Good ID: What’s trust got to do with it?

Bangkok Workshop Report

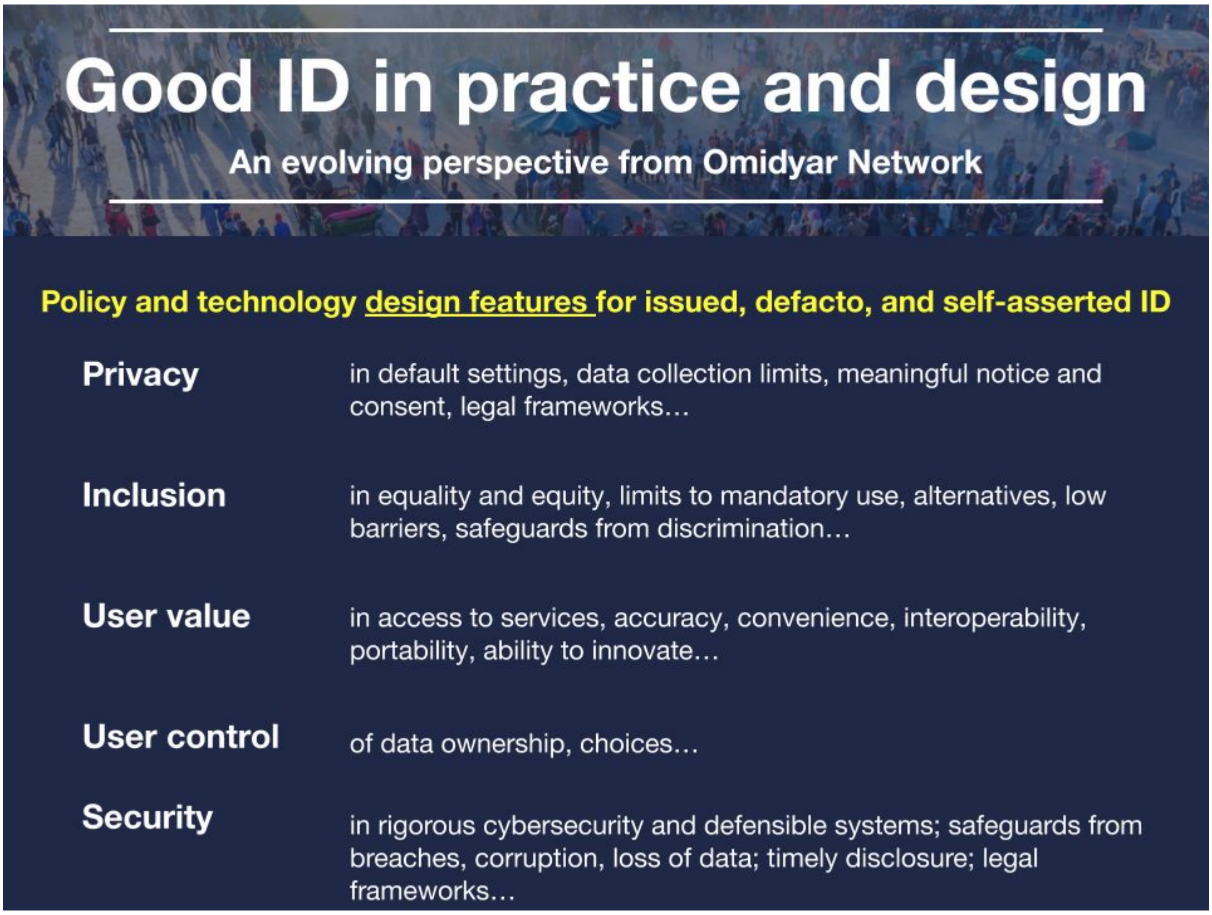
The Good ID workshops are a series of three workshops focused on good policy, good technology, and good practice to inform digital identity conversations and decisions. The #GoodID movement is a constructive debate led by Omidyar Network for the development of new, future-facing ID norms, intended to strengthen standards and tools to build better identification systems that work for everyone. Caribou Digital co-organized the three workshops with facilitation by Future Agenda’s Robin Pharoah.

