Levels of Identity Discovery

Kim Shepard
Duane Blackburn
Skip Reindollar

MITRE

November 25, 2013

Introduction

Multiple "applications" within the federal government and the private sector require some level of knowledge of the individual they are interacting with in order to provide specialized services. These applications could range anywhere from issuing a passport or checking employment verification to logging into a pseudo-anonymous online gaming network. The number of such applications within just the federal government is vast. A 2008 analysis[1] of 3400 federal information technology systems revealed that 27.4% of these systems required knowledge of a user's social security number, 26.6% required knowledge of an individual's name, and 13.2% required a date of birth. The numbers within the private sector are unknown, but anticipated to be significantly larger as the use of personal identification within both online applications and in-person interactions has rapidly proliferated.

Most attention within the identity community on this front has centered on recognizing individuals on repeat visits, because it is the more politically sensitive and technologically centered aspect of the problem set. The more important consideration, however, is often how these applications determine the individual's identity in the first place. In most cases this identity discovery is performed by the system managers themselves.[2] This siloed approach generates extra costs (an individual's identity must be established multiple times, even for the same federal agency or other system provider) while simultaneously increasing privacy impacts and possibilities of identity theft for the individuals (as personally identifiable information has to be transmitted to the system provider each time).

If a scheme could be developed that enabled prior identity discovery decisions to be trusted and used by others, then these costs and privacy impacts would significantly decline. As seen in the numbers above, the savings within just the federal government could be significant. Because of the distributed nature of this problem, there is no ideal entity to develop the scheme and no one has attempted to do so. MITRE's Capstone program was created to "fill the white space" on such issues for the federal government, and funded this project to initiate progress in a learned manner.

The basic premise behind this paper is that various applications require differing levels of assurance to know who is standing before them (physically or remotely for online applications) upon initial enrollment. A free online gaming portal does not have a definitive need to know the true identity of the person requesting an account, but a bank certainly wants to ensure that it is granting access to a 401k account to which an employer is depositing funds. Applications today use some form of graduated levels to establish a user's initial identity through some combination of selected identity attributes. There is just no consensus on how these levels are defined or implemented. This creates privacy issues, as

[1] The National Science and Technology Council's Identity Management Task Force Report, http://www.whitehouse.gov/sites/default/files/microsites/ostp/nstc-identitymgmt-2008.pdf.

[2] In the 2008 analysis mentioned above, only 28 of the 3400 IT systems analyzed accepted an identity that was generated externally from the federal agency that managed it.

personally identifiable information (PII) is often requested when it really is not needed. It also creates unnecessary economic burdens as application managers perform individual assessments instead of simply leveraging an assessment someone else performed previously.

This paper begins to explore this issue and aims to initiate further dialogue. It does not propose a detailed, peer-reviewed process that the authors feel solves this issue. Multiple parties with disconnected interests would need to first study the problem and voice constructive needs before a solution could be proposed. Rather, this paper provides a starting point so that those studies can take place, and provides data to enable discussions to begin with a common foundation.

Technical Approach

The authors approached this study via a two-step process. Step 1 entailed an online survey to gain critical insight into both current practices and the public's perception on various PII attributes. Step 2 was a workshop consisting of identity professionals. Survey results were shared, and workshop participants shared comments to drive future discussions. This paper presents results from each step, and concludes with potential actions for consideration based on workshop dialogue.

The online survey consisted of two separate parts.

Part 1 studied 15 PII attributes and how different sectors view them based on individuality, permanence, and importance. The four sectors were 1) law enforcement and homeland security professional, 2) national security and intelligence professional, 3) commercial goods/services provider, and 4) user of commercial services. The attributes included full name, date of birth (DOB), financial ID (e.g., credit/debit card number), Social Security Number (SSN), voter registration, and biometrics.

Part 2 gathered data on how current applications use PII attributes to initially establish a user's identity. Survey respondents were asked to consider applications in which they had recently enrolled, and to identify the PII attributes that were used within each enrollment. The 15 attributes were identical to those in Part 1. Respondents were then provided five graduated levels and asked which one they felt best related to the application:

> 1 = There is an extremely close alignment between me and this account. Great care was taken to ensure that I am the only one able to create the account. I would experience significant, long-term impacts should others be able to do so. (Extremely Me)
>
> 2 = I am the only one able to establish this account in my name. If others are able to do so, it would have a negative impact on me personally for a period of time. (Only Me)

3 = Others could create this account for me, provided they are doing so with my permission (or on my behalf). (My Behalf)

4 = There is no true connection to me at all with this account. It would be okay if someone pretending to be me created this account. (No Connection)

5 = Whatever, it's pretty much anonymous anyway. (Anonymous)

Survey Results

Approximately 225 participants completed the survey. A small percentage of surveys were partial completions; they were deemed inconsequential to the comprehensive results. As designed, Part 2 yielded more data rows than Part 1.[3] The remainder of this section summarizes the analysis findings and corresponding observations revealed in the survey data. Additional detail for Parts 1 and 2 can be found in Appendix A and Appendix B, respectively.

[3] Survey participants could take Part 1 only once but were encouraged to take Part 2 multiple times, once for each application.

Part 1: Data Analysis Findings

- Participants were diverse, with almost half defining themselves as predominantly commercial users versus someone in a community charged with managing an application (see Figure 1). The authors feel this to be a good balance.

