the future, discuss prior or ongoing efforts, and ask leading questions. The second half-hour provided an opportunity for others, primarily non-federal employees, to respond via multiple short duration "lightning talks". Speakers in this subsection could provide unique perspectives, discuss lessons-learned from prior efforts, or present innovative ideas for consideration. The final hour of the meetup focused on multiple small-group discussions, led by an overall proctor. This workshop segment operated under Chatham House Rule[1]

[1] https://www.chathamhouse.org/chatham-house-rule

The schedule for 20 June meet-up:

1:00 – 1:05 Welcome by NCCoE and FedID Planning Committee

1:05 – 1:35 Federal presentations

- Steve Posnack, Health and Human Services
- Matthew Scholl, NIST

1:35 – 2:05 Lightning Talks

- Industry Perspectives. Neville Pattinson, Gemalto
- Strategic Communications for Federal Identity Efforts. Tony Brown, BRTRC
- Helping the press get it right. Shaun Waterman, freelance journalist
- Dialogue on legislative & policy considerations. Tiffany Angulo, Congressional Blockchain Caucus & Duane Blackburn, MITRE (and former OSTP)

2:05 – 2:50 Workshop/Small group discussions

2:50 – 3:00 Small group report-outs and moderator closing thoughts

3:00 – 4:00 NCCoE-hosted light reception and facility tours.

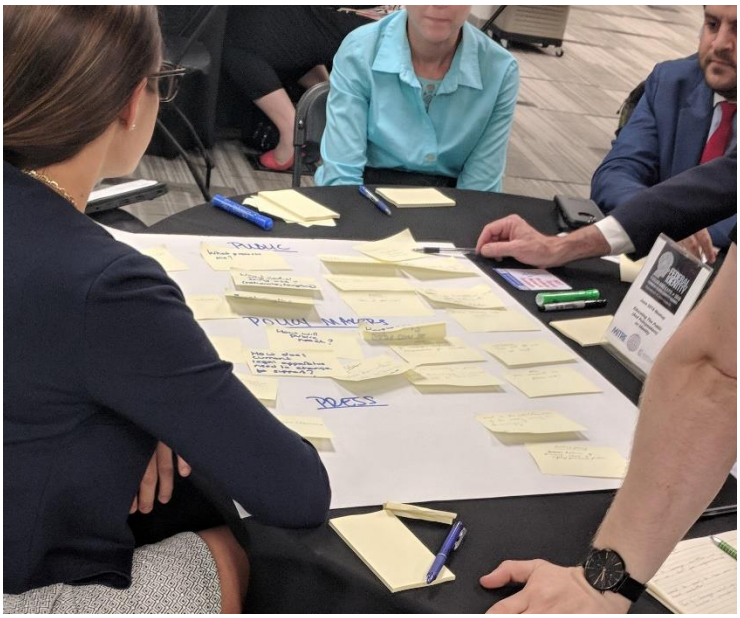
Workshop Approach

During the workshop, participants were seated in eight-person roundtables and worked through a series of steps to brainstorm concepts that could solve the meetup's *educating the public* focus and to draft an initial action plan for their favorite idea. That said, our primary driver for the workshop was to help spur conversations and build new relationships, rather than being predominantly focused on developing these action plans. There is always a need to balance between these two outcomes. For this meetup and topic, we leaned more towards ensuring conversations and relationships. For other topics, we would likely design the workshops so that action plan development would be the primary driver.

