ID Pro Taxonomy and Body of Knowledge DRAFT

Introduction

A shared body of knowledge sits at the heart of any professional association.

For ID Professionals, the body of knowledge will contain the information that an ID Pro is expected to master, in their specific circumstances. So systems architects, security specialists, policy analysts, marketing representatives and business leaders should have knowledge of and possibly experience in specific subsections of information in the body of knowledge.

The ID Pro body of knowledge is structured around a taxonomy. The taxonomy is the organizational scaffolding used to categorize information. It has a regular structure within the different information domains to promote consistency. It is designed to be extendable to accommodate future authors' needs and priorities. The taxonomy should allow the project teams to fill in portions of the body of knowledge piece by piece, without having to create a linear narrative.

The section in this document on representational models includes visualizations of the taxonomy that can be used by different audiences: practitioners in specific job roles; consultants; regulators; exam takers; educators; and learners in general.

The taxonomy and table of contents for the body of knowledge are being developed in the current work phase. The objective is to describe the boundaries of information for practitioners. In future work phases, citations to published work will be added, and then new content will be incorporated.

The work is challenging but we hope it will stand the test of time and become one of the central structures keeping ID professionals connected.

-- The Editors

Table of Contents

High Level Concepts

Taxonomy

Taxonomy, in this context, refers to the overall scheme of classification used to describe the Digital Identity practices body of knowledge. Information is categorized into an initial layer which is used to separate specific areas of interest. These four areas are Identity, Authentication, Authorization and Management. Each of those four areas are described in the same four common sub sections of Concepts, Regulations, Best Practice and ‘Standards and Protocols’. By applying a consistent overarching categorization structure the Taxonomy becomes a device that can be depicted in numerous ways. This allows for an efficient means for the Identity Professional to expand and assess their level of knowledge.

Body of Knowledge

Whilst the Taxonomy describes the structure, the Body of Knowledge is the categorized information within the Taxonomy itself. It is the detailed content in each category and sub-category that provides the guiding data for professionals. The BoK is the living and breathing aparatus of the Taxonomy and will grow and contract based on the input of the Identity Professional community.

Representational Models

The taxonomy and body of knowledge are intended to contain a structured repository of information that an ID Professional could be expected to master, depending on their role and specializations. This structured repository is essential as a means of organizing the information, however the repository will not be very usable unless careful attention is paid to creation of representational models and finding aids which are tailored to specific consumers.

We use the term Representational Model to describe how information can be structured and organized for use by a specific audience or consumer. For example, a hiring manager might want to see a list of job skills related to a certain role; an exam-taker might want a cross-referenced textbook; an instructor might want concepts grouped by credential lifecycle. The representational model or models make it possible to generate these different outputs or representations of the body of knowledge.

Although the taxonomy already tries to describe the concepts of identity, authentication, authorization and management, each of those have multiple dimensions or viewpoints: vertically as with concepts, regulations, best practice and standards/protocols and horizontally if applying operational concepts such as what can be seen in the COBIT ‘Process Reference Model’ or within Project Management Approaches.

The group’s goal was to find a representational model which is able to combine all the different axes and viewpoints in a consistent and logical way, while the model itself should be as complete as possible but still easy to understand.

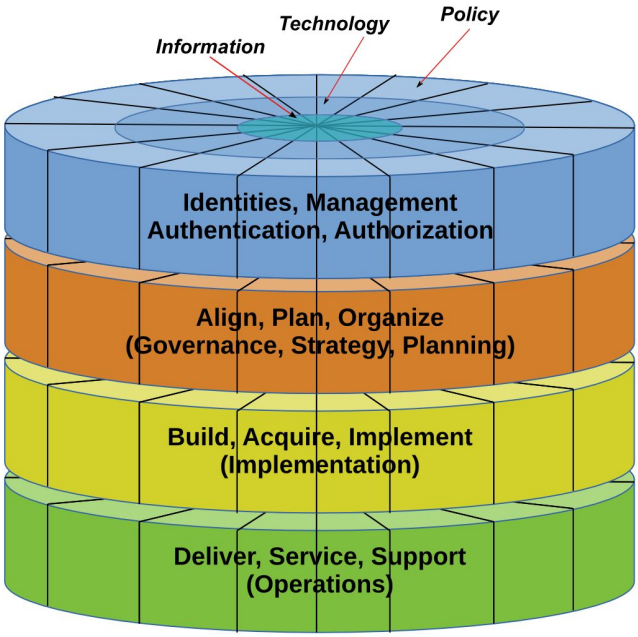
Another challenge during the model development was the fact that we explicitly tried to avoid to concentrate on ONE standard for a given area, even if that standard is widely adopted: We think, a complete body of Knowledge should also include concepts and ideas which are not commonly applied throughout the topic of interest. Apart from the fact that there is no such standard.