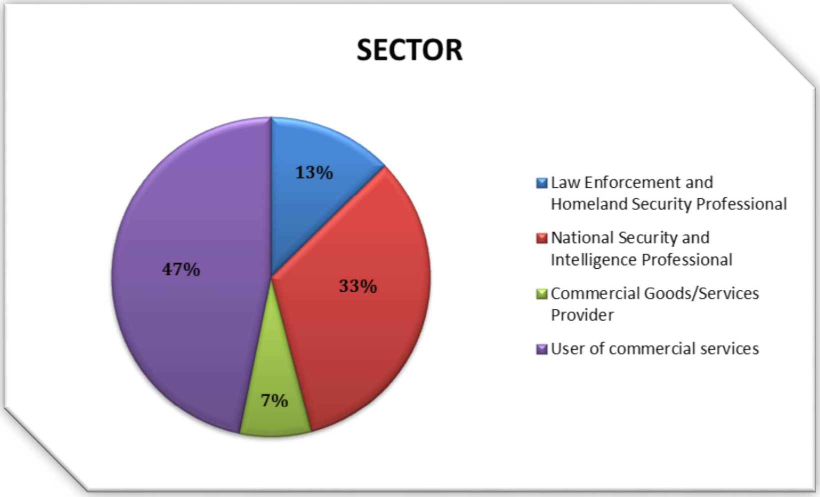


Figure 1. Participant Breakout by Sector

- Individuality
  - All sectors agree:
    - Biometrics is extremely individual-specific.
    - Nationality is not individual-specific.
  - Physical address is also viewed as very individual-specific.
  - Full name and DOB also rank high in individuality with the provider sector.
- Permanence
  - SSN and biometrics are viewed as extremely permanent.
  - Physical address, telephone number, and email address are viewed as less than permanent.
- Importance
  - SSN and biometrics are viewed as extremely important.
  - Nationality ranks as less important.

Part 1: Notable Observations

- Diligence: Respondents were more diligent in noting attributes viewed as individual-specific, permanent, and important— and less diligent when the attribute was viewed as less so.
- Nationality: Commercial providers had a higher regard for nationality than law enforcement and homeland security professionals.
- Individuality: Law enforcement and homeland security professionals viewed full name as less individual-specific than the other sectors.
- Permanence: Commercial providers often notably deviate from the response by other sectors. What is the key differentiator in the thought processes behind this response deviation?
- Importance: Commercial providers often notably deviate from the response by other sectors.

Part 2: Data Analysis Findings

- Full name is the most required attribute when establishing an identity.

- Full name, DOB, and physical address are the top required attributes when establishing an identity viewed as “Extremely Me.”
- SSN and telephone number are secondary attributes when establishing an “Extremely Me” identity.
- Email address is the top required attribute when establishing an identity viewed as “Anonymous.”
- Voter registration and marriage license are the attributes least used to establish an identity.
- Biometrics is not a frequently used attribute to establish an identity; when used, it is considered “Extremely Me” or “Very Me.”

Part 2: Notable Observations

- Nationality rated low in individuality and importance when studied in Part 1, but was often required in current applications when establishing identities viewed as “Extremely Me.”
- Biometrics rated high in individuality, permanence, and importance in Part 1; but is not often used when establishing an identity in current applications.
- Full name and DOB rated high in individuality and permanence in Part 1, and they are the most often used PII attributes when establishing an identity that is “Extremely Me” or “Very Me.”
- Full Name, DOB, and physical address rated low in Importance in Part 1, but were most often used when establishing an identity that is “Extremely Me” or “Very Me.”
- Permanence does not detract from requiring an attribute when establishing an identity (e.g., physical address).
- Respondents' feelings on individuality, permanence, and importance do not necessarily correlate to the attributes most frequently requested to establish an identity.

Workshop Discoveries

A collaborative workshop was conducted at the 2013 Biometric Consortium Conference. The survey results were summarized and workshop contributors were presented with two discussion starters drawn from the survey data. The first indicated a sample trust framework of five identity levels, with graduated attribute requirements based on how today’s current applications establish identity (refer to Appendix C). The second was an alternative framework based on survey participants’ viewpoints on the individuality, permanence, and importance of PII attributes (refer to Appendix D).

Workshop discussion, launched from the two sample trust frameworks, led to the development of a theoretical model for describing the five graduated levels, as shown in Figure 2.

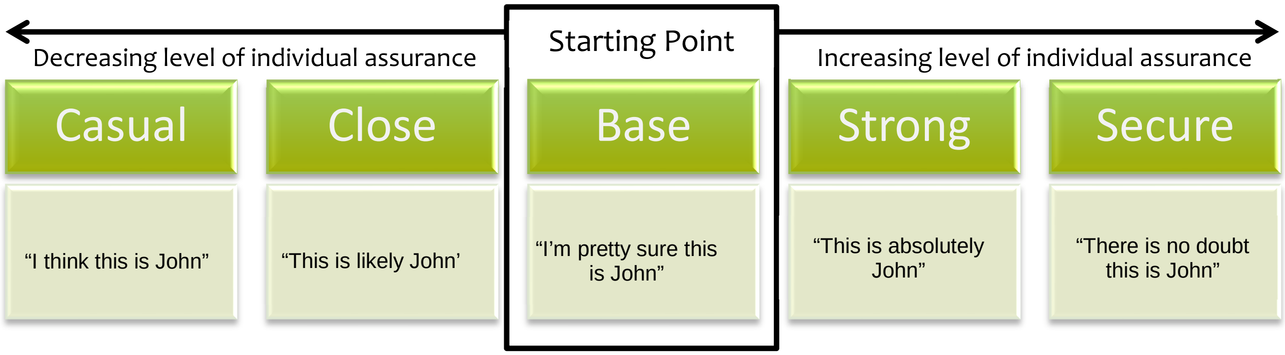

Starting Point
Decreasing level of individual assurance
Increasing level of individual assurance
Casual
Close
Base
Strong
Secure
"I think this is John"
"This is likely John'
"I'm pretty sure this is John"
"This is absolutely John"
"There is no doubt this is John"

Figure 2. Trust Framework Model, Workshop

This model assumes there is a "base" level that most applications would find sufficient; however, others would require greater or lesser levels of assurance that they truly know who is presenting themselves at enrollment. Potential applications within each identity level are noted below:

- Casual: fantasy football, blogs
- Close: retail reward programs, social media
- Base: most applications
- Strong: banking, employer credentials
- Secure: government-issued identity documents.