The workshop proctor issued a series of successive timed tasks, which each table worked through independently. Each table had a rapporteur, who briefly summarized the discussion and outcome in reports that are available in Appendix B. The assigned tasks are as follows:

1. Take three minutes for introductions at the tables.

    a. If you're finding that your table is full of federal employees, get up and move to a table that doesn't have any!
2. Three categories of interest (public, policymakers/legislators, and press/social media). What do we need each to know? (What would be our ideal outcome for each?)
    a. Take two minutes to individually brainstorm – write on the sticky note, then add it to the poster paper
    b. Then five minutes to share and discuss
3. Looking at the desired outcomes brainstormed, what are the limiting factors to achieving them?
    a. Individually brainstorm (write with marker on a sticky pad, place it overlapping the desired outcome). Then time for everyone to share their brainstormed ideas with the group
    b. 3 minutes brainstorm, 7 minutes discuss



4. Looking at the desired outcomes & limiting factors: what can be done, from a public-private partnership (PPP) perspective, to overcome the limiters and meet the objectives?
    a. Individually brainstorm (write with marker on a sticky pad, place it overlapping the desired outcome). Then time for everyone to share their brainstormed ideas with the group
    b. 3 minutes brainstorm, 7 minutes discuss
5. Take 3-4 minutes to select the group's favorite for each of the three categories, and your overall favorite. (No definition of "favorite" was given – enabled each group to define their own criteria.)
6. Now, take some time (ten minutes?) to develop an action plan. Some questions to consider:
    a. Are there any potential activities already in process that could be leveraged?
    b. What entities would need to be involved – who would best be able to help the government/community solve this?
    c. Who would be good at providing advice or mentorship?
    d. What would an ultimate solution to this issue look like?
    e. How does the community get from here to there?
7. Whole-room report-out.
    a. What groups picked the policymaker/legislators category as their favorite? Three minutes to explain your outcome and PPP plan.
    b. What groups picked the public category as their favorite? Three minutes to explain your outcome and PPP plan.
    c. What groups picked the press/social media category as their favorite? Three minutes to explain your outcome and PPP plan.

Feedback Received

Participants had generally positive reactions to the meetup, as they were happy to have the opportunity to meet individuals with similar interests and forge relationships with them. There seemed to be high levels of interest in holding future meetups.

One stated drawback to the approach was that we were trying to accomplish a lot in a short timeframe. The Planning Committee realized going into the event that two hours is certainly not enough time to generate public-private consensus on how to move forward on any topic. What we were hoping was to create a high-energy event that started conversations on an important topic and helped to grow the federal identity community. Both of those are necessary precursors for anyone wanting to take on this topic in more depth in the future.

Another stated observation was that it wasn't immediately clear what the common thread was that tied together the federal and lightning talk speakers, and which led to the workshops. This was discussed in the meetup announcement, but could have been better restated at the start of the meetup. It also would have benefitted for each individual speaker to tie their individual message into the broader theme – this is an important observation that should be considered when designing similarly-organized events in the future.

The proctor's instructions to the tables were given verbally. This was done by design so that adjustments could be made on the fly based on the proctor's observations, but it also led to some confusion at the tables (some tables were so invested in the prior conversations that they talked through their next instructions). Projecting instructions onto the presentation screen would have helped. Relatedly, the proctor kept time himself and gave verbal "two-minute warnings". Some groups felt a visible timer would have helped them manage their time better.

The end goal of the workshop wasn't stated at inception. Some attendees liked this, as it enabled them to flow through the steps without worrying about the end result; others felt the process would have been better, and some people more engaged, had the end result been known.

Proper seating within each small groups is always an issue. We worked to ensure that the federal attendees were well distributed throughout the groups and asked that people not sit with those they already know, but otherwise did not assign seating. We could have achieved better workshop results with strategically assigned seating, but doing so would have opened up additional issues (such as handling registrants that don't show up, and having to sort out who already knows whom in advance).

The tours at the end of the meetup were a nice touch that provided added value to participants and the host entity.

Acknowledgements

The FedID Planning Committee expresses their gratitude to:

- NIST and the NCCoE for hosting the event
- AFCEA for assistance with the Call for Presenters and meetup registration
- MITRE for strategic and logistics support, as well as the workshop table rapporteurs.