Based on these considerations, we developed two models: a Dart-Board (or cake?) model which is oriented on the taxonomy idea, and a fishbone model, which is (by its nature) event oriented.

‘Dart Board’ (or ‘Cake’ or ‘pie’) model

The idea of the ‘dart board’ or ‘cake’ model is based on the sections we call ‘slices’. To explain the concept, lets first start the explanation with a view on a kind of wedding cake:

A cake like this consists of different levels; our cake has (at least) three levels representing typical operational known from Enterprise IT governance models (such as ISMS, COBIT, PMI, etc) and one level (on top) for IAM specific areas.



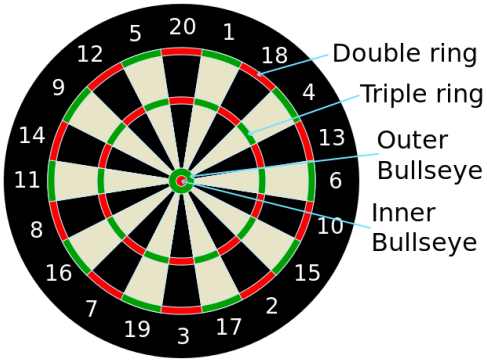
An idea for ‘terms’ to be used to reference the elements of the model:

- ‘Layer’ for the 4 parts of the cake
- ‘Sections’ for the toplevel areas (at least for the upper wafer)
- ‘Slices’ for the sublevels within the sections
- ? do we still need Information/technology/policy?

Now imaging you would like to have a piece from this cake. Most likely, you will not try to cut a piece just from the lowest layer: you will get a slice which ‘covers’ all the layers. But which slice you will have?

If we have a look on this cake from the top, will you have the slice on the right or from the left? And where is right or left?

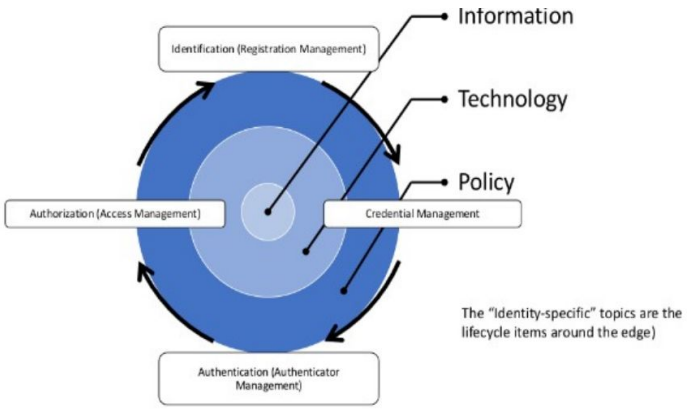
To further explain the concept, lets have a look on the top, from a birds perspective. A possible model for this could be clock, deviding it into slices representing the hours from 1-12. Another approach is to use a ‘dart-board’ analogy, which gives us a few additional sections we can use.



On a dart board, we have different slices representing specific scores (1-20). Those slices are intersectioned by ‘rings’ representing a multiplier for the score: a dart which ends up in the ‘triple ring’ gets a triple score, allowing you to get a score of 60 if you hit ‘triple 20’.