The workshop discussion centered on the concept that a standard vetting process for a base identity can be created using a limited number of PII attributes. Identities established via accredited applications could then be used by any other applications at the base level. Individuals would have a choice to also use this accredited identity decision on lower level (Casual or Close) applications, or they could choose not to and would thus have to re-establish their identity within those applications by sharing PII attributes. Individuals attempting to establish their identity for higher level (Strong or Secure) applications could use an accredited identity decision as a starting point, but would be required to share additional PII attributes.

The concept has potential for both economic and privacy benefits. Reuse of an accredited base identity in different applications saves resources for both the individual and the application provider. Reuse of the accredited base identity also means that individuals do not have to share PII attributes with every application provider, which would be a significant privacy enhancement.

The workshop was held as a session in a much larger federal identity conference, so discussion time was limited. Thus, the participants were not able to develop a consensus of which PII attributes should be used to create the base identity (or the other levels).

Participants did agree that the assignments shown in Appendix D, based on viewpoints of PII attributes, would be a better (and more thoughtful) starting point than those shown in Appendix C, based on current practices.

The workshop also yielded a number of other discussion points that should be considered in further refinement of the trust framework concept. The list below summarizes these discussion points.

- Consideration needs to be given to the power of multi-modal fusion. Analyzing two PII attributes in coordination is often more powerful than looking at two PII attributes individually. For example, approximately 87 percent of the U.S. population can be uniquely identified through this type of analysis using only their birth date, gender, and ZIP Code.[4] Performing this type of analysis would mean that fewer PII attributes would need to be collected.
- Applications participating in the trust framework must be accredited at a specified level of identity (e.g., Base or some other level).
- Individuals may choose not to participate in the trust framework; therefore, an alternate avenue to establish an identity must be available. For example, if individuals choose not to establish a base identity, an avenue to establish an identity with different applications should still be available to them, even if it means sharing their PII attributes multiple times across various applications.
- Applications users should be able to opt out of the trust framework. Confidence that their information will be properly removed will have to be demonstrated.
- Risk drives the level of identity required.

Potential Follow-on Actions

The survey results and workshop discussion indicate that this topic has interest and potential. Additional anecdotal evidence suggest a willingness for application managers to use other's identity discovery decisions in low assurance applications[5], but that a standards-based trust framework would need to be developed for higher assurance applications.

MITRE recommends the following as next steps to continue development of this trust framework:

Additional investigation. This project was designed to quickly verify the utility of the concept and to provide useful data for future consideration. Additional workshop-style discussions should take place to refine an initial trust framework (Figure 2) by fleshing out appropriate attributes by identity level. Simultaneously, an investigation into the costs of various applications' identity discovery decisionmaking should be performed, and potential

[4] L. Sweeney, *Simple Demographics Often Identify People Uniquely*. Data Privacy Working Paper 3. Pittsburgh, PA: Carnegie Mellon University, 2000.

[5] Consider how many online news sources and blogs already allow you to use your Facebook account to post comments.

cost savings should be estimated for the use of a trusted framework. One ideal study in this regard would focus on the DoD's Common Access Card, but others in different sectors would also need to be performed.

Pilots. Numerous pilots should then be performed within and across different assurance levels (Figure 2). The pilots would identify and overcome unforeseen issues, and provide valuable lessons-learned for refining the trust framework. Within the federal government, DHS could potentially take a lead in this regard with their numerous public-facing programs. Private sector pilots could focus more on the cyber subset of this space, and could be coordinated as part of a future phase of the National Strategy for Trusted Identities in Cyberspace[6].

Standards Development. A trusted framework as envisioned in this paper will require formal standards as its foundation. The National Institute of Standards and Technology, the federal government's lead for bringing together agencies and the public to develop standards, could convene an experts panel to initiate the process.

