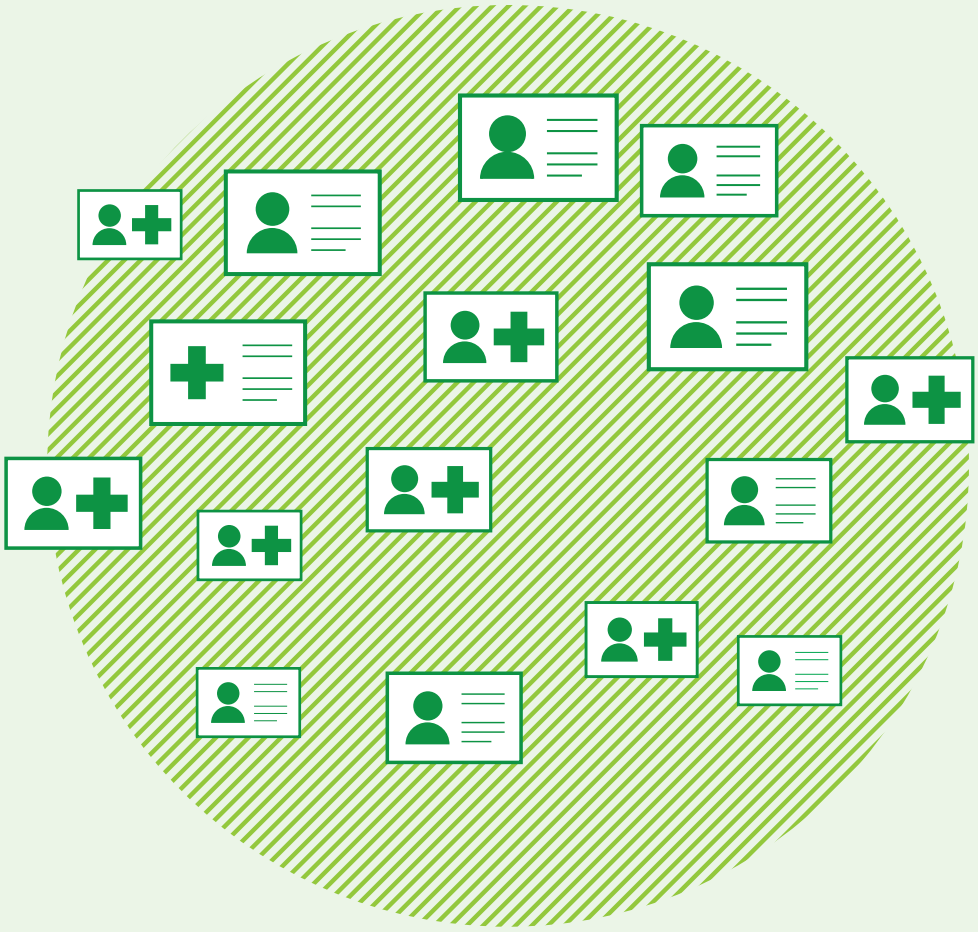
Digital Identity Ecosystems

By Pam Dixon



JANUARY 30, 2019

WORLD PRIVACY FORUM

WORLD **PRIVACY** FORUM

Digital Identity Ecosystems

Pam Dixon, Executive Director
30 January 2019

Identity is a data-rich key that acts to unlock all levels of the emerging digital ecosystem. All forms of ID carry some risk, but digital forms of ID, or "dematerialized ID," cuts across all sectors and generates particularly copious data about people, their behaviors, financial status, associates, and potentially even political and religious views. Over time, distinct patterns emerge from the data and have in the past created new kinds of risks for individuals and groups. As the world is becoming increasingly digitized, we can expect challenges in the identity space to grow apace unless proactive attention is given to identifying and mitigating the risks.

Balanced policy making that adheres to now well-established, internationally accepted standards for privacy and data protection is a crucial fundamental step to setting up core protections for digital identity ecosystems. When ID systems are created and allowed to operate without underlying data protection law and policy in place prior to implementation, case studies show that risks mount quickly — as does "mission creep" and other permutations that often have meaningful negative impacts for people and society.