This is a summary report of the final workshop held in Bangkok on July 2, 2019, and hosted by Mrs. Vunnaporn Devahastin, Deputy Permanent Secretary of Thailand’s Ministry of Digital Economy and Society (MDES), and by the Thailand National Broadcast and Telecommunications Commission (NBTC)[1]. The workshop was held under Chatham House Rule and follows the flow of the day (see Annex 3 for the workshop agenda). This workshop focused on Good ID in practice and explored trust-building behaviors involved in advancing

[1] The first workshop, held at Harvard University’s Shorenstein Center on February 5, 2019, explored the role of policy for Good ID (workshop report is here). The second workshop, held in Nairobi, Kenya, on May 25, 2019, focused on technologies and Good ID (workshop report is here).

digital ID systems that uphold transparency, accountability, public engagement, individual privacy, inclusion, user value and control, and security.

To begin the discussion in Bangkok, following Mrs. Devahastin's opening remarks, Abiah Weaver introduced Omidyar Network's evolving normative point of view on Good ID as distinguished by five policy and technology design features: (1) *inclusive*, (2) *offers user-value*, and embedded with (3) *privacy*, (4) *security*, and (5) *user control* and supported by trust-building practices including transparency and accountability.



Good ID in practice and design

An evolving perspective from Omidyar Network

Policy and technology design features for issued, defacto, and self-asserted ID

Privacy in default settings, data collection limits, meaningful notice and consent, legal frameworks…

Inclusion in equality and equity, limits to mandatory use, alternatives, low barriers, safeguards from discrimination…

User value in access to services, accuracy, convenience, interoperability, portability, ability to innovate…

User control of data ownership, choices…

Security in rigorous cybersecurity and defensible systems; safeguards from breaches, corruption, loss of data; timely disclosure; legal frameworks…

In response to this prompt—and in the spirit of Hemingway's six-word novel—each participant wrote their own definition of what Good ID would look like in Thailand, in ten words or less. Examples include:

"Good ID aims to identify individuals and connect the world."
"You know me well, work with me."
"Only minimum data required to identify."
"Contextual, configurable, controllable."
"Respect my privacy, make it secure."
"You know, I control my ID."
"Good ID is bad without proper consent."
"My ID, my life, my personality."
"Include me, don't discriminate against me, forget me."
"Good ID is basic human rights."
"Good ID is useful, private and compartmentalized."

One participant emphasized the *"trade off one has to make when designing a secure system*." "Privacy" was seen as a category of "security." In the process of coming up with their definitions, some participants discussed systems that would be useful (i.e., *"serve people and make resources accessible"*) while respecting human rights, ensuring *"private control,"* and being *"compartmentalized"* — that is, control over data points before they are shared with others.

On the whole, workshop participants indicated that Good ID should ensure user value and agency, safeguard user privacy, support portability, be consultative and accountable, and reflect the complexity of human identity. See Annex 1 for a full list of participants' ten-word definitions.

Taking action for #GoodID

Digital ID is a particularly relevant topic in Thailand because the Thai government is in the process of launching the new National Digital Identification (NDID) system. Workshop participants included several stakeholders involved in the NDID design — including government representatives, technology companies, and regulators — as well as interested parties such as entrepreneurs, academics, and civil society representatives. Because of the diversity of participants, the workshop's discussions were meaningful and conducted with a sense that outcomes could directly influence Thailand's digital future.

At the end of the workshop participants made individual commitments to *"ensure that Thai ID will be Good ID."* Each participant, translating the day's discussions into practice, reflected on their own roles in order to identify the actions they could take to accelerate the Good ID movement across Thailand.