[6] http://www.nist.gov/nstic/

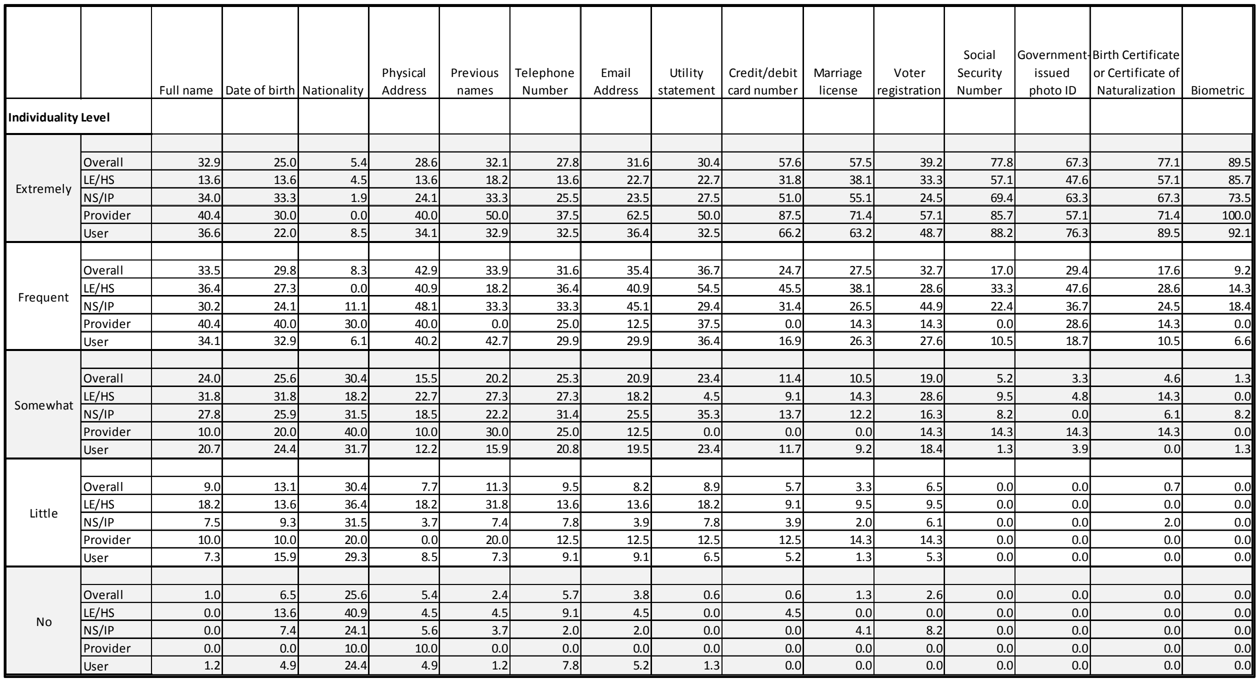
Appendix A
Part 1 Survey Data

In Part 1 of the survey, respondents were given a list of PII attributes and asked how they felt about each attribute in terms of its individuality, permanence, and importance. Figure A-1 presents the survey results on the individuality aspect, and presents how often (percentage of time) each attribute was selected as:

- Extremely individual-specific
- Very individual-specific
- Somewhat balanced
- Little individual-specific
- Not individual-specific.

An overall score is shown, as well as grouped by the following sectors:

- Law enforcement and homeland security (LE/HS)
- National security and intelligence professional (NS/IP)
- Commercial goods/service provider (Provider)
- None of the above, user of commercial services (User).



		Full name	Date of birth	Nationality	Physical Address	Previous names	Telephone Number	Email Address	Utility statement	Credit/debit card number	Marriage license	Voter registration	Social Security Number	Government-issued photo ID	Birth Certificate or Certificate of Naturalization	Biometric
Individuality Level																
Extremely																
	Overall	32.9	25.0	5.4	28.6	32.1	27.8	31.6	30.4	57.6	57.5	39.2	77.8	67.3	77.1	89.5
	LE/HS	13.6	13.6	4.5	13.6	18.2	13.6	22.7	22.7	31.8	38.1	33.3	57.1	47.6	57.1	85.7
	NS/IP	34.0	33.3	1.9	24.1	33.3	25.5	23.5	27.5	51.0	55.1	24.5	69.4	63.3	67.3	73.5
	Provider	40.4	30.0	0.0	40.0	50.0	37.5	62.5	50.0	87.5	71.4	57.1	85.7	57.1	71.4	100.0
	User	36.6	22.0	8.5	34.1	32.9	32.5	36.4	32.5	66.2	63.2	48.7	88.2	76.3	89.5	92.1
Frequent																
	Overall	33.5	29.8	8.3	42.9	33.9	31.6	35.4	36.7	24.7	27.5	32.7	17.0	29.4	17.6	9.2
	LE/HS	36.4	27.3	0.0	40.9	18.2	36.4	40.9	54.5	45.5	38.1	28.6	33.3	47.6	28.6	14.3
	NS/IP	30.2	24.1	11.1	48.1	33.3	33.3	45.1	29.4	31.4	26.5	44.9	22.4	36.7	24.5	18.4
	Provider	40.4	40.0	30.0	40.0	0.0	25.0	12.5	37.5	0.0	14.3	14.3	0.0	28.6	14.3	0.0
	User	34.1	32.9	6.1	40.2	42.7	29.9	29.9	36.4	16.9	26.3	27.6	10.5	18.7	10.5	6.6
Somewhat																
	Overall	24.0	25.6	30.4	15.5	20.2	25.3	20.9	23.4	11.4	10.5	19.0	5.2	3.3	4.6	1.3
	LE/HS	31.8	31.8	18.2	22.7	27.3	27.3	18.2	4.5	9.1	14.3	28.6	9.5	4.8	14.3	0.0
	NS/IP	27.8	25.9	31.5	18.5	22.2	31.4	25.5	35.3	13.7	12.2	16.3	8.2	0.0	6.1	8.2
	Provider	10.0	20.0	40.0	10.0	30.0	25.0	12.5	0.0	0.0	0.0	14.3	14.3	14.3	14.3	0.0
	User	20.7	24.4	31.7	12.2	15.9	20.8	19.5	23.4	11.7	9.2	18.4	1.3	3.9	0.0	1.3
Little																
	Overall	9.0	13.1	30.4	7.7	11.3	9.5	8.2	8.9	5.7	3.3	6.5	0.0	0.0	0.7	0.0
	LE/HS	18.2	13.6	36.4	18.2	31.8	13.6	13.6	18.2	9.1	9.5	9.5	0.0	0.0	0.0	0.0
	NS/IP	7.5	9.3	31.5	3.7	7.4	7.8	3.9	7.8	3.9	2.0	6.1	0.0	0.0	2.0	0.0
	Provider	10.0	10.0	20.0	0.0	20.0	12.5	12.5	12.5	12.5	14.3	14.3	0.0	0.0	0.0	0.0
	User	7.3	15.9	29.3	8.5	7.3	9.1	9.1	6.5	5.2	1.3	5.3	0.0	0.0	0.0	0.0
No																
	Overall	1.0	6.5	25.6	5.4	2.4	5.7	3.8	0.6	0.6	1.3	2.6	0.0	0.0	0.0	0.0
	LE/HS	0.0	13.6	40.9	4.5	4.5	9.1	4.5	0.0	4.5	0.0	0.0	0.0	0.0	0.0	0.0
	NS/IP	0.0	7.4	24.1	5.6	3.7	2.0	2.0	0.0	0.0	4.1	8.2	0.0	0.0	0.0	0.0
	Provider	0.0	0.0	10.0	10.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
	User	1.2	4.9	24.4	4.9	1.2	7.8	5.2	1.3	0.0	0.0	0.0	0.0	0.0	0.0	0.0