Ensuring that broad legal and policy protections are in place prior to identity ecosystem implementations is essential. When these protections also include adequate enforcement mechanisms, ID sector stakeholders can then begin to create appropriate and responsive practical governance in their respective spheres. When such identity governance is crafted correctly by the core stakeholders in the identity ecosystem, it can tip the balance of ID ecosystems toward mutual benefit and trust as digital identity is used for the public good.

The Context for Modern Identity

Identity is woven into the modern digital environment in meaningfully different use cases. Identity ecosystems can be created and managed by governments, commercial sector companies, academic institutions, by individuals, and combinations thereof for many purposes. The technologies of identity are profuse, and range from stunningly large databases to blockchain technologies to biometrics and more. Perhaps one of the best-known traditional use cases for identity is that of a government-issued ID, which is then typically used for all manner of authentication, among other tasks. This and other other traditional identity use cases are not disappearing — but they are being transformed.

The emerging data world is one of rapid data transformation and data fusion, and it has changed and expanded how traditional identity operates. While government-issued identity credentials and ecosystems still exist, they are no longer the only important identity ecosystems. Multiple identity ecosystems have now emerged, with more still emerging, each employing different digital architectures and uses. These systems frequently overlap, and may vary in size from global in scope to micro-identity systems.[1]

Consider just a few ecosystems illustrating the range of modern digital identity structures. Large centralized national identity databases, where identity information is held in one central location, is a type of identity ecosystem. These types of identity ecosystems are most often operated by a government. These systems are often mandatory, and are usually associated with legislation crafted to guide the system's purpose and operations; in some jurisdictions, government identity systems are also governed within the context of broader privacy, data, and civil liberties protections. Many governments have identity authorities that are specifically focused on managing national identity ecosystems.

Compare a national centralized database structure with a blockchain-based identity system, where identity information is decentralized.[2] Information in this type of a system is decidedly held and controlled by the individual. Governments have begun experimenting with blockchain and identity ecosystems, particularly cities.[3] Thus far, though, comparatively little formal policy has been written around decentralized types of identity systems, particularly at a national level.

The technical architecture underlying the two types of systems sits at opposite ends of the spectrum. The policies and governance of the systems is just as different, with meaningful consequences for trust and adoption. Yet the two systems may operate simultaneously in any one jurisdiction, layered with other interconnecting identity ecosystems such as those that can be found in health care, educational, financial, and other settings. Add to this the distributed identity networks being contemplated and

---

[1] An identity microsystem is one in which an individual or small group of people are assigned unique identities in a digital ecosystem existing in a limited space. A biometric car cockpit with ADAS biometric driver monitoring enhancements is a good example of this. In some ADAS systems, the heartbeat becomes part of the identifying biometric. See Valeo, https://www.valeo.com/en/comfort-driving-assistance-systems/ and Valeo driver monitoring: https://www.valeo.com/en/driver-monitoring/.

[2] A blockchain is in its simplest definition a distributed database. For a good introduction to this topic, see Bernard Marr, Beginner's guide to Blockchain, Forbes, Jan. 24, 2017. https://www.forbes.com/sites/bernardmarr/2017/01/24/a-complete-beginners-guide-to-blockchain/#23930cb56e60.

[3] See the Dubai Blockchain Strategy, https://smartdubai.ae/initiatives/blockchain See also: Illinois Blockchain Initiative, https://illinoisblockchain.tech. The state of Washington has introduced broad legislation that would begin to provide some legal context for blockchain-based technologies. See: Washington State Legislature, SB 5638 - 2019-20, Recognizing the validity of distributed ledger technology, https://app.leg.wa.gov/billsummary?BillNumber=5638&Initiative=false&Year=2019.

piloted in smart cities.[4] On top of this add trans-national digital identity ecosystems. These can vary from borderless digital IDs issued from Estonia, to uses of identity via multinational social media platforms.[5] Individuals can and do have multiple valid identities when identity is dematerialized. The systems themselves are complex, and their interactions are growing more complex still.