The inclusion of digital ID designers and implementers in the workshop meant that many of the participants' commitments were concretely practical. In the words of one participant: *"we will provide technology to implement the Good ID whatever shape or form it may take."* While another participant said, *"I will take transparency logic and apply it in design and definitely I will design the opt-out option."*

Others committed to increasing (1) awareness and accountability of digital and Good ID and (2) the inclusion of vulnerable groups. As one participant said, *"we take action today by opening a public forum to get Thai audiences to understand the issues and to participate in policy-making processes."* And another pledged, *"to think more about ways that we can build in social value for disadvantaged groups so that it becomes something that people want to pursue and opt into."*

See Annex 2 for a full list of participants' pledges to the group.

Mapping Digital ID systems in Thailand

After generating their ten-word definitions, participants listed the identification systems, digital and otherwise, that they knew of in Thailand, before exploring the practices required to build Good ID. This list of identification systems is not exhaustive, as the large number of identification systems in Thailand soon became clear during the conversation. Participants grouped credentials into three categories. The first category, *Issued ID* describes an “ID that is issued to you by a government, a business, or another institution” (e.g., a driver's license, birth certificate, or birth registration). The second, *Defacto ID,* is “the digital identity that is built about us based on the data trail we leave, our data shadow… all the things that can be deduced about us… put together to create an identity.” The third category, *Self-asserted ID,* is “any kind of ID which you create and over which you have control” (e.g., a social media identity or persona).

Issued ID	Defacto ID	Self-asserted ID
Personal ID	Credit card	Grab/Uber
Passport	Mobile phone number	Facebook
Driver’s license	Travelling cards	Google ID and other social media
Corporate identity	e-wallet/cash card	“sharing economy”applications (Airbnb, Agoda, Booking.com)
Hospital number	eBay, Amazon, and other shopping apps	Digital Footprint
Student ID	Bitcoin address	Social Media
Thai ID card	membership cards/ points for all services	Disability Card/Medical Condition Card
Birth certificate	biometrics (fingerprint/face)	Transport Cards
Marriage certificate	condo/hotel/parking key cards	Email Address
Death certificate	Prompt Pay	
Digital work permit		
Pink card for foreigners		

In discussing the different credentials and forms of identification, participants debated to which category each belonged.[2] This debate demonstrates that these categories can be porous: for example many self-asserted identifications, such as Grab and Facebook, could also be classified as defacto. Indeed, some groups classified particular IDs as between categories. For example, there was a debate about how to categorize phone numbers because they are "*issued by the telecommunications industry*" but some people "*use such numbers as defacto IDs.*" It was also noted that in Thailand phone numbers *"are used to send money," "record who called us,"* and access services like Grab Taxi. Further, although Grab uses phone numbers to identify their clients, it is not responsible for issuing the ID and therefore *"cannot be confident that the ID is real."* The group noted that *"the phone number can be a strong ID in one context, but a weaker ID in another."* This drove home the idea that the classification of IDs among the three categories depends on context.

Practices for Good ID systems in Thailand

Good ID in practice means choices and decisions made in the design, delivery, and management of identity systems, and the extent to which they uphold the characteristics of Good ID. Participants were first introduced to two case studies, one of a state-issued identification system and the other of a commercially developed, defacto identification system. Drawing on these case studies to further discuss the IDs mentioned earlier, participants reflected on each identification system's purpose — asking "Who does it serve?" and "Who is it for?".

Case Study 1: State-Issued ID

Issued IDs include both public and private sector identification systems, but participants focused mainly on state-issued IDs. The first speaker described three trust building challenges and practices around India's Aadhaar scheme: how to design for trust in procurement, the use (or non-use) of biometrics, and data storage models.

First, the presenter described how large-scale identity and registration databases often involve a chain of contractors and subcontractors (*"layers and layers of outsourcing"*) which can make them both (a) prone to errors and leaks and (b) difficult to hold accountable for delivery failures. To strengthen the identification systems, the participants concluded that the Thai national government should hold these actors *"accountable, liable, and culpable"* and that, *"if this is not clear in your ID system, then you are not building for trust."* Aadhaar's reliance on biometrics is an ongoing challenge, as the speaker suggested many users found them *"remote," "covert,"* and *"non-consensual."*[3] Addressing the issue of biometrics, it was suggested that a Good ID is one that can be *"disposed of"* if the ID holder does not want to

[2] An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a card or token possessed and controlled by a cardholder or subscriber (NIST SP 800-79-2, p. 45, under Credential).