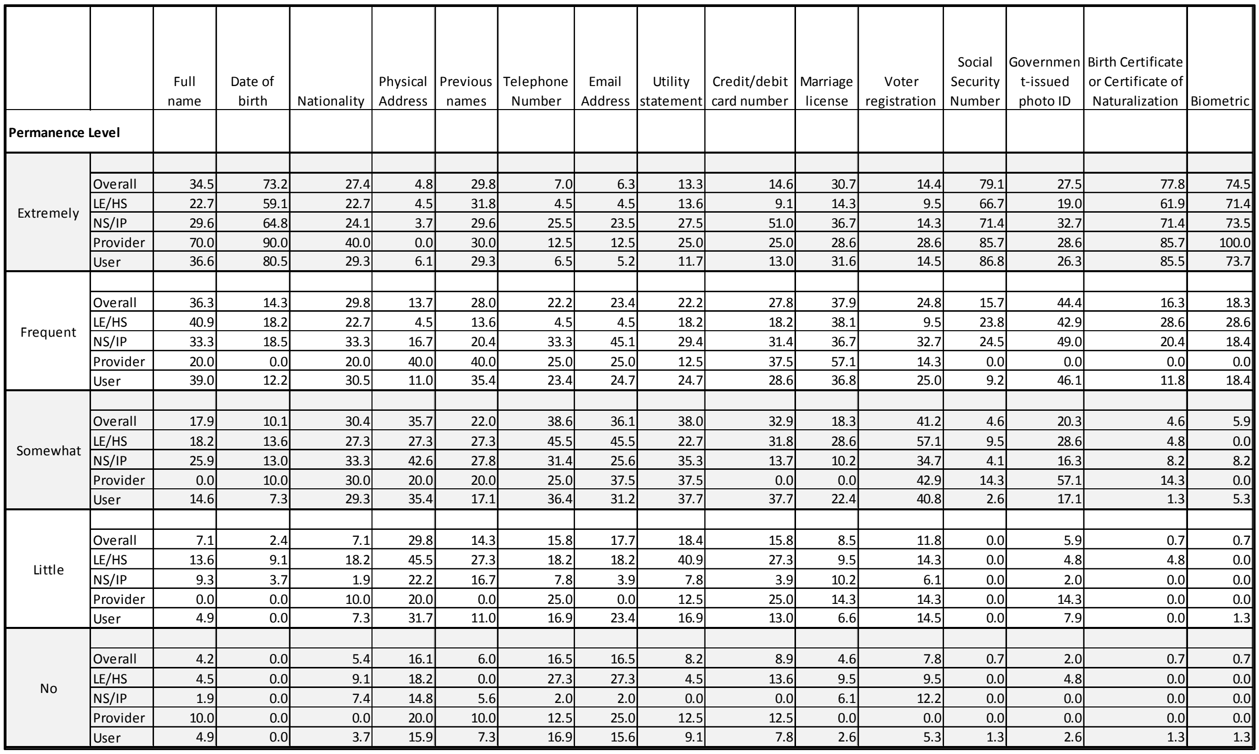
Figure A-1: Individuality Viewpoint

Figure A-2 presents the survey results on the permanence aspect, and presents how often (percentage of time) each attribute was selected as:

- Extremely permanent
- Very permanent
- Somewhat balanced
- Little permanence
- Not permanent.

An overall score is shown, as well as grouped by the following sectors:

- LE/HS
- NS/IP
- Provider
- User.