Policies meant to address new challenges and risks in identity ecosystems require an approach that will address all aspects of the complex and rapidly evolving identity environments today. This is not an easy task, and a great deal of effort has gone into understanding what solutions might address how to "future proof" legislation and adapt it to rapid technological change.

It is our view that the most effective approach will be based on providing identity systems and their users with baseline data protection, privacy, and other protections via sturdy international consensus privacy principles (such as the existing Fair Information Practices, or FIPs model, or a variation of this model)[6] combined with, or layered with, equally sturdy and tested knowledge governance principles (such as those articulated by Nobel Laureate Elinor Ostrom, discussed more below.)

Baseline protections can provide the rules, enforcement procedures, and a legal context for the identity system, and governance can provide the specific management principles for individual identity ecosystems. The principles will, ideally, be able to assess, address, and mitigate risks inherent in the system, which will vary from system to system based on structure, intended identity uses, and other factors. Focused governance crafted specific to systems will allow for contextualization of the broader principles. This is an important aspect, as practical governance for a global identity platform will differ meaningfully from that for an identity microsystem. Both need contextualized practical codes of conduct.

Laws regarding identity ecosystems that do not include attention to data protection, privacy, and other concerns may simply mandate the creation of a system without providing a full context for fair and just use of that system. Where this has occurred, there are frequent problems. Joining FIPs (or other baseline privacy principles) with governance principles specific to identity concerns will allow for

---

[4] See discussions of identity data in smart cities: Yoti talks blockchain and digital government at World Economic Forum, Find Biometrics, Jan. 29, 2019. https://findbiometrics.com/yoti-world-economic-forum-501295/ See also: Nicole Lindsey, Smart cities begin to embrace digital rights for personal privacy and data protection, CPO Magazine, Dec. 18, 2018. https://www.cpomagazine.com/data-privacy/smart-cities-begin-to-embrace-digital-rights-for-personal-privacy-and-data-protection/ See also: Ava Kofman, …Sidewalk Labs plans to package and sell the location data of millions of cell phones, The Intercept, Jan. 28, 2019. https://theintercept.com/2019/01/28/google-alphabet-sidewalk-labs-replica-cellphone-data/.

[5] Estonia has created a borderless digital ID. See E-Estonia, e-identity and e-residency. https://e-estonia.com/solutions/e-identity/id-card/ "E-Residency is a transnational digital identity that anyone in the world can apply for to obtain access to a platform built on inclusion, legitimacy and transparency. E-residents then have access to the EU business environment and can use public e-services through their digital identity."

[6] Robert Gellman. *Fair Information Practices: A Basic History*. V. 2.18, April 10, 2017, https://bobgellman.com/rg-docs/rg-FIPshistory.pdf. See also: HEW Report: Records, Computers and the Rights of Citizens Report of the Secretary's Advisory Committee on Automated Personal Data Systems
July, 1973. Available at: https://www.justice.gov/opcl/docs/rec-com-rights.pdf.

many benefits, including ongoing risk assessment, evolution of practices, iterative benchmarking, and the development of mutual trust between stakeholders in the ecosystem.

This kind of overarching framework consisting of FIPs plus modern governance, correctly constructed, can create a system of identity governance that will allow for an approach to privacy, data, and identity that is collaborative, fair, and acknowledges the challenges of highly complex data environments where digital identity operates today. Risks associated with traditional and newer uses of identity will still exist, and will vary depending on the specific application and structure of the technology and policies of the identity system. It makes sense to adapt the frameworks we are using to iteratively solve new data-related problems as they attach to the creation and use of identity.

The Role of Trust in Identity Ecosystems

Trust is arguably the most important ingredient a good digital identity ecosystem must have to thrive. Bo Rothstein and others describe a lack of trust between parties (consumers, companies, other stakeholders) as the core basis of a detrimental social trap.[7] Trust in digital ecosystems overall is decreasing, which has overlaps with some digital identity concerns.[8] In the wake of multiple large data breaches, all relating in some way to the unauthorized release or use of identity and information keyed to identity, and in the ongoing response to data scandals such as Cambridge Analytica,[9] the importance of trust should be understood to be of central importance in identity systems.