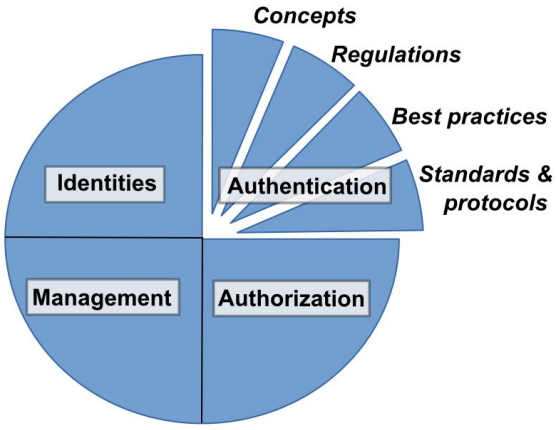
The rings on the dart board are representing additional layers in our model, but without the idea that a specific ring is more or less important (more or less score) than any other: they are just part of the slice you will investigate.

Back to our ‘birds’ perspective. Analogue to
the ‘rings’ on the dart board we introduced
rings on the top level of our cake. These rings
deal with the ‘information itself’, so any PII in the
very center, sorrounded by technology
and policies.



The rings themself belong to four different basic knowledge areas (sections), which we have identified as

- The concept of ‘identity’
- Authentication
- Authorization
- Management



Each of these sections can be further subdivided into topics (slices) related to

- Concepts
- Regulations
- Best Practices
- Standards and Protocols

	Concepts...	**Regulations...**	**Best Practices...**	**Standard and Protocols...**
Identities / Authentication / Authorization / Management	...that have evolved during time dealing with (digital) identities and their many facets. Concepts describes ideas, theories, procedures and common terms a ID-Professional should be aware of, even though the described concept might not be covered by regulations, best practices or standards.	...and laws which are to be taken into account when dealing with (digital) identities, either in general or within a given industry	… are methods or techniques within the given field which have gained wide acceptance to be applied in preference to other methods and techniques.The superiority of a ‘best practice’ is commonly measured based on better results (in quantity, quality or manageability). This also includes ‘de-facto’ standards.	...are norms, requirements and conventions. This can be described as a general principle to be followed (canon), as industry standard such as RFC and ISO or technically as communication protocol describing the interaction between two or more computer systems.

ID Professional Body of Knowledge

These tables contain the topics that an an ID Professional should know *something* about and eventually master. The depth of knowledge and experience will vary by individual and role.

The bulleted items in the tables are topic labels, not wordy descriptions of the topic itself. The detailed elaboration of each topic label will occur in a future revision.

Identities

The term or concept of ‘identity’, and what it means exactly is subject to discussion since the very beginning of science and scholarship, especially in philosophy. In much the same way, a single, reliable definition of the term is still debated extensively and internationally.

Much simplified, an identity can be seen as **one** subject which is **uniquely** identifiable, to a given level of certainty (or ‘assurance’) in a given set of **many** subjects. A ‘digital identity’ is a cybernated representation of this subject. This definition includes human and non-human subjects - although generally, the discipline of ‘Identity Management’ most often deals with human subjects, or at least subjects that are directly or indirectly related to human beings. This relation to a human being (a real person) is what makes ‚identity management‘ so special within information technology. Personal Identifiable Information (PII) is protected by several laws and regulations, they demand ethical behavior and they generally have a direct (or indirect) impact on our self.

The IDPro BoK Model‘s section on ‚Identities‘ should give an overview /collection which concepts, regulations, best practices and standards are to be taken into account when talking about ‚identities‘ in this context.

Identities	Examples (collection, not meant to be complete)
Concepts	● Identities and their digital representation ○ Identity Types in context ● Identity Relationship ○ Business (reports-to / reports-to-me) ○ Social (Foaf) ○ Asset Ownership ○ Customer (‘know-your-’) ○ Patient (medical) ● Entities (non-human identities) ● Ethics ● Aggregation and Verification, Levels of assurance, ● Uniqueness in Population (domain) (→ Management?) ● (Self)-Sovereign (authority)
Regulations	● EU-GDPR ● EU-eIDAS ● US-ESIGN
Best Practice	● Contextual Identity Management ○ Privileged Identity Management ○ Customer Identity Management ● Master Data Management ○ Relationship Hierarchies ○ Relationship Management ● Privacy Protection and consent management ○ Selective and minimal disclosure ○ Pseudonymity and anonymity ● Identity Proofing ○ Evidence requirements ○ Process requirements
Standards and Protocols	● ISO/IEC 24760 ● ITU-T X.1252 ● NIST 800-63-3

Authentication

The term ‘Authentication’ has many meanings and usage contexts for ID Professionals.