[3] Aadhaar is 12-digit unique identification (UID) number granted to all the residents of India. The number is linked to the resident's basic demographic and biometric information such as a photograph, ten fingerprints, and two iris scans, which are stored in a centralized database.
http://timesofindia.indiatimes.com/articleshow/6680601.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

be identified: *“a Good ID can be flushed down the toilet”* but *“you cannot do that with the Indian ID as your body is the ID card.”* Additionally, Aadhaar’s centralized data storage was considered an obstacle to data security in contrast to decentralized and local storage and processing. This was illustrated by reference to what Apple does with iPhone facial recognition, which was felt to be stronger than the centralized *“single point of failure”* characteristic of many national ID systems. Centralization requires accountability, such as through a *“constant audit system”* that employs *“a random, mechanized system”* and *“audit firms.”* Finally, reflecting on how credential models can enable mutual accountability, the presenter described how private key-based cartography could support a *“double cartographic signature.”* This record of both citizen and state interactions could help ensure that *“the state is also transparent to the citizen” — “this is why private key-based cartography or 'smart-card' based cartography is a very good design option.”*

Case Study 2: Defacto ID

The second case study looked at Grab Taxi, a taxi app that developed *defacto* identification through the use of mobile phone numbers, location data, purchase histories, and other personal identifiers. This study addressed the importance of digital ID for reliable payments, the challenge of credential portability (for drivers), and the implications of services changes for credential management. The discussion was oriented around ways Grab might design for Good ID as the company’s products evolve and its services expand beyond taxis.

Firstly, the presenter outlined how digital ID is vital for the reliable payments infrastructure that supports Grab and illustrated the practices through which a defacto identification service was developed: When the service launched, drivers had to visit the company’s offices to be paid in cash because there was no way to verify their identity. The company later developed and adopted an app using information (such as telephone numbers and an “info trail” that includes where the drivers live) to address this challenge.According to the speaker, KYC/AML requirements *“mean mobile numbers and financial services can enable robust identification.”*

A further challenge revolves around practices related to credential portability. One participant noted that “the driver’s reputation” (or consumer’s reputation) is *“one of the biggest defacto IDs… and is locked into the platform.”* Participants raised as a challenge to the taxi app, and whether they had plans to change its system or policy to allow the driver to *“‘take their reputations with them when migrating to another network.”* This was considered a challenge of **data portability**. Finally, there was discussion around the challenges presented by the evolution of the service. The group asked how personally identifying information would be managed as the company evolves from a simple taxi app into “a super app.” In other words, as the company goes from a *specialized* transport provider to an *overarching* service provider, how will the customer’s data be treated? Is the customer data for each service going to be “compartmentalized” and stored differently, with the data set looked at “separately”?

Exploring Good ID practices

Understanding the purpose of identification systems is critical to defining practices that shape Good ID. At a general level, the purpose of state-issued identification systems is categorized by the World Bank as foundational or functional.[4] The World Bank defines foundational identification systems as systems *“created for general public administration and identification...and may serve as the basis for a wide variety of public and private transactions, services, and derivative identity credentials.”* Similarly, the World Bank defines functional identification systems as systems *“created in response to a demand for a particular service or transaction” that “may be commonly accepted for broader identification purposes, but may not always bestow legal identity.”* Clarity around purpose is key to appropriate design and practices that can help achieve Good ID.

Participants selected one of the forms of IDs they had discussed earlier and reflected on questions related to “purpose” — specifically “Who does it serve?” and “Who is it for?”. For example, one table discussed the opportunistic as well as intended uses of driver’s licenses. The purpose for the individuals was discussed in terms of *“getting jobs,” “earning their living,’”* as well as their intended use for *“identifying their competence”* (i.e., “what category of vehicle they can drive”). For businesses, the purpose was described in terms of *“enabling new business, e.g., car rentals.”* As for government, the issuance of driver’s licenses was seen as connected to transport safety issues.