Appendix A – FedID Planning Committee Members

- **Department of Commerce:** Diane Stephens
- **Department of Defense:** Tom Clancy
- **Department of Health & Human Services:** Gary Cantrell
- **Department of Homeland Security:** John Boyd
- **Department of Justice:** Tom Callaghan
- **Department of Treasury:** Mark Hanson
- **General Services Administration:** Jim Sheire
- **Private Sector:** Jeremy Grant and Don Thibeau
- **Academia:** Stephanie Schuckers

The Planning Committee is chaired by Duane Blackburn; Combiz Abdolrahimi serves as a Special Advisor and Kelly Faddis is the Executive Secretary. The interagency partners with AFCEA to host the Federal Identity Forum; Ben Smith serves as the conference co-chair.

Appendix B – Rapporteur table reports

Federal Identity Forum
6/20 Meetup: Educating the public (and policymakers) on identity

Workshop table report-out[2]

Brainstorm: What do we need different groups to know, what are the limiting factors, and how do we overcome them?

Public

What do they need to know?

- Beware of promotional companies that overpromise solutions for consumers. There is no 100% secure solution – it's a matter of risk.
- The public needs to know the importance of Identity and why it's not an easy problem to solve
- You use 2FA already at your bank. Think of your debit card + PIN to access your account. Relate this to web use case.

Limiting factors?

- Skepticism of government in general
- Fear of biometrics misuse/loss

How do we overcome them?

- More education initiatives. For example, mobile devices generally store biometric data locally on device and is not transmitted.

Policymakers/legislators

What do they need to know?

- Ask for proof for any solutions. Again, commercial entities will promise 100% solutions that will not meet expectations.
- Not using 2FA/MFA is like keeping your front door unlocked
- Beware of vendor lock-in. Vendors will often propose solutions that inhibit the flexibility of organizations to move to different technologies.
- The policymakers need to know the importance of Identity and why it's not an easy problem to solve

Limiting factors?

- A general lack of awareness of policies / requirements of federal agencies.

[2] Workshop conversations followed the Chatham House Rule. (Participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.) Items presented aren't the positions of NIST, MITRE, or the organizations of the FedID Planning Committee.

- Lack of understand of how to operationalize laws/regulations once they are passed
- The cost of solutions often causes misunderstanding. There are significant upfront costs to identity solutions that are off-putting to legislators.
- Jurisdictional conflicts

How do we overcome them?

- Government certification programs
- Gov't agencies publish details about identity management approaches they use
- Jointly funded R&D (public / private)

Press/social media

What do they need to know?

- Beware promotional people. See Public section.
- It's important not to assume that there are simple solutions

Limiting factors?

- Lack of consequences for journalism that isn't accurate or explain identity issues adequately

How do we overcome them?

Action Plan – Which issue did the table decide to pursue, and what's the draft plan to move forward?

Issue:

- The public is not well educated on general identity issues and why they should go through the trouble of using technologies such as MFA.

Action plan:

- FTC/Industry Public/private initiative
- Educate congress about funding
- Using reporters/press to promote previous action items

Federal Identity Forum
6/20 Meetup: Educating the public (and policymakers) on identity

Workshop table report-out[3]

Brainstorm: What do we need different groups to know, what are the limiting factors, and how do we overcome them?

Public

What do they need to know?

- The public needs to understand basic terms and definitions around identity (this applies to all groups);
- They need to understand the context and culture around identity (e.g. how is it being used today that they may not be aware of, and in what circumstances; e.g., driver's license with RealID);
- Your information is already out there (compliments of many breaches) and opting out of an identity solution isn't really an option. The idea of anonymity is "quaint" but not realistic;
- Public should know how their identities, and the systems that hold them, connect (if at all). Many assume there is lots of information sharing around identity between different organizations and agencies, but that's not the reality;
- Users need to be informed (and shown) how to use identity tools and technologies.

Limiting factors?

- Fear is a limiting factor with this group; some fears are real and some are unfounded;
- Balancing "don't be afraid" with "anonymity is over";
- Lack of a federal ID program in the United States. This concept is not familiar to people and there is a general distrust around federal programs (and federal overreach) in this area ("big brother is watching" mentality);
- Large-scale data breaches continue to happen;
- Too many information resources, both trusted and untrusted;
- Technology usability issues; many people don't know how to use tech and don't want to learn;
- Users are often beholden to legacy infrastructure.