		Full name	Date of birth	Nationality	Physical Address	Previous names	Telephone Number	Email Address	Utility statement	Credit/debit card number	Marriage license	Voter registration	Social Security Number	Government-issued photo ID	Birth Certificate or Certificate of Naturalization	Biometric
Permanence Level																
Extremely	Overall	34.5	73.2	27.4	4.8	29.8	7.0	6.3	13.3	14.6	30.7	14.4	79.1	27.5	77.8	74.5
	LE/HS	22.7	59.1	22.7	4.5	31.8	4.5	4.5	13.6	9.1	14.3	9.5	66.7	19.0	61.9	71.4
	NS/IP	29.6	64.8	24.1	3.7	29.6	25.5	23.5	27.5	51.0	36.7	14.3	71.4	32.7	71.4	73.5
	Provider	70.0	90.0	40.0	0.0	30.0	12.5	12.5	25.0	25.0	28.6	28.6	85.7	28.6	85.7	100.0
	User	36.6	80.5	29.3	6.1	29.3	6.5	5.2	11.7	13.0	31.6	14.5	86.8	26.3	85.5	73.7
Frequent	Overall	36.3	14.3	29.8	13.7	28.0	22.2	23.4	22.2	27.8	37.9	24.8	15.7	44.4	16.3	18.3
	LE/HS	40.9	18.2	22.7	4.5	13.6	4.5	4.5	18.2	18.2	38.1	9.5	23.8	42.9	28.6	28.6
	NS/IP	33.3	18.5	33.3	16.7	20.4	33.3	45.1	29.4	31.4	36.7	32.7	24.5	49.0	20.4	18.4
	Provider	20.0	0.0	20.0	40.0	40.0	25.0	25.0	12.5	37.5	57.1	14.3	0.0	0.0	0.0	0.0
	User	39.0	12.2	30.5	11.0	35.4	23.4	24.7	24.7	28.6	36.8	25.0	9.2	46.1	11.8	18.4
Somewhat	Overall	17.9	10.1	30.4	35.7	22.0	38.6	36.1	38.0	32.9	18.3	41.2	4.6	20.3	4.6	5.9
	LE/HS	18.2	13.6	27.3	27.3	27.3	45.5	45.5	22.7	31.8	28.6	57.1	9.5	28.6	4.8	0.0
	NS/IP	25.9	13.0	33.3	42.6	27.8	31.4	25.6	35.3	13.7	10.2	34.7	4.1	16.3	8.2	8.2
	Provider	0.0	10.0	30.0	20.0	20.0	25.0	37.5	37.5	0.0	0.0	42.9	14.3	57.1	14.3	0.0
	User	14.6	7.3	29.3	35.4	17.1	36.4	31.2	37.7	37.7	22.4	40.8	2.6	17.1	1.3	5.3
Little	Overall	7.1	2.4	7.1	29.8	14.3	15.8	17.7	18.4	15.8	8.5	11.8	0.0	5.9	0.7	0.7
	LE/HS	13.6	9.1	18.2	45.5	27.3	18.2	18.2	40.9	27.3	9.5	14.3	0.0	4.8	4.8	0.0
	NS/IP	9.3	3.7	1.9	22.2	16.7	7.8	3.9	7.8	3.9	10.2	6.1	0.0	2.0	0.0	0.0
	Provider	0.0	0.0	10.0	20.0	0.0	25.0	0.0	12.5	25.0	14.3	14.3	0.0	14.3	0.0	0.0
	User	4.9	0.0	7.3	31.7	11.0	16.9	23.4	16.9	13.0	6.6	14.5	0.0	7.9	0.0	1.3
No	Overall	4.2	0.0	5.4	16.1	6.0	16.5	16.5	8.2	8.9	4.6	7.8	0.7	2.0	0.7	0.7
	LE/HS	4.5	0.0	9.1	18.2	0.0	27.3	27.3	4.5	13.6	9.5	9.5	0.0	4.8	0.0	0.0
	NS/IP	1.9	0.0	7.4	14.8	5.6	2.0	2.0	0.0	0.0	6.1	12.2	0.0	0.0	0.0	0.0
	Provider	10.0	0.0	0.0	20.0	10.0	12.5	25.0	12.5	12.5	0.0	0.0	0.0	0.0	0.0	0.0
	User	4.9	0.0	3.7	15.9	7.3	16.9	15.6	9.1	7.8	2.6	5.3	1.3	2.6	1.3	1.3

Figure A-2: Permanence Viewpoint

Figure A-3 presents the survey results on the importance aspect, and presents how often (percentage of time) that each attribute was selected as:

- Extremely important
- Very important
- Somewhat balanced
- Little importance
- Not important.

An overall score is shown, as well as grouped by the following sectors:

- LE/HS
- NS/IP
- Provider
- User

		Full name	Date of birth	Nationality	Physical Address	Previous names	Telephone Number	Email Address	Utility statement	Credit/debit card number	Marriage license	Voter registration	Social Security Number	Government-issued photo ID	Birth Certificate or Certificate of Naturalization	Biometric
Importance Level																
Extremely	Overall	48.8	43.5	11.3	18.5	23.2	20.9	20.3	20.3	39.9	30.7	17.0	73.2	58.2	67.3	74.5
	LE/HS	36.4	40.9	9.1	13.6	13.6	18.2	18.2	9.1	18.2	23.8	4.8	57.1	61.9	52.4	71.4
	NS/IP	46.3	38.9	11.1	18.5	25.9	29.4	27.5	27.5	49.0	36.7	14.3	75.5	63.3	69.4	67.3
	Provider	60.0	60.0	10.0	10.0	20.0	12.5	12.5	37.5	62.5	28.6	28.6	71.4	42.9	71.4	85.7
	User	52.4	45.1	12.2	20.7	24.4	16.9	16.9	16.9	37.7	28.9	21.1	76.3	55.3	69.7	78.9
Frequent	Overall	33.9	29.8	19.6	28.0	35.1	28.5	25.9	30.4	31.0	20.9	20.9	17.6	30.7	18.3	18.3
	LE/HS	27.3	27.3	18.2	31.8	27.3	22.7	22.7	45.5	36.4	19.0	19.0	19.0	23.8	14.3	28.6
	NS/IP	35.2	31.5	24.1	35.2	37.0	27.5	25.5	23.5	29.4	16.3	26.5	20.4	32.7	14.3	24.5
	Provider	30.0	10.0	30.0	30.0	30.0	25.0	37.5	12.5	12.5	28.6	14.3	0.0	14.3	0.0	0.0
	User	35.4	31.7	15.9	22.0	36.6	31.2	26.0	32.5	32.5	23.7	18.4	17.1	32.9	23.7	13.2
Somewhat	Overall	13.1	20.2	41.7	36.9	22.6	34.8	33.5	31.6	18.4	24.8	32.7	7.8	9.8	9.2	5.2
	LE/HS	27.3	22.7	36.4	36.4	40.9	40.9	36.4	31.8	22.7	33.3	47.6	23.8	9.5	19.0	0.0
	NS/IP	16.7	20.4	42.6	31.5	24.1	41.2	37.3	35.3	17.6	20.4	26.5	4.1	2.0	12.2	6.1
	Provider	0.0	10.0	50.0	30.0	10.0	37.5	37.5	25.0	0.0	14.3	28.6	14.3	42.9	14.3	14.3
	User	8.5	20.7	41.5	41.5	18.3	28.8	29.9	29.9	19.5	26.3	32.9	5.3	11.8	3.9	5.3
Little	Overall	4.2	5.4	22.6	13.1	12.5	10.1	17.1	12.0	7.6	16.3	21.6	0.0	0.7	3.9	2.0
	LE/HS	9.1	9.1	36.4	18.2	18.2	9.1	18.2	13.6	13.6	19.0	28.6	0.0	4.8	14.3	0.0
	NS/IP	1.9	7.4	20.4	9.3	7.4	2.0	9.8	9.8	3.9	16.3	22.4	0.0	0.0	2.0	2.0
	Provider	10.0	20.0	10.0	30.0	20.0	12.5	12.5	12.5	12.5	14.3	14.3	0.0	0.0	14.3	0.0
	User	3.7	1.2	22.0	12.2	13.4	15.6	22.1	13.0	7.8	15.8	19.7	0.0	0.0	1.3	2.6
No	Overall	0.0	1.2	4.8	3.6	6.5	5.7	3.2	5.7	3.2	7.2	7.8	1.3	0.7	1.3	0.0
	LE/HS	0.0	0.0	0.0	0.0	0.0	9.1	4.5	0.0	9.1	4.8	0.0	0.0	0.0	0.0	0.0
	NS/IP	0.0	1.9	1.9	5.6	5.6	0.0	0.0	3.9	0.0	10.2	10.2	0.0	2.0	2.0	0.0
	Provider	0.0	0.0	0.0	0.0	20.0	12.5	0.0	12.5	12.5	14.3	14.3	14.3	0.0	0.0	0.0
	User	0.0	1.2	8.5	3.7	7.3	7.8	5.2	7.8	2.6	5.3	7.9	1.3	0.0	1.3	0.0