There was a lively debate around the use of the **mobile phone number as a credential** in part because one group included representatives from both mobile operators and the Thai regulatory agency. One participant with knowledge of the telecoms industry was convinced that the user benefits from the system while representatives of the regulator spoke of the many complaints they received from mobile users regarding, for example, unwanted spam and commercial offers. Thailand’s transition from a SIM to a biometric mobile ID was regarded as a cause for concern. The participants noted the potential *“tensions between different stakeholders*.” In their opinion, the mobile operators may see benefits to the users in terms of “convenience” and “efficiency” but some users may find the biometric technology invasive and lose trust in the system.

For the group looking at the Thai **national health ID,** it was less clear **“***how trust is created.”* The National Health Security ID, issued by the National Health Security Office (NHSO), was seen as facing significant trust challenges. While the information in this ID is linked to the existing Thai National ID, there are loopholes in that linkage. Although an important step had been taken to address the public's lack of trust in the system arising from the loopholes — in the form of a board with oversight functions and a complaint mechanism — participants felt that the system to address complaints lacked transparency and accountability.

Trust in the transaction patterns of mobile users as the basis for **defacto ID** relied on individual consent, customer rights and security, transparency, and good governance of

[4] World Bank. 2018. Technology Landscape for Digital Identification, Washington, DC: World Bank License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO).

those systems. There were important roles for government to uphold regulation and efficiency. For individuals, it was not clear if consent is meaningful because the customer does not have the option to say "yes. Indeed, there was a belief that "*most people have no idea what the service provider is doing with the data"* — and that this would need to be addressed to build meaningful trust.

Trust in **digital ID for finance** was discussed in the context of the **payment history** of a consumer/user of private services. One participant said:

> *"consumer trust in the service provider is created by the past conduct (of the service provider) and the consumer's 'experience' of data use or misuse. Once there has been a misuse or data breach, the consumers will not trust the service provider anymore*."

The group also noted the ratification of Thailand's new data protection law while indicating that implementation will take time. One participant suggested that some companies may create trust by being *"internally compliant,"* adding that the provisions and ethos of the GDPR would influence some European companies.

In discussing **an ID issued by an employer**, in the context of a contract driver for a company providing commuter services**,** there was an acknowledgement of the *"asymmetry of power of the two essential parties — the company and driver*." The participants explored this asymmetry by asking questions such as *"What does the employer provide in this relationship?" and "What are the obligations and rights of the contract driver?"* They emphasized *reciprocity* as the *foundation for trust."* The role of trust was felt to be critical in terms of "*the company trusting that work will be completed as agreed"* and "*the driver trusting to be paid*." At the same time, customers gain trust in the validity of the credential. They trust that *"there is a background check on the company drivers and that they will be driven safely."* Essential to the customer's trust is their *"brand identification*" of the transport service in question.

Practices for Good ID

Good ID is established through trust-building practices that Omidyar Network defines as transparency and accountability as well as design features like user control, user value, inclusion, privacy, and security.[5] Participants discussed practices that could help strengthen the elements of trust and design required to establish Good ID in Thailand, focusing on state-issued credentials.

The element of **transparency** was recognized as particularly important in building trust. There was a sense among the group that building Good ID must start with a policy-making process that is *"transparent, involving consumers*." The group also felt that emerging policy should allow the consumer to select which information to provide or *export* and include *opt-in* or *opt-out* options (with each *opt-in* accompanied by *"the ability to opt out in future"*). There was also a strong emphasis on the inclusion of auditing processes to control

[5] Omidyar Network, Omidyar Network Unpacks Good ID - May 2019.
https://www.omidyar.com/sites/default/files/ON%20Unpacks%20Good%20ID_Final_3.7.19.pdf

governance. The group emphasized that transparency should be built into the *“design of the technology,”* and discussed whether newer technologies, such as the hot topic of blockchain, would be helpful. Although, blockchain is often held up as a transparency enabling technology, participants felt that the *“privacy and governance issues”* of decentralized technology have not been fully explored.