The Merriam-Webster dictionary definition is: “*Authentication (verb): to prove or serve to prove to be real, true, or genuine*”[1]. In the domain of ID Professionals, this definition can be used as a starting point.

Some of the contexts which ID Professionals will encounter Authentication include:

- **Document verification[2]:** checking that data is correct and valid by corroboration or source verification; checking that any document security features are intact; searching for duplicates. Often used in ID Proofing and Verification processes.
- **Credential authentication:** can include a) a form of document verification where the credential is a controlled document issued by an authority; or b) a form of user login where a credential and authenticator are used to prove that the credential is presented and controlled by the true owner.
- **Entity authentication:** synonym for ID Proofing and Verification OR a form of login using credentials and authenticators. This form deliberately avoids specification of human entities versus non-person entities.
- **Federated authentication:** entity authentication where the authentication verifier is remote or separate from the resource being requested and the verifier and relying system use the same standards for confidence in authentication. The authentication verifier communicates, or asserts, the result of the authentication to the system that is relying on the authentication decision.

These contexts and usages have similar operations: presentation of evidence, sometimes known as ‘authenticators’ to a verifier; verification of the evidence either as-presented or against a data repository; optional corroboration of data related to the evidence; decision; action resulting from decision.

In entity authentication systems for system access, credentials are created and issued to enrolled system users. Credentials for authentication conform to specifications of the authentication mechanism or technology for those credentials. The authenticators specified in an authentication system are presented to the authentication verifier such that the verifier is able to determine the nature of and characteristics of and perhaps the identity of the entity which aims to use the credential for authentication. For example, for username and password credentials, the authenticator is often a cryptographic hash of the password. The verifier can determine that the hash received matches that on record for the username, but cannot know if the human that originally controlled the username is still the same human.

Qualities of authentication systems should include security, reliability and usability qualities. Authentication systems are critical for identification of human and non-person entities to a degree of confidence. Identification is an early step in processes related to authorization policy evaluation, and control of information or system access.

---

[1] https://www.merriam-webster.com/dictionary/authenticate Accessed 2017-03-22

[2] Verification and validation are very similar in meaning and usage. Verification of information leans toward comparison of the presented information against a known authoritative source. Validation of information leans towards providing proof or corroboration to substantiate the information.

The ID Pro Taxonomy and Body of Knowledge includes concepts of authentication and widely-used authentication methods and techniques, depending on the context.

Regulations and standards are emerging for the public sector and regulated industries. Standards for the determination of relative authentication 'strength levels' are under development. Standards and guidance for evaluation of confidence in authentication exist and are being improved over time.

Authentication	Examples (collection, not meant to be complete)
Concepts	● What are the commonly-used frames of reference for the term 'Authentication'? ○ Document verification ○ Person fact verification ○ Recognition of a prior encounter ○ Identification (in different contexts) ○ Verification of authenticators bound or contained in Credentials ● What is the relationship of Authentication to Identification ● Authenticators (Credentials) ○ Categories and characteristics ○ Single- and multi-factor authenticators: objectives, threat mitigation ○ Verification mechanisms ○ Cryptographic mechanisms ○ Lifecycle management ○ Misuse and impersonation detection ○ Usability considerations ● Authentication Architectures ○ Federated authentication ○ Single sign-on ○ Challenge-response ● User interaction techniques ○ Forms-based ○ Image based ○ Operating system pop-up ○ Out of band techniques ● Impersonation ○ Authorized ○ Fraudulent
Regulations	● US Government MFA mandatory ● State-level regulation - some have these regulations ● US Health IT ● US Financial Services Industry ● EU-PSD2 (explicit authentication requirements) ● EU-GDPR (implicit authentication requirements) ● **TODO: find links and citations for regulations** ○ ****** We need to figure out what regulations are significant for ID Pros to know about ******
Best Practice	● Methods to choose appropriate authentication techniques ○ Risk evaluation considerations ○ Cost considerations ○ Usability ○ Manageability ○ Attack Resistance ○ Models of Authentication 'levels' ● 'Binding' of authenticators to entity records ○ Uniqueness within a population scope or 'namespace' ● Decision factors to determine if authentication is needed, and to what degree and what appropriate mechanisms ● Privacy matters ○ Correlation across multiple transactions ○ Decoupling of personal information to authentication events

Standards and Protocols	● OpenID Connect ● SAML ● WS-Federation? ● Shibboleth? ● PKI-based ● Kerberos ● FIDO Universal 2nd Factor, Universal Authentication Framework protocols ● Does OATH fit in here somewhere? ● IF-FF? (mainly historical, I grant you) ● RADIUS ● **TODO: List all of the other protocols related to Authentication**

Authorization

Authorization is one of the primary purposes of any identity management system.