Figure A-3: Importance Viewpoint

Appendix B
Part 2 Survey Data

In Part 2 of the survey, respondents were asked to think of a time when they had to initially establish their identity for some reason (e.g., an application). They were then asked how closely aligned to them (and only them) they felt the application was, using the following guide:

1 = There is an extremely close alignment between me and this account. Great care was taken to ensure that I am the only one able to create the account. I would experience significant, long-term impacts should others be able to do so. (Extremely Me)

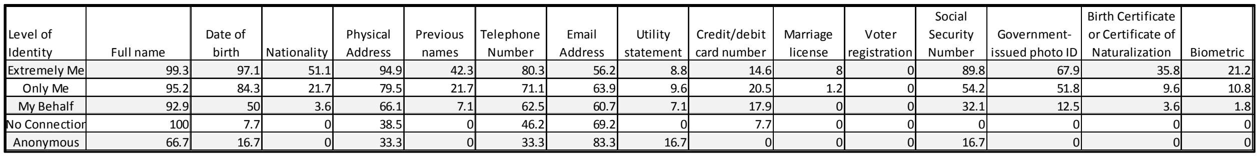
2 = I am the only one able to establish this account in my name. If others are able to do so, it would have a negative impact on me personally for a period of time. (Only Me)

3 = Others could create this account for me, provided they are doing so with my permission (or on my behalf). (My Behalf)

4 = There is no true connection to me at all with this account. It would be okay if someone pretending to be me created this account. (No Connection)

5 = Whatever, it's pretty much anonymous anyway. (Anonymous)

They were finally asked which PII attributes were requested when they attempted to establish their identity for that application. Figure B-1 shows how often each attribute was requested for each alignment level.