Another vital element in building trust for Good ID is **accountability**, and the group explored this across a number of different dimensions. They recognized that Thailand’s existing national ID presented issues of standardization and *“vendor lock-in,”* limiting the realization of accountability. Participants also proposed that any new design should involve a national ID *“linked to the (user’s) account for access to government and business services*.” The issuance and misuse of credentials is a common vector for accountability, and participants felt that *“the government has to give accountability to the citizen in exchange for data from the citizen.”* Participants also reflected on the challenges of accountability, noting both the difficulty of holding businesses to account and the complexity of governmental complaint processes or even identifying the responsible department.

The group emphasized that strengthening **privacy** as part of state-issued ID could be achieved in part through utilizing ‘*“technical features which exist (in the current system) but are not utilized*.” Some felt that *“the physical card is overused and over-shared, while the technology is underutilized.”* The participants also highlighted the cultural element in the use of the ID, observing that “*people in Thailand are used to using their ID in contexts that do not strictly require it.”* They noted that *“there is too much personal data on the card.”* An important design choice that could strengthen privacy would be to ensure that future ID schemes *“reduce personal data and raise more privacy awareness,”* enabling individuals *“to choose what data to review by transaction.”* The participants stressed the need to **partition** the data. As a principle to guide decision making, one participant suggested that although *“we cannot change people’s culture right away, we can change the design.”*

The element of **inclusion** was discussed in various ways but particularly in the context of vulnerable groups. This included discussion about digital ID and inclusion for refugees, and how the UNHCR credential “*unlocks a lot of opportunities”* for refugees. Participants viewed control over data as particularly important for vulnerable populations, especially refugees, but also as relevant to everyone; in short, extreme cases, such as identification for refugees can and should inform mass market design.

Finally, to really achieve ID that is good for individuals, it must be valuable to the user (i.e., have **user value**). Participants felt that one of the strongest cases for user value was simplicity and ease of use—the fact that the users currently “*have to carry around tons of IDs”* and that *“combining everything into one ID*” would appeal to users. The practices to achieve this in Thailand would include a collaborative effort on the part of key stakeholders—such as the provincial department, the National Broadcasting and Telecommunications Commission (NBTC), and the financial sector (including Bank of Thailand). Although getting everyone on the same page will be challenging because *“each sector has its own way to focus on consent,”* it is vital *“to deal with all parties and get consent from each sector.”*

The element of **user control** emphasizes the importance of the individual in the functionality of an identification system. A number of participants felt that there was currently little user control over what and how data is used—indeed, most have little idea what happens to their data once collected. In deciding what information to include in the ID, participants again expressed concern for protecting individual privacy and ensuring that *"identity attributes [. .] be separated from socio-economic status."* It was agreed that information such as *"disability, lifestyle preferences, religion, caste and socio-economic background"* should be excluded.

Additionally, convoluted bureaucratic systems can make it difficult to see where data is stored. For example, participants discussed the complex system of land registration in Thailand wherein any change of information on the registry involves many layers of approval from different departments. There was a sense that an important set of practices to move towards Good ID would be to include tools and properties to enable users to update data as well as increase the visibility of data use. Specific recommendations included that the user have *"discretionary privacy control"* on who can access their data, including sensitive data on education or criminal history. Furthermore, there should be *"multiple means of authentication"* and an accessible grievance system.

Achieving **security** is critical to successful state-issued ID, both for institutional data protection and for individual protection of rights and entitlements. The group discussed this latter aspect, noting that "*today a citizen's ID in Thailand is offline, manual and used for identification"* and, as a result, one cannot not *"prove"* oneself without the card, creating a risk for individual security and rights protection. While the ID card is in fact a smart card that can be retrieved using a pin, *"many, if not most, people do not know their pin*." In creating its Good ID scenario, the group specifically emphasized the importance of design principles, online usage, and security features. And they made a particular case for decentralization, noting that *"decentralization of authentication matches more the way we actually do things in life."* The group additionally suggested that authentication should depend not on a single factor, such as having to carry the physical card, as under the existing ID system.