The Merriam-Webster dictionary definition is: "*Authorize (verb): to […] permit by [...] some recognized or proper authority (such as custom, evidence, personal right, or regulating power)*"[3].

The processes of deciding whether some requested activity is allowed are the processes of authorization.

When discussed in the context of information systems, access control is preceded by an authorization decision process.

When discussed in the context of information exchange, authorization is often called 'consent'.

Authorization decisions use identification of the requesting and requested entities plus rules. Entity authentication is typically required to gain confidence in the entity identification.

Authorization	Examples (collection, not meant to be complete)
Concepts	● Relationship to Identification, Authentication, Access Control ● Access control models ○ RBAC, ABAC, PBAC, ID-BAC ○ ACL-based ○ Centralized, decentralized ● Prerequisites and Duties ○ Trust elevation (e.g. re-authentication, step-up authentication, claims gathering) - items done before access is granted ○ Duties - items that are requested to be performed after the fact
Regulations	●
Best Practice	● Authorization policy evaluation ○ Proofs of assertion (tokens, tickets, cookies, cryptographic methods) ■ Bearer methods v proof of possession methods ○ Access control policy, authorization policy, ○ Static evaluation, dynamic evaluation ○ Is there an 'authorization equation' for policy evaluation? e.g. Given an identified entity and a requested resource, select the correctly-scoped authorization policy, evaluate the policy, grant || deny || require trust elevation for the resource access, log the events ● Considerations for choosing specific models, protocols ○ Risk ○ Authorization model matching to credential characteristics, identification method, available authenticators ○ Centralized v decentralized

[3] https://www.merriam-webster.com/dictionary/authorize Accessed 2017-03-22

	○ Degree of independence of authorization policy decision v access control decision ○ Manageability - can I make changes that have predictable outcomes ○ Forensics - (e.g. answer questions like who had access to X on date?) ●
Standards and Protocols	● OAuth ● UMA ● Active Directory ● LDAP ? ● XACML ●

Management

Management	Examples (collection, not meant to be complete)
Concepts	● Identity Technologies ● Entitlement Dictionary ● Identity Governance ● Least Privilege ● JIT and other forms of Provisioning ● Identity Store and associated Identity data ● SoD and Toxic Combinations ● Termination and removal ● Identity Life Cycle ● Information Recording (-> moved from 'identities') ●
Regulations	● PHI / HIPAA ● PII ● PCI DSS ● GDPR
Best Practice	● Requirements Definition ○ Clearly define Joiners/Movers/Leavers Management ○ Establish clear ownership of all identity types ○ Establish policies for the lifecycle (Joiner/Movers/Leavers) ○ Establish policies and processes for non-human identities/accounts (e.g. Service Accounts) ○ Align with required regulations especially around entitlement revalidation periods ○ Define a Privileged Identity Policy and processes ○ Identifying authoritative identity sources ○ Password policy definition, lost password management and password reset ● Self Service ○ Establish processes for self registration and management ○ Storage of Consent ○ ● Certification and re-validation ● Program Buy-In - Management Support ● Auditing and Logging ● Reconciliation ● Establish Metrics - KPI, KRI's & KTI's ● Management of Physical components supporting identity information recording, assertion, integrity, verification ● Management of information related to identity records ● Management of linking identifiers (relationships) between information assets and/or physical assets
Standards and Protocols	● SCIM ● <add standards>

Management

Management at it's broadest sense defines how the life cycle of identity records, physical things and relationships are managed. For Identity Management we define this as the administrative tasks associated with the handling of Identities and their entitlements. It refers to the processes that ensure the maintenance

and fidelity of associated data of the identities and their relationship to entitlements within and of systems, applications and devices.

Management consists of initial tasks that include defining requirements, creating policies and implementing base technological systems to ensure alignment with business requirements and security needs.