---

[7] A social trap is a situation where cooperation between individuals, groups, organizations, multi-stakeholders, or societies has become impossible due to mutual lack of trust. See in particular Bo Rothstein. The Quality of Government: Corruption, Social Trust, and Inequality in International Perspective. University of Chicago Press, 2011. See Ch. 7 and discussion of social trust and the consequences of its loss: "…Since agents in a group that have lost trust in one another cannot easily mimic or fabricate the level of trust needed to ensure collaboration even if they all know they would benefit if they could (Ostrom 1998; Rothstein 2005)." See also: Bo Rothstein. Social Traps and the Problem of Trust, University of Cambridge Press, 2005. https://www.cambridge.org/core/books/social-traps-and-the-problem-of-trust/02225C0B-B48764F18F287FD6569EEF2E#fndtn-information See also: Bo Rothstein, *The Chinese Paradox of High Growth and Low Quality of Government: The Cadre Organization Meets Max Weber*. Governance: An International Journal of Policy, Administration, and Institutions, Vol. 28, No. 4, October 2015 (pp. 533–548). doi:10.1111/gove.12128.

[8] The US Census Bureau collected significant national consumer research regarding privacy and trust in July 2015. The results were given to the NTIA and form the basis of an extensive national survey and analyses published in 2016. NTIA, based on the survey results, found that a lack of consumer trust was negatively impacting economic activity. The NTIA noted: "Perhaps the most direct threat to maintaining consumer trust is negative personal experience. Nineteen percent of Internet-using households—representing nearly 19 million households—reported that they had been affected by an online security breach, identity theft, or similar malicious activity during the 12 months prior to the July 2015 survey." See: NTIA, *Lack of trust in Internet privacy and security may deter economic and other online activities*. May 13, 2016. Available at: https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.

[9] Multiple authors. *The Cambridge Analytica Files: A Year-Long Investigation into Facebook, data, and Influencing Elections in the Digital Age*. The Guardian. Available at: https://www.theguardian.com/news/series/cambridge-analytica-files.

WPF has long predicted that as people become more aware of data brokers,[10] and in particular, of expansive uses of individuals' retail, location-related, and financial transactional histories attached to digital identity, that this will create additional serious trust issues, which in turn can lead to a lack of cooperation, to everyone's detriment. Identity, in particular, is an ecosystem that is significantly impacted by trust.

Identity Case Studies

History is littered with examples of large and even national-level identity ecosystems which failed after end-user stakeholders lost trust in those systems and their controllers. This is particularly true in the government-issued ID sphere. The now disbanded UK National ID Card System is an exemplar of a system that experienced failure at a national level. The system, approximately 8 years in the planning, was launched and partially implemented, but was not trusted due to highly intrusive, non-voluntary measures many of those who were to be subject to the cards objected to. The system was disbanded just after its launch, at significant expense.[11]

India, which has provided the world's most significant case study on the implementation of nationwide biometric systems in voluntary and non-voluntary environments, provides important lessons. WPF researched the Aadhaar ecosystem extensively in the field, and wrote a large research report on the system.[12] Our research and policy analysis was cited twice in the Supreme Court of India's landmark Aadhaar case, in 2018.[13]

India went from adding its first voluntary enrollee in its Aadhaar biometric ID program in 2010, to boasting more than 1 billion enrollees in 2016. In order to allow for innovation, growth, and modernization, privacy and data protection regulations were eschewed in favor of technological advancement

---

[10] The state of Vermont, the first to pass data broker legislation, defines data brokers in its 2018 statute as: "a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship." See: H.764, An act relating to data brokers and consumer protection. https://legislature.vermont.gov/bill/status/2018/H.764.