In plenary discussion participants debated the different models of identification, especially the respective values of centralized, universal identification systems, such as India's Aadhaar, and more decentralized, federated identification systems such as Thailand's planned NDID program. However, NDID still leverages the existing centralized national ID system in Thailand to onboard people and link digital identities with their respective legal identities as they exist in the civil register. In other words, when it comes to identification systems, centralized/decentralized is not either/or. Notably, when asked how many favored a centralized identification system, no participant raised their hand.

Reflections and summary discussion: Good ID in Thailand

There was a palpable sense of collective purpose around the imminent launch of the Thai national digital ID (NDID) in the room. Initially that purpose was expressed through three lenses reflecting the different responsibilities and backgrounds of the participants, which ranged from government bodies directly responsible for the technical design of the programme and financial organizations with vested interests in the enabling function of the system to regulators and civil society actors concerned about the impact of the NDID on individuals. Thus, the three lenses the discussion centered on were (1) an attractive user proposition (convenience, interoperability, etc.), (2) safety and security (largely expressed through technological solutions such as encryption and blockchain), and (3) the need to address unintended consequences (a far less well defined, but no less important lens).

As conversations in the room evolved, however, two further, cross-cutting issues emerged as important for the next stages of digital ID development, namely: **transparency** and **greater digital literacy**. The former was seen as crucial to addressing some of the potential unintended consequences (which had become more clearly articulated throughout the day). The latter was seen as important to allowing citizens to claim necessary digital rights and better understanding of the potential benefits of a digital ID (many of which are not being realized in the current iteration of the national ID, according to the participants; e.g., people not knowing their pins and the full capabilities of the smart card chip not being used, such as secure partitions).[6] Participants discussed these issues both in terms of the ID issuers' responsibilities to design for inclusion so that they can be used by anyone eligible for ID, as well as the need for residents of Thailand to be more aware of the digital system.

The **technical discussion** generated specific, concrete recommendations for action around the new digital ID scheme. One of the strengths of the overarching conversation taking place within the workshop was that, where goals conflicted (such as the disconnect between the notion of convenience brought about by a single digital identity vs. the need to prevent digital oligarchies arising from the mass — and covert — collection of personal data), they were immediately translated into real conversations about how each goal could be addressed within the technological development of the national ID. This demonstrated a sense of entrepreneurialism in the room in which design and technological innovation were seen as having the potential to address concerns.

The **regulatory discussion** focused on the Thai Data Protection Act was approved and endorsed by the National Legislative Assembly in February 2018,[7] and is to be upheld by a specially convened Personal Data Protection Committee, but the group only made limited progress in producing specific, concrete regulatory recommendations. The notion of strong systems of punishment and reward for poor stewardship of data was embraced with some gusto (though it also met with incredulity), and much reference was made to the forthcoming data protection act and its possible role in introducing data rights to Thailand. However, there was little success in identifying governance mechanisms that could identify bad practice and hold those responsible to account.

[6] Under the new Digital ID bill, a national digital ID company (NDID) will build a digital ID platform to identify and authenticate citizens' digital IDs.
https://www.bangkokpost.com/business/1545478/paving-the-way-to-digital-id

[7] https://www.endpointprotector.com/blog/the-thailand-personal-data-protection-act-what-we-know-so-far/

Decisions for Good ID

Participants in Bangkok identified concrete actions to advance Good ID in Thailand, organized around the two practices that support Good ID — **transparency** and **accountability** — followed by the five design features of Good ID — **privacy**, **inclusion**, **user value**, **user control**, and **security**.

Transparency group: participants proposed a *six-step solution* for Thailand's national ID. 1), legislation through public consultation; 2), improving user access to system and data; 3), increasing transparency on data access and use; 4), opt-in and opt-out options for users; 5), raising awareness of systems, data and transparency through increased user literacy; and 6), improving auditing processes of systems and data use.