How do we overcome them?

- Encourage discussion between users (e.g., social media);
- Start small and demonstrate what's in it for them;
- Focus on younger generations and imparting knowledge at young age;

[3] Workshop conversations followed the Chatham House Rule. (Participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.) Items presented aren't the positions of NIST, MITRE, or the organizations of the FedID Planning Committee.

- Forced opt-in (think chips in credit cards; you don't have to use them, but then you don't get a credit card);
- Good user experience can overcome fears and increase adoption.

Policymakers/legislators

What do they need to know?

- Basic terms and maybe take it up a notch;
- State-of-the-art around identity is much farther along than they think;
- There is an identity ownership imbalance;
- Scope of government programs, and what may limit them (e.g., is there a lack of sharing);
- Opting-out of ID technology is not an option;
- Don't overestimate interoperability of systems.

Limiting factors?

- Fear around IDs and connections between biometric and other forms of ID;
- There are limitations (policy and technical limits), particularly around using biometrics;
- Policymakers and legislators have limited time and attention span; only focused on crisis of the day;
- What's important to constituents may not revolve around identity;
- Lots of turnover at the leadership level can upend projects and initiatives;
- Federal v. states rights issues (e.g., there are still several states that don't use RealID Driver's license).

How do we overcome them?

- Demonstrate cost savings;
- Demonstrate what's in it for them or what is good for constituents;
- Demonstrate technology (hands-on demonstrations);
- Catalog and amplify success stories.

Press/social media

What do they need to know?

- Basic definitions and terms around identity;
- Good identity technology can preserve privacy;
- Who the thought leaders are in this space;
- Scope of government programs;
- Success stories.

Limiting factors?

- Dissemination issues; sources are fragmented right now;
- How to find success stories when details are often classified;
- Knowing what you can and cannot share, particularly around say law enforcement sensitive info (cannot share).

How do we overcome them?

- Leverage them to get the word out and help explain tough concepts.
- Show how strong identity strengthens privacy.

Action Plan – Which issue did the table decide to pursue, and what's the draft plan to move forward?

Issue: Usability and user acceptance of identity solutions (for the public)

Action plan:

- Use government services to rollout identity technology and showcase successes; government is not just federal, but state and local level should be explored (start small);
- Leverage lessons-learned (successes and failures); find those who have rolled out successful innovations and leverage their knowledge;
- Showcase success stories (common theme throughout);
- What does the ultimate outcome look like? One identity credential that can be used across many identities (interoperable) and is strong;
- Who should provide? Big providers like Google, Apple, Facebook, Amazon etc. should be involved; we are their product and they can drive user adoption. Government should be involved, but not via regulation.

Federal Identity Forum
6/20 Meetup: Educating the public (and policymakers) on identity

Workshop table report-out[4]

Brainstorm: What do we need different groups to know, what are the limiting factors, and how do we overcome them?

Public

What do they need to know?

- Digital identity is important.
- Determine what the identity is
- How to differentiate identity and authentications
- Establish trust
- Educate that not all biometrics systems are the same
- The mental model
    - A mental model is an explanation of someone's thought process about how something works in the real world. It is a representation of the surrounding world, the relationships between its various parts and a person's intuitive perception about his or her own acts and their consequences.

Limiting factors?

- Making it seem like a benefit to the public
- Highlighting the benefits
- Trust
- Friction and how people identify product
- Technology adaption
- User friction
- Connection to the source
    - Accessibility to information
    - Harder to identify and stop

How do we overcome them?

- Education
- Press, establishing a good relationship with the press can help you overcome obstacles. People trust what the press/media release.
- Changing language so that the public can understand.