[11] For background, see: Alan Travis. *ID cards scheme to be scrapped within 100 days*. The Guardian, 27 May, 2010. Available at: https://www.theguardian.com/politics/2010/may/27/theresa-may-scrapping-id-cards . The £ 4.5 billion UK system, which was envisioned to encompass an ID register, biometric passports, and a mandatory ID, was scrapped after 15,000 ID cards were already issued. Legislation was passed abolishing the system in 2010; The Identity Documents Act 2010 repealed the Identity Cards Act 2006. See Identity Documents Act 2010. Parliament, UK. Available at: https://services.parliament.uk/bills/2010-11/identitydocuments.html.

[12] Pam Dixon, A Failure to Do No Harm: India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S. Springer Nature, Health Technology. DOI 10.1007/s12553-017-0202-6. http://rdcu.be/tsWv. Open Access via Harvard- Based Technology Science: https://techscience.org/a/2017082901/.

[13] Aadhaar case: Supreme Court of India, Justice K.S. Puttaswamy (Retd.) and another v. Union of India and others. Writ Petition (Civil) No. 494 of 2012. Decided Sept. 26, 2018. Available at: http://www.worldprivacyforum.org/wp-content/uploads/2018/09/Supreme-Court-Aadhaar-Judgment-26-Sep-2018.pdf.

and modernization of the governmental, financial, health and other sectors. The Aadhaar digital identity ecosystem was intended to act as an identity key for the poor and to allow for unfettered, frictionless delivery of subsidies. The vision was well-meaning, but the system suffered from multiple challenges, including security breaches, that caused the entire system to be brought into question. Ultimately, the system was sharply curtailed by the 2018 Aadhaar Supreme Court of India decision.

One notable challenge the system experienced was significant mission creep, which caused a lack of user trust in the system over time. Instead of just being used for delivery of subsidies, it became increasingly difficult to get paid, receive pensions, file taxes, bank, or get health services in India without an Aadhaar ID. As the Aadhaar become used more widely, Aadhaar also went from being a voluntary system to a mandatory system. Three factors: the lack of stakeholder input, mission creep, and eventually a loss of user trust in the system, are what truly caused the curtailment of Aadhaar.[14] The lack of policy and governance allowed these problems to persist without being addressed.

Currently, Kenya's national identity system is showing early warning signs of a system exemplifying what we now know are very poor identity and data practices. Kenya's government has added amendments to existing identity legislation enabling the collection of DNA from its citizens and foreign residents.[15] The DNA is planned to be put in a centralized national database, and used by the government for multiple purposes. No collection has occurred yet, but already, unrest and deep concern over the potential for serious abuse of a centralized DNA database has arisen.[16]

A key difficulty is that Kenya has passed legislation allowing the DNA collection, but it has not yet passed overarching data protection legislation that would protect individuals from abuse of the identity data, or provide avenues for redress if harm has occurred. The stage is set for significant harm to develop in respect to Kenya's identity ecosystem. Unless the government of Kenya enacts significant baseline legislative and policy protections incorporating protections in place *prior* to the collection,

---

[14] There were additional issues related to technical limitations of biometrics, which are well-studied and documented. These technical limitations created harms that the implementers did not anticipate. Across India, government reports faithfully noted extraordinary and mass "failures to authenticate." That is, individuals with Aadhaar IDs could not use their biometric IDs to authenticate themselves. The authentication problems stemmed from failures within the biometric system itself. At scale, statistically low rates of multi-factor or multi-modal biometrics systems can become millions of people who could not get food. In India, there were reports of people dying because of failures to authenticate. Dhananjay Mahapatra, Don't let poor suffer due to lack of infrastructure for authentication of Aadhaar, Times of India, April 24, 2018. https://timesofindia.indiatimes.com/india/dont-let-poor- suffer-due-to-lack-of-aadhaar-tech-sc/articleshow/62842733.cms.

[15] Kenya's Registration of Persons Act doesn't specifically mention DNA but has an open list for the data available for collection. In January 2019, President Uhuru Kenyatta signed new amendments into law that changed the requirements for new applicants for National ID cards. See: New ID requirements after Uhuru amends law, January 21, 2019. Pulse Live, https://www.pulselive.co.ke/news/new-id-requirements-after-president-uhuru-kenyatta-amends-the-registration-of-persons/ze50lth.