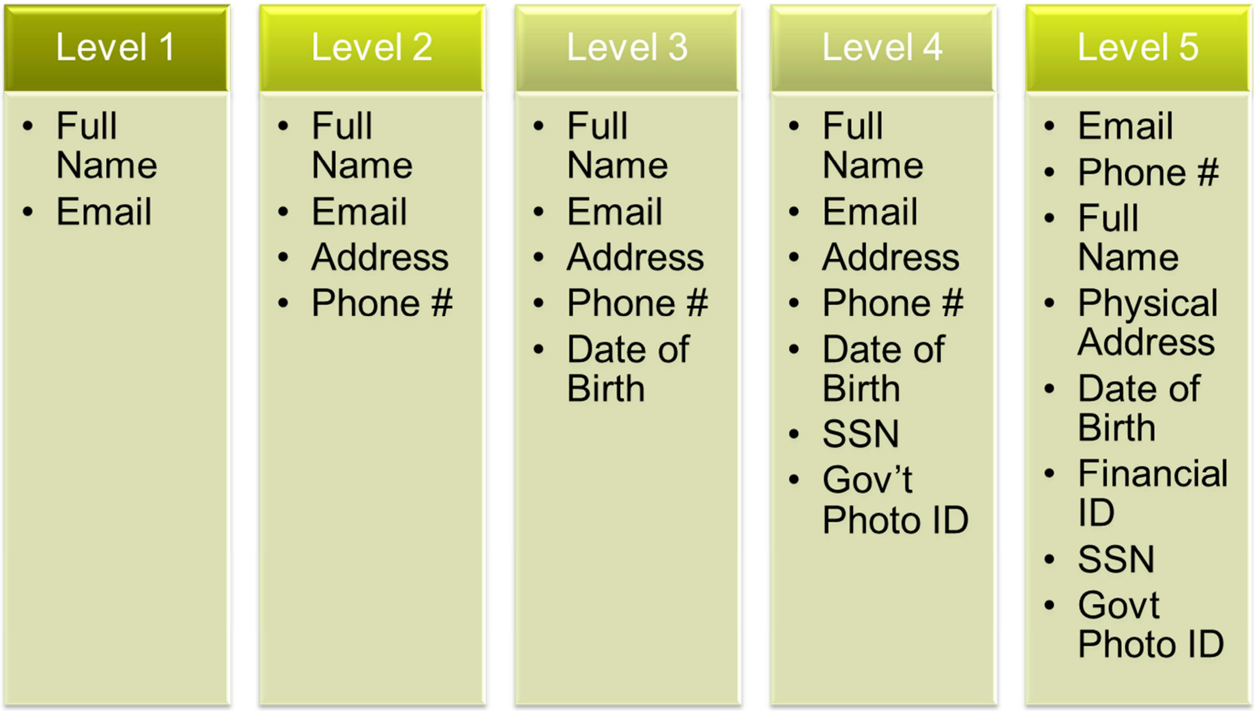


Level of Identity	Full name	Date of birth	Nationality	Physical Address	Previous names	Telephone Number	Email Address	Utility statement	Credit/debit card number	Marriage license	Voter registration	Social Security Number	Government-issued photo ID	Birth Certificate or Certificate of Naturalization	Biometric
Extremely Me	99.3	97.1	51.1	94.9	42.3	80.3	56.2	8.8	14.6	8	0	89.8	67.9	35.8	21.2
Only Me	95.2	84.3	21.7	79.5	21.7	71.1	63.9	9.6	20.5	1.2	0	54.2	51.8	9.6	10.8
My Behalf	92.9	50	3.6	66.1	7.1	62.5	60.7	7.1	17.9	0	0	32.1	12.5	3.6	1.8
No Connectio	100	7.7	0	38.5	0	46.2	69.2	0	7.7	0	0	0	0	0	0
Anonymous	66.7	16.7	0	33.3	0	33.3	83.3	16.7	0	0	0	16.7	0	0	0

Figure B-1: Attributes required to establish an Identity by Individual Alignment Rating

Appendix C
Starting Point A: Current Practices

To stimulate conversation at the workshop, the authors created two sample trust frameworks that show how PII attributes could be assigned to different levels. The trust framework in this appendix is based on an analysis from survey part 2 (see Appendix B), and shows what a framework would look like based on current practices.



Level 1

- Full Name
- Email

Level 2

- Full Name
- Email
- Address
- Phone #

Level 3

- Full Name
- Email
- Address
- Phone #
- Date of Birth

Level 4

- Full Name
- Email
- Address
- Phone #
- Date of Birth
- SSN
- Gov't Photo ID

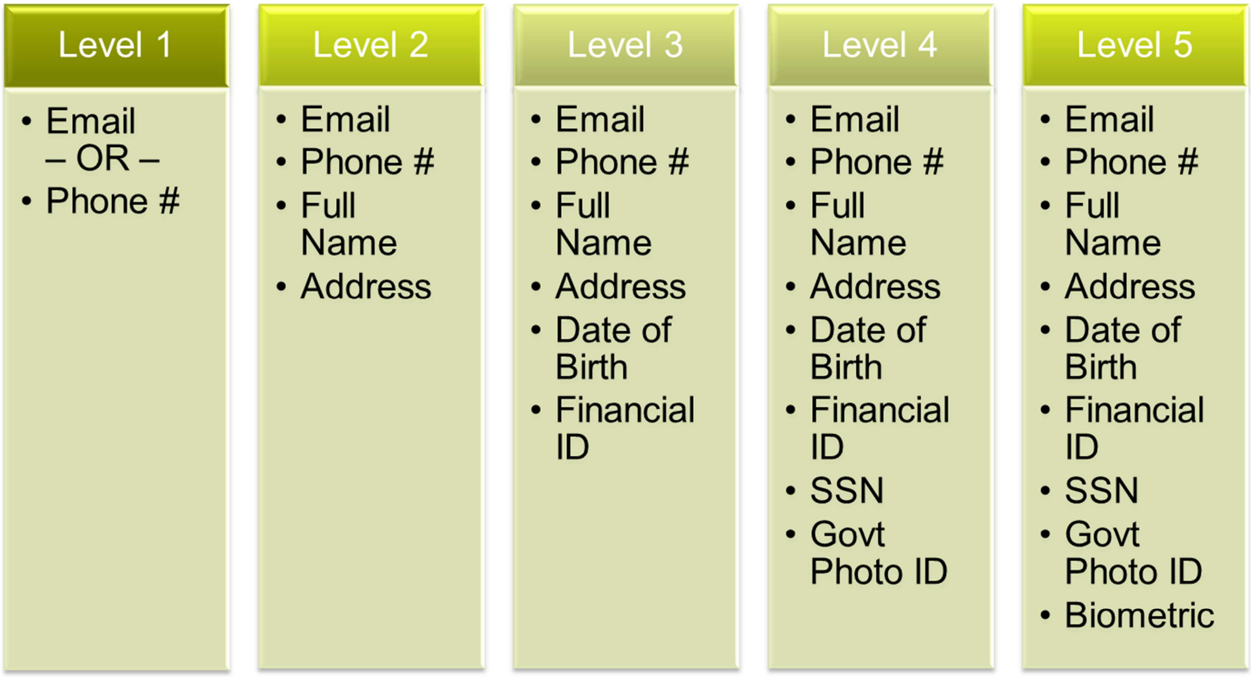
Level 5

- Email
- Phone #
- Full Name
- Physical Address
- Date of Birth
- Financial ID
- SSN
- Govt Photo ID

Figure C-1. Trust Framework Based on Current Practices

Appendix D
Starting Point B: Survey Participants' Viewpoints

To stimulate conversation at the workshop, the authors created two sample trust frameworks that show how PII attributes could be assigned to different levels. The trust framework in this appendix is based on an analysis from survey part 1 (see Appendix A), and shows what a framework would look like based on how individuals view individual PII attributes.



Level 1

- Email
  – OR –
- Phone #

Level 2

- Email
- Phone #
- Full Name
- Address

Level 3

- Email
- Phone #
- Full Name
- Address
- Date of Birth
- Financial ID

Level 4

- Email
- Phone #
- Full Name
- Address
- Date of Birth
- Financial ID
- SSN
- Govt Photo ID

Level 5

- Email
- Phone #
- Full Name
- Address
- Date of Birth
- Financial ID
- SSN
- Govt Photo ID
- Biometric

Figure D-1. Trust Framework Based on Participants' Responses