[4] Workshop conversations followed the Chatham House Rule. (Participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.) Items presented aren't the positions of NIST, MITRE, or the organizations of the FedID Planning Committee.

Action Plan – Which issue did the table decide to pursue, and what's the draft plan to move forward?

Issue:

- Trust

Action plan:

- Education
    - Introduce the topic in early education in STEM
    - Promote good practices
    - Demonstration of real world
    - Induce economic studies
    - Establish incentives to encourage
- Changing language
    - Comprehension and it will help them adapt and accept the benefits
- Media
    - Using Media (social media, press, etc.) as an avenue to establish trust

Federal Identity Forum

Educating Public and Policymakers on Identity

Group Discussion Notes

Session took place on June 20th, 2018

Held at the National Cybersecurity Centre of Excellence (Rockville, MD., USA)

Group brainstorming session

Public

What do they need to know	Limiting factors	How do we overcome them?
• Why should I care? What is in it for me? Why helpful? Why would I use this? How can life get easier?	• Benefits may be esoteric, delayed, non-specific, academic. • Conflicting information. Non- sequential delivery of information • Education • Trust • Habits and Attitudes not aligned with the product. • Loud stories that impacts public view into soundbite that isn't the whole story (e.g. Silk Road, Bitcoin are different from the rest of blockchain).	• Public campaigns, nuances to specific groups. • Telling the right story/narrative • Present positive case studies.
• What happens to my data? Who has access? What is the intent/mission of the entity using the technology?	• General distrust. Aversion to change. • How to be vague so no specific answers.	
• Can I trust? Lack of trust in government and elected offices	• Fear of change. Need for education. Past issue impacting trust. • Lack of understanding. • "Big Brother" argument	• Havin a universal regulation or certification. • Bust myths and understanding • Get companies to bring technology into the workplace where the employees will be surrounded by it – and

		then transition into the consumer world. • Transparency – purpose/goal, use/impact, combat fears • Senior Champions, with Vision and Governance
• What protects me? Can I opt out? Is my identity safe?	• These are real vulnerabilities and risks	• Leverage historical comparisons.
• What are the privacy boundaries?		
• What is the personally identifying information exposure?		
• Why do we need identify information?	• Knowledge/legacy systems and dogma.	• Asking thoughtful questions – keeping open mind on each end.

Policy Makers

What do they need to know	**Limiting factors**	**How do we overcome them?**
• Education and understanding of technology		• Better dialogue with stakeholders in private and public. Open mind with potential of technology
• Benefits – cut of waste, fraud, and abuse. How could it be abused or gaps be exploited?		
• How does current legal apparatus need to change to support new technology changes/policies?	• New set of laws, undiscovered landscape	
• How will public react?	• Too many subgroups to predict reactions/make happy	• One solidified statement • Not having ten people saying ten different things.
• Who are the decision-makers?		
• What is currently in place?		

• What technology is available? What will be available?		
• How does/will the process work?	• It's not defined or it's complicated	
• What are boundaries for usage, collection, transmission for identity?	• Many ideas. No collective voice. No singular correct answer.	
• How do we balance personal choice, public safety and public protocol?		

Press was not discussed in any depth.

Action plan

The group tackled the Policy Maker issue of: What are boundaries for usage, collection, transmission of/for identity?

- A working group session was proposed to involve public sector and private sector audiences, law-makers, international parties. The public sector would have to involve large and small parties. Large parties who might be reluctant to join may not want to interact or discuss much therefore may need to convince them to attend and collaborate (rather than passively attend and listen).
- The working group would need an initial vision/charter including timelines, roles and responsibilities, deadlines, and deliverables that people are held accountable for producing. The strong, focused leadership and vision will be pivotal to ensure inertia and motivation to continue – and that the working group is dedicated an appropriate priority amongst their other work.
- The working group would need to define/scope the problems that identity solves, the way it could be used. Consistent, specific terminology needs to be used by the group to ensure that that confusion does not arise. The focus may need to work less current technologies and more on conceptual capabilities to ensure that the working group produces recommendations that are future-proofed.
- Policy makers would need education on specific issues.