[16] Editorial, Address concerns over taking DNA samples from Kenyans, Standard Media, Jan. 29, 2019. https://www.standardmedia.co.ke/article/2001311128/address-concerns-over-taking-dna-samples-from-kenyans.

creation, or use of a central DNA registry, then the system is likely to cause potentially profound harms.

Aadhaar has already shown us where the end stages of centralized biometric identity database deployments are, what they look like, and how they operate. The lessons are already there, including the loss of trust the Aadhaar system experienced and the harm some Aadhaar enrollees experienced. There is no reason to repeat these kinds of mistakes in Kenya.

Solutions

Much has been learned in the last 25 years about data protection and digital identity ecosystems. Data protection laws that have already been enacted in 89 countries have significant similarities, even when aspects of the law have been adapted to unique county-level conditions.[17] This is well understood and documented at this point. However, baseline digital ecosystem *governance* principles are generally not as well-understood or known outside of certain contexts where they are often found in use, such as environmental, production, and law enforcement contexts.

We discuss governance in some detail here, as it is a key component of managing digital identity ecosystems, and one that is far too frequently overlooked. Overarching principles are necessary, but by themselves are not enough to create good results in the long term. There must also be structures facilitating the creation of specific governance, or codes of practice, and the enforcement of that governance.

Nobel Laureate and economist Elinor Ostrom spent her entire career observing and analyzing governance of complex ecosystems, particularly the commons, or shared resources. Over the span of decades, she observed and distilled the most effective ways of managing complex ecosystems where stakeholders share resources ("common pool" resources). Identity — particularly digital identity — is one such common pool resource. The issue of who owns identity is particularly contentious, and we will not delve into that topic here. Suffice it to note that there is much disagreement about who owns identity. Each stakeholder — individuals, governments, corporations, and so forth, have a different answer.

In complex digital ecosystems, strict top-down ownership is a difficult position to uphold, as is demand for full individual control of data. However, mutually agreed governance of resources that are shared can work, and has proven to work. If we think of data — and identity data — as a shared resource, one in which multiple stakeholders have involvement with and an interest in, then we have a pathway to govern those systems as shared resource systems. It is in this context that Elinor Ostrom's work is of central importance.

---

[17] See Greenleaf, Graham, Global Data Privacy Laws: 89 Countries, and Accelerating (February 6, 2012, updated 2017). Privacy Laws & Business International Report, Issue 115, Special Supplement, February 2012; Queen Mary School of Law Legal Studies Research Paper No. 98/2012. Available at SSRN: https://ssrn.com/abstract=2000034.

Ostrom set forth 8 principles for governance of complex systems using shared resources. As mentioned earlier, the Ostrom governance principles were originally derived from observations in complex environmental and other ecosystems. They can also be applied in complex data and identity ecosystems where frameworks such as FIPs provide baseline principles to apply and implement. Just as privacy impact assessments (PIAs) originated from environmental impact assessments,[18] the Ostrom principles that have worked to govern complex environmental and other ecosystems can also work to create desired outcomes in complex digital identity ecosystems.

The Ostrom general principles are as follows:

1. Rules are devised and managed by resource users.
2. Compliance with rules is easy to monitor.
3. Rules are enforceable.
4. Sanctions are graduated.
5. Adjudication is available at low cost.
6. Monitors and other officials are accountable to users.
7. Institutions to regulate a given common-pool resource may need to be devised at multiple levels.
8. Procedures exist for revising rules."[19]

This governance structure is what facilitates the creation of further, practical guidance implementing baseline data protection and other protective principles, which are often broadly worded. Governance needs to be particular, iterative, and continually updated. "Living" governance is the key.[20] Governance also facilitates identification and mitigation of identity ecosystem risks, which can then assessed continually in a ongoing benchmarking of established rules against reality. Adjustment of daily practices then are based on actual, provable, repeatable feedback.