Once base systems and processes are in place, maintenance tasks are carried out which include auditing, reconciliation, reporting and process improvement tasks. A core component of this maintenance is also the ongoing validation of the relationship between identities and their entitlements via access certifications.

Overall, Management seeks to set a clear set of engagement rules for the control of Identities and what they are entitled to.

Citations and Bibliography

[1] EU-GDPR
http://eur-lex.europa.eu/eli/reg/2016/679/oj
[2] EU-eIDAS
http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&from=EN
[3] US-ESIGN
https://www.law.cornell.edu/uscode/text/15/chapter-96
[4] ISO/IEC 24760-1
http://standards.iso.org/ittf/PubliclyAvailableStandards/c057914_ISO_IEC_24760-1_2011.zip
[5] NIST 800-63-3 (DRAFT)
https://www.nist.gov/itl/tig/special-publication-800-63-3
[6] Best Practices
https://en.wikipedia.org/wiki/Best_practice
[7] Canon
https://en.wikipedia.org/wiki/Canon_(basic_principle)
[8] Government of Canada: 'Directive on Identity management'
https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16577
[9] Web of Trust, Identity Crisis
https://github.com/WebOfTrustInfo/ID2020DesignWorkshop/blob/master/final-documents/identity-crisis.pdf
[10]
[11] Bla
[12] B
[13] Bla
[14] Bla
[15] Bla
[16] Bla
[17] Bla
[18] Bla
[19] BlaBla
[20] Bla
[21] Bla
[22] Bla
[23] Bla
[24] Bla

Additional Body of Knowledge Items

This section of the Body of Knowledge should contain topics that do not fit easily into the taxonomy.

Links and Language around Federal and State Laws & Regulations that Impact Identity Management for Students, Patients, Customers & Citizens

http://www.uniformlaws.org/Committee.aspx?title=Identity%20Management%20in%20Electronic%20Commerce

*The **Uniform Law Commission** provides states with non-partisan, well-conceived, and well drafted legislation that brings clarity and stability to critical areas of state statutory law.*

A ULC Study Committee on ID Management in Electronic Commerce was recently formed that "will study the need for and feasibility of uniform or model state legislation concerning identity management in electronic commerce"

---

http://www.secureidnews.com/news-item/company-to-pay-1-5-million-in-suit-filed-under-illinois-biometric-privacy-act/?tag=email
http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

Illinois state law requires that:
"No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:

1. *informs the subject … in writing that a biometric … is being collected or stored;*
2. *informs the subject … in writing of the specific purpose and length of term for which a biometric is being collected, stored, and used; and*
3. *receives a written release executed by the subject …"*

(c) Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.

---

http://www.americanbar.org/publications/blt/2016/05/08_claypoole.html

Privacy Laws Specifically Targeted to Biometric Information

A few states have enacted legislation specifically to regulate third parties' use and collection of individuals' biometric information. State laws concerning biometric information fall roughly into one of three categories: (1) laws with respect to the collection and use of biometric information belonging to students; (2) laws dealing with collection by government actors; and (3) laws targeting the collection and use of biometric information by businesses.

Student Biometric Information

California law prohibits operators of websites geared towards K-12 school purposes from selling students' biometric data and restricts their use. Delaware has a similar law. In North Carolina and West Virginia, student biometric data may not be kept in the student data systems.

Illinois law prohibits school districts from collecting biometric information from students without parental consent, and they must stop using such information when the student graduates, leaves the school district, or when the district received a written request from the student and all biometric information must be destroyed within 30 days of discontinued use. The school district may only use biometric information for

student identification or fraud prevention and may not sell or disclose to third parties without parental consent or pursuant to a court order. Arizona, Wisconsin, Louisiana, and Kansas have similar laws. Colorado law prohibits its Department of Education from collecting student biometric information unless required by state or federal law. A new Florida law enacted in 2014 goes even further than the foregoing state laws by prohibiting schools from collecting, obtaining, or retaining biometric information from students, their parents, or their siblings.

Government Actors Collecting Biometric Information

Missouri, Maine, and New Hampshire laws prevent state agencies from collecting, storing, or using individuals' biometric data in connection with ID cards or driver's licenses. Neither these laws nor any existing laws prohibit government actors from collecting or using biometric information in connection with law enforcement, immigration, border security, or national security.