Federal Identity Forum
6/20 Meetup: Educating the public (and policymakers) on identity

Workshop table report-out[5]

Brainstorm: What do we need different groups to know, what are the limiting factors, and how do we overcome them?

Public

What do they need to know? Their digital identity matters because they don't think much about it. They think about Google login, Facebook login. Understanding what the identity is. How do you communicate identity is different from authentication and Federation. Making the connection between authN to phone vice giving their fingerprints to someone. The trust isn't there with federal government. Education is key. Biometrics aren't all the same.

Limiting factors? Make it a benefit to the public for adoption and acceptance. Change the mindset to the public. Speed of adoption. Friction is biggest limiting factor.

How do we overcome them? Awareness and training to the public. What is the mental model depending on maturity and context. Theme park model is very different then TSA. How is data being monetized?

Policymakers/legislators

What do they need to know?

Limiting factors? Friction of policy level and technology. How mitigate the risk.

How do we overcome them?

Press/social media

What do they need to know?

Limiting factors?

How do we overcome them? Credible stories/sources.

Action Plan – Which issue did the table decide to pursue, and what's the draft plan to move forward?

[5] Workshop conversations followed the Chatham House Rule. (Participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.) Items presented aren't the positions of NIST, MITRE, or the organizations of the FedID Planning Committee.

Issue: Trust and Acceptance primarily with public.

Action plan: Education, demos. Having a policy establishes trust. Education, changing the process.

Introduce the topic in early education as part of STEM. Success stories in real world. Demonstration real world applications. Introduce economic studies. Bring bank's level of success to public awareness from economic studies perspective.

More comprehensive to general public.

Use media as an avenue to educate the public.

Federal Identity Forum
6/20 Meetup: Educating the public (and policymakers) on identity

Workshop table report-out[6]

Brainstorm: What do we need different groups to know, what are the limiting factors, and how do we overcome them?

Public

What do they need to know?

- Identity is important to them
- Understand what "identity" means
- A Digital ID is based off of attributes of who you are
- Private information should be kept *private*
    - Regulations/laws on what must be kept private on websites can differ by where you live
- If you're only using a username/password – you're vulnerable

Limiting factors?

- Ease of use vs. burden
    - People want something that is easy – if it is difficult, it becomes a burden and they won't want to do it
        - i.e. Many people use the same password for all places because it's easier – they don't think about their security
- No one place
    - No technology or solution that works across all internet and platforms

How do we overcome them?

- First, people need to understand they're not in a good position – their security is at risk
- The only way to get people to take action into protecting their security is to create some simple tools/tech that protect identity

Policymakers/legislators

What do they need to know?

- Understand forms of ID
    - Public vs. government have very different needs, guidelines and capabilities
- Technologies involved

[6] Workshop conversations followed the Chatham House Rule. (Participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.) Items presented aren't the positions of NIST, MITRE, or the organizations of the FedID Planning Committee.

    - Understanding how Digital ID works so they can understand how important it can be
- Complex interdependencies between different technologies

Limiting factors?

- No authority over domain
- No government committee on identity
    - No one place to discuss and look to for best practices

How do we overcome them?

- Understand where they can make an effect
    - What regulations can be put in place to encourage people to protect their identity

Press/social media

What do they need to know?

- It is their responsibility to educate people on importance of identity

Limiting factors?

- Understanding the full picture of what is happening
    - Different guidelines from different sources across government – can be difficult because there is no one place to look for best practices
- Public is getting conflicting information from multiple press sources

How do we overcome them?

- Understanding public demand drives them
    - Figuring out how to drive public demand

Action Plan – Which issue did the table decide to pursue, and what's the draft plan to move forward?