Governance, to be effective for all stakeholders, needs to be collaborative and not dominated by certain participants in identity ecosystems. In the past, the creation of specific standards of privacy or other conduct for specific slices of the ecosystem, such as online advertising, has been an area of considerable difficulty. WPF has written about and documented the difficulty in a report about the chal-

---

[18]Bamberger, Kenneth A. and Mulligan, Deirdre K., *PIA Requirements and Privacy Decision-Making in US Government Agencies.* July 22, 2012. D. Wright, P. DeHert (eds.), Privacy Impact Assessment (2012); UC Berkeley Public Law Research Paper No. 2222322. Available at: https://ssrn.com/abstract=2222322 ***See also***: Roger Clarke, *A History of Privacy Impact Assessments*. Available at: http://www.rogerclarke.com/DV/PIAHist.htmlRoger Clarke. ***See also***: Roger Clarke, *Privacy Impact Assessment: Its origins and development*. Computer Law & Security Review, Vol. 25, Issue 2. 2009. https://doi.org/10.1016/j.clsr.2009.02.002.

[19] Nives Dolšak, Elinor Ostrom & Bonnie J. Mccay, The Commons in the New Millenium. MIT Press: 2003. See esp. Chapter 1, The Challenges of the Commons, New and Old Challenges to Governing Common Pool Resources.

[20] NIST's Facial Recognition Vendor Tests are an excellent example of the application of the idea of iterative work. In the past, NIST's tests were periodically conducted. Now, they are ongoing via what NIST calls "living documents." NIST FRVT 1:N 2018 Evaluation. https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-1n-2018-evaluation.

lenges and failures of privacy self-regulation.[21] What we envision here is not the self-regulation of old; it is a different system that has appropriate checks and balances and is based on mutuality, as defined first in the HEW report and then expanded upon by Ostrom's work and made practical by, for example, the *ANSI Essential Requirements*.[22] Creating a replicable, cooperative way to understand and create the conditions for social trust also plays a role in solving todays's digital identity challenges.

For this to happen, formal rules for creating multi-stakeholder principles will need to be employed. Thoughtful, tested rules such as those in the *ANSI Essential Requirements*[23] will be crucially important, as they provide due process in the creation of contextual guidance, allowing all system stakeholders an appropriate voice. There needs to be a give and take with common pool resources. This can happen where treatment is fair, and outcomes are unbiased and checked for risks. The decision making should occur at the beginning and throughout the process, beginning with setting rules and moving through to the end points of application and feedback on how the rules are working.

It is essential to avoid and prevent social traps in identity ecosystems, such as the development or worsening of a lack of trust between identity stakeholders. The lack of trust or a basis upon which to build trust is a very significant problem that needs to be addressed early in an ecosystem's life cycle. Governance will help, but only if it is based on mutuality, not command and control structures where end users do not have a seat at the table and where some actors are allowed unfettered dominance.

In a national digital ID ecosystem setting, if a broad principles-based legislative framework providing meaningful protections for an identity ecosystem were in place, and were then implemented with tools including a governance framework based on mutuality, such as Ostrom's, the government would have an important role in ensuring that the governance aspect of the system was appropriate, fair, and mutual. After the conditions are in place, then trust and the capacity for creating a dialogue can be fostered and built.[24]

Practical Application: Biometrics

---

[21] Robert Gellman and Pam Dixon. *Many Failures: A brief history of privacy self-regulation.* World Privacy Forum, 2011. Available at: https://www.worldprivacyforum.org/2011/10/report-many-failures-introduction-and-summary/.

[22] American National Standards Institute. *ANSI Essential Requirements: Due process requirements for American National Standards*. Edition: Jan. 2018. https://share.ansi.org/Shared%20Documents/Standards%20Activities/American%20National%20Standards/Procedures%2C%20Guides%2C%20and%20Forms/ANSI-Essential-Requirements-2018.pdf. The ANSI standards require openness, lack of dominance, balance, coordination and harmonization, notification of standards development, consideration of views and objections, consensus vote, appeals, and written procedures. There are also benchmarking procedures and compliance procedures with the rules.