Collection of Biometric Information by Businesses

The first state law to address business' collection of biometric data was the Illinois Biometric Information Privacy Act, 740 ILCS 14 et seq. (BIPA) in 2008, followed shortly thereafter by Texas's biometric law, contained in Section 503.001 of the Texas Business and Commercial Code, effective in 2009. BIPA sets forth a comprehensive set of rules for companies collecting biometric data and creates a private right of action for Illinois residents whose biometric data is collected or used in violation of BIPA's rules. Generally, BIPA is composed of five primary elements. BIPA: (1) requires informed consent prior to collection; (2) prohibits profiting from biometric data; (3) permits only a limited right to disclose; (4) mandates protection obligations and retention guidelines; and (5) creates a private right of action for individuals harmed by violators of BIPA.

The FTC and Biometrics

The FTC has thrown its hat into the ring as well, by issuing recommended best practices for companies using facial recognition technology, but the FTC has stopped short of creating rules or laws in this space. The FTC published "Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies" in October 2012 (the FTC Recommendations) to provide guidance to companies under its purview that currently or seek to incorporate facial recognition technology in their products or services.

The FTC first recommends that companies implement "privacy by design" by (i) maintaining reasonable data security protections for biometric information; (ii) establishing and maintaining appropriate retention and disposal practices for biometric information; and (iii) considering the sensitivity of biometric information when designing facial recognition technologies. In the FTC Recommendations, the FTC also suggests that companies employing facial recognition technologies should increase transparency of their methods and provide consumers with choices, such as the opportunity to opt out of collection of their biometric information. The FTC specifically advises social networking companies to give consumers a clear notice, apart from its privacy policies, that it collects faceprints, how the technology works, and how the company will use the data. The FTC also advises that social networking companies shall give consumers an easy way to opt out of collection and ability to turn off the facial recognition feature at any time and have the company delete the biometric data already collected.

Lastly, the FTC recommends that companies obtain subject's express consent before collecting or using faceprints in two situations: (i) before using an image or faceprint in a materially different way than the

company represented at the time of collection; and (ii) when using a faceprint to identify anonymous images of a subject to someone who could not otherwise identify the subject, such as in public places. The FTC Recommendations mirror BIPA's requirements, without going as far as to advise against disclosure to third parties.

Financial Institutions

Financial institutions must comply with the provisions of the Gramm-Leach Bliley Act (GLBA), enacted in 1999, addressing the privacy of personally identifiable financial and account data. The privacy requirements of GLBA, Title V apply to "financial institutions," which are essentially any business institutions significantly engaged in financial activities. GLBA's privacy rule applies to the collection of nonpublic personal information (NPI). GLBA's definition of NPI does not expressly list biometric information, but the expansive definition of NPI certainly includes biometric data. NPI is defined as personally identifiable financial information:

Educational Institutions

The Family Educational Rights and Privacy Act, 34 CFR Part 99 (FERPA) governs the disclosure of students' biometric information, to the extent that it is contained in student records. A student's biometric record is included in the definition of personally identifiable information, and is a type of information that may be included in students' education records. As such, FERPA prohibits schools from releasing students' biometric information without parental consent, to the extent that it is contained in students' education records, with some limited exceptions.

ISO/IEC Standards

<< Include the Terms and Definitions sections of each of the relevant published standards. We will then examine the lists to decide on which definitions should be 'covered' in the BoK. For each 'covered' term, we will have a 'concept' or other inclusion in the BoK. >>

Older content and discussion (moved, so we do not lose those important views….)

Section ‘Identities’ (primer)

The term or concept of ‘identity’, and what it means exactly is subject to discussion since the very beginning of science and scholarship, especially in philosophy. In much the same way, a single, reliable definition of the term is still debated extensively and internationally.

Much simplified, an identity can be seen as **one** subject which is **uniquely** identifiable, to a given level of certainty (or ‘assurance’) in a given set of **many** subjects.

A ‘digital identity’ is a cybernated representation of this subject. This definition includes human and non-human subjects - although generally, the discipline of ‘Identity Management’ most often deals with human subjects, or at least subjects that are directly or indirectly related to human beings.

-