Issue: Getting the public to understand that identity is important to them

Action plan:

Three main drives that can get people to adopt:

- Removing barriers and make it easier to be more secure
    - Simplified technology, streamlining where guidelines are coming from
- Needs to be pushed by large companies/big names
    - If Facebook/Google/Amazon, etc. required more stringent security, people would do it and could learn that it is important
- Education is crucial

- It is more important for people to know why they need to protect their identity rather than just forcing them to do it when logging in

Federal Identity Forum
6/20 Meetup: Educating the public (and policymakers) on identity

Workshop table report-out[7]

Brainstorm: What do we need different groups to know, what are the limiting factors, and how do we overcome them?

Public

What do they need to know?

-They play a role (referring to consumers)

-How do we better teach that to them?

-What constitutes identity?

-Differences with online reputation and actual data

-Needs to know different options (e.g. opt-in vs opt-out)

- People are being defined; actions, behaviors, thoughts, etc. – and as a tool for analytics

Limiting factors?

For all categories:

- We don't know the future
- The complexity of the ecosystem
- Education: social continuum that look at the issue of ID (rich vs poor think differently)
- Convenience plays a factor (e.g. Apple caters to customers)
- Is there something holding us back from a governance standpoint?
- Where are the carriers in all of this? Commercial vs. ethical incentives are misaligned
- Greater good is inconsistent among audiences
- Responsibility is vacant
- Identity is not a national priority

How do we overcome them?

For all categories:

- Begin thinking locally even though it's a global issue

[7] Workshop conversations followed the Chatham House Rule. (Participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.) Items presented aren't the positions of NIST, MITRE, or the organizations of the FedID Planning Committee.

- The government has a role in determining who we are; define core attributes; central identity proofing has to be made as priority so that it can be decided whether the policy makers, press, or an agency or carrier will lead governance
- Bring everyone together to look at this holistically
- Collaboration
- Education
- Tap into data
- Go beyond the social security number; it doesn't cover the people who aren't U.S. citizens

Policymakers/legislators

What do they need to know?

-Identity is an ecosystem; think about it more holistically

-They are serving multiple stakeholder groups

-Standard definition

-What is risk

Limiting factors?

See Public section above

How do we overcome them?

See Public section above

Press/social media

What do they need to know?

-The public needs educations

-Concepts of ID are culturally based

-Understanding proofing is difficult

Limiting factors?

See Public section above

How do we overcome them?

See Public section above

Action Plan – Which issue did the table decide to pursue, and what's the draft plan to move forward?

Issue: Incentive Structures are misaligned. (Policy makers)

General thoughts:

-Dilemma over regulating business.

-Can security be used as the common theme for a national action plan?

-For some sectors (like finance), better to rely on the government

Who needs to be involved?

Ecosystem

Public side: Govt agencies creating credentials

Private side: Carriers with cell phone data, device manufacturers, data brokers, social media sites, etc.

What does the ultimate solution involve?

-An authoritative source is necessary

-Only align the incentive to the extent that it's necessary

-"If you don't, then…" needs to be enforced.

****Note from attendees=Please display the questions on the screen to avoid confusion in the future.

Federal Identity Forum
6/20 Meetup: Educating the public (and policymakers) on identity

Workshop table report-out[8]

Public

- Needs to know they don't have to be afraid. Don't worry about biometrics. It's not something to be afraid of.
- How does a consumer correct a breach problem? Consumers have to go through a proxy to make sure that the issue is fixed. Like the Equifax problem.
- The public doesn't really understand the modalities. People are afraid of someone getting our fingerprint – but no their picture. Facial recognition is as advanced as fingerprints.
- You can request the FBI to provide everything that they have on you. Like getting your credit report.
    - Continuous evaluation is a problem – how do you get rid of the periodic investigations. There are thousands of background checks that are in process. Initial and investigation
- Have to let people know how important it is to identify them and that we can keep that information safe. **Facial recognition is the good news about identity – this is the idea we chose**
- Reassure the public that there's oversight and that there's checks and balances to make sure they aren't over-reaching.
- We need to be transparent
- Share success stories – like cold cases that are solved. DNA – 23 and Me