[23] Supra note 22.

[24] See Bo Rothstein. Social Traps and the Problem of Trust. Cambridge University Press, 2005. See in particular Chapters 8 and 9.

Biometrics has become a popular topic of debate in digital identity. In the US, as well as in other jurisdictions, there is a great deal of interest in creating some form of individual control over biometrics use. In the US, at least one state, Illinois, has a state-level law mandating consent prior to biometrics collection in the commercial sector.[25] A handful of states in the US have laws governing how schools handle student biometric collection, and some additional biometric use statutes exist. As concern about biometrics has grown, a spectrum of groups have proposed general principles for biometric deployment and use, and some companies have proposed ideas and called for legislation.

Currently, the biometric debate often reflects narrow bands of a few selected stakeholders, resulting overall in competing ideas that meaningfully diverge. Some proposed principles that have been circulating are crafted with corporate goals in mind, some principles have been crafted with privacy goals in mind from a consumer point of view. However, none of the broad biometric and identity ecosystem principles have been created with meaningful stakeholder input that would meet, for example, the due process requirements set forth in the *ANSI Essential Requirements*. (Non-technical principles.)

With the existing lack of mutual trust in biometrics combined with the lack of a well-managed and fair dialogue between all stakeholders, it will be very difficult to reach agreement on principles, craft a legislative approach, or craft specific governance principles that are responsive to the full range of stakeholders. A substantive process that facilitates fair dialogue and outcomes on the issue of digital identity and biometrics would be a helpful step in negotiating across the differing views of multiple stakeholders and finding areas of agreement. Otherwise, dominant participants are likely to determine key aspects of the outcome. Non-dominant stakeholders - including companies in a second-tier position, individuals, municipalities, and many other stakeholders may have a loss of trust in the overall identity system involved due to a lack of agency.

Key lessons may be drawn here. Identity ecosystems that utilize biometrics require great care in planning. If the systems rise to a level of public importance or widespread use or implementation, formal policy controls in the form of legislation must be in place well prior to installation. After legislation is in place — which ensures FIPs or something similar are applied, as well as key rights — then a fair and iterative governance process will be needed to assess and address risks, and the changing roles, responsibilities and duties of stakeholders, as well as other tasks. Legislation alone cannot accomplish day-to-day governance, which is where all of the practices live.

Consider the specific issue of consent. In biometrics, it can become extremely difficult to get consent in every instance. Stakeholders disagree about the need for consent. But what will this mean in practice? Do we accept lesser freedoms, or do we impose stricter privacy controls? Is there another pathway? A formal standards - principles setting process such as articulated by the WTO procedures or the ANSI Essential Requirements — or another system for ensuring a fair hearing for all stakeholders, would facilitate all stakeholders to work toward building trust and crafting *mutually acceptable* rules.

---

[25] Biometric Information Privacy Act (760 ILCS 14/) Available at: http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

This would not be easy. But it is necessary if we want to achieve long-term benefits from technology while minimizing and mitigating risks of its use over time.

Conclusion

The World Privacy Forum has frequently said that ID systems must do no harm, and must create a public good. This is not just a theoretical goal or statement; it is a genuine, achievable goal that is imperative for all of us to work toward as we enter a much more complex digital environment with dematerialized identity ecosystems. In the end, history has shown us that identity systems — whether national in scope or micro-systems, rely on mutual trust. And mutual trust is present when there are clear legal protections and ideally some form of systemic practical governance in place.

Most privacy experts can agree that there are gaps in privacy protections today that matter in peoples' lives. What people disagree on is how to close the gaps. Whether individuals disagree about installing a pure FIPs program or a modification thereof, whether individuals disagree about aspects of baseline digital identity principles and many other areas of disagreement, the one thing we can potentially find some agreement on is that moving forward, we will need to find a way to work with data resources in a way that is cooperative, that allows for win-win solutions that appropriately empower all stakeholders, that address and mitigate risks on an ongoing basis, and that at the end of the day, intentionally avoid causing harm and create a public good.