Policy makers

- Identity is an enabler – it can do great things in govt. it can save us a lot of money.
- Requirements over time shape policy – how do you get policy to shift to reflect the privacy issues.
- We have the ability to identify anyone. Where's the balance against privacy. Accountability, checks and balances
- One way to influence policy makers is more meet ups like this.
- Tell policy makers what's required. Be transparent. Then make sure that people understand that we're going to be fair and equitable.
- Political appointees. Need to motivate them to want to do this. Having measurable successes – show them how they can have an impact – i.e., saving money, getting funding. Easier to get a congressman to understand the issues and risks than policy makers. Avoid strawmen.
- You're important, but not as important as you think. You have to engage the policy makers to help them get to know you. Networking is important

Press/Social Media

- I'm a real person – don't destroy my life. Like what happened to McCrystal

[8] Workshop conversations followed the Chatham House Rule. (Participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.) Items presented aren't the positions of NIST, MITRE, or the organizations of the FedID Planning Committee.

- How can you tell if someone is a legitimate press person vs. a blogger who has an agenda, etc.
- The press will only publish things that are negative. It's difficult to manage the relationships so the message gets out correctly. FBI guy talked about the cold cases and how the press only printed stories critical of their efforts
- Faces are not protected by the 4th amendment. This message needs to be gotten out.
- The press is hard to do business with today.
- How do we make social media better – it's a huge megaphone that can sometimes do more harm than good
- Flood the press with positive stories.

We liked facial identity as an idea to solve identity issues– speed and accuracy are not a problem. 98% accurate now and only a year or so until it's perfect.

Identify a benefit for the public – i.e. reduced lines at the airport. Position it as a way of making you safer, i.e., scanning a crowd for bad actors. Another benefit is protecting your assets, you can get what's yours and no one else can. People can steal your phone and/or other ways for identification, but they can't steal your facial identity.

Oversight and policy. Lawmakers need to be tighter with their bounds so there's not as much interpretation. Reduce the amount of delegation of authority to the agencies that make policy. Congress needs to do a better job.

Flood the press with positive stories on why it's a good thing.

Federal Identity Forum
6/20 Meetup: Educating the public (and policymakers) on identity

Workshop table report-out[9]

Brainstorm: What do we need different groups to know, what are the limiting factors, and how do we overcome them?

Public: Generational Challenges

What do they need to know? Security aspects (i.e. security privacy vs. convenience); benefits (i.e. efficiencies, cost effectiveness); processes

Limiting factors? Lack of awareness; age (i.e. generational gap/challenges); economic status; competitive advantages

How do we overcome them? Increased/effective communication (i.e. gaps/risks); identify steps to educate the public on understanding and implementing transitions to new technologies

Policymakers/legislators: Knowledge

What do they need to know? Liabilities; regulatory/law requirements; how new technologies work; efficiencies (i.e. time, cost)

Limiting factors? Lack of awareness; age (i.e. generational gap/challenges); policies, laws and regulations; adoption rate gaps

How do we overcome them? Increased/effective communication (i.e. identify gaps/risks, align workstreams); use of social media (better more flexible communication with the public)

Press/social media: Benefits

What do they need to know? Benefits (i.e. use case protections)

Limiting factors? Lack of knowledge

How do we overcome them? Communicate positive/proactive use cases and consumer protections; simplify concepts; broader audience; breakdown industry specific streams; diversify strategies; appeal to an older audience

[9] Workshop conversations followed the Chatham House Rule. (Participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.) Items presented aren't the positions of NIST, MITRE, or the organizations of the FedID Planning Committee.

Action Plan – Which issue did the table decide to pursue, and what's the draft plan to move forward?

Issue: Knowledge (relevant across all 3 sectors)

Action plan: Better communication across all three sectors (i.e. closing the gap); simplifying information that is provided to the public; educate on cybersecurity early on (i.e. high school students); be proactive vs. reactive; be cohesive/consistent with messaging across all sectors