Accountability group: To strengthen accountability, participants recommended raising awareness and improving compliance through monitoring and reporting mechanisms as well as strengthening sanctions. It was said that *"accountability arises from the moment that someone is doing something in relation to the control of the data or when someone is processing something"* and that *"we want to build the awareness of the whole ecosystem… If something wrong happens, it is not only one person or entity who is accountable but the whole ecosystem."* To achieve this understanding, participants proposed a comprehensive program of "communications, incentives, user awareness, and standards."

Privacy group: participants identified four measures that could strengthen privacy in Thailand's national ID. Firstly, strengthening citizen awareness of privacy (and security issues) through a broad education and awareness campaign. Secondly, strengthening regulatory capacity to uphold data and privacy laws "*faithfully while assisting consumers."* Thirdly, the private sector needs to *"create collaborative practices that build trust."* And, fourthly, the government sector should lead by example by demonstrating practices of transparency in data management and use. As an underlying principle across each of these measures, participants recommended data minimization and **privacy by design** in system and technology design.

Inclusion group: to achieve inclusion for refugees, participants recommended the establishment of *"a transnational ID with minimum data (as needed) . . . and an option to delete yourself."* This would provide real value for refugees in cases of resettlement, but should be designed according to the principles of data minimization to limit the exposure of vulnerable information.

User value group: participants emphasized that user value is particularly important for the adoption of digital ID — that any system will fail *"if the customer does not want to use it."* Participants also highlighted the importance of establishing trust as key to achieving user value — specifically, trust between government, businesses, and users. The government's responsibility was to ensure that the system is stable and can be audited while also monitoring in order to prevent violation or unnecessary use of the user's basic information. The private sector's responsibility was to emphasize *"customer value"* and ensure the **ease** and **convenience** of transactions. An emerging theme within this discussion was the tension between this model of user value and the elements of transparency because increased transparency may limit trust and adoption.

User control group: participants proposed three key measures that need to be effected that needed to be taken to advance Thailand toward Good ID: (1) building literacy, focusing on the marginalized and excluded; (2) ensuring the ability of the user to delegate agency and enabling an industry of agents who can act on behalf of the user — *"If I don't control my data I should at least know who should control my data"*; and (3) strengthening grievance control mechanisms to support greater user control. Recognizing that these were very political decisions, there was debate around who is critical to implementing user control and the different roles of the government, the judiciary, the media, and other actors. Underlying this discussion was a key principle of enabling data control through the idea of **design for delegation**.

Security group: participants focused on decisions that could support a Good ID platform that would be secure while allowing for transactions. One concrete idea was to *"use the public infrastructure for encryption to ensure confidentiality."* This could be furthered by using a decentralized design model to separate *"authentication"* from the *"transactional use"* of the Good ID.

Annex 1: Participant definitions of “Good ID”

“Good ID aims to identify individuals and connect the world.”

“Good ID identifies a person correctly in a convenient way.”

“Easy to identify in one hand.”

“Verify me to know me.”

“ID comprises collective of data footprint.”

“Digital ID records and easy to use.”

“You know me well, work with me.”

“Works on my behalf”

“Only minimum data required to identify.”

“Contextual, configurable, controllable.”

“Can be re-secured after identity theft/compromise.”

“Secured, private, controllable ID for all.”

“Respect my privacy, make it secure.”

“ID for me, not for anyone.”

“You know, I control my ID.”

“Don’t track without necessity or consent.”

“Secure, unforgettable, private, representation I control.”

“Personal, secure, private, control.”

“Good ID should have privacy, security, is easy to remember and control.”

“Privacy and cannot track.”

“Know who accesses and uses us.”

“Good ID is bad without proper consent.”

“Protect individuals and accountable, purposeful design.”

“Good ID is identity for protection of people using the system.”

“Good ID: convenient, privacy, and trusted ecosystem.”

“My ID, my life, my personality.”

“Good ID is reliable, interoperable, inclusive, secure, transparent, and controlled by user.”

“Include me, don’t discriminate against me, forget me.”

“Good ID is basic human rights.”

“Trusted Good ID is a foundation for human rights.”

“Value my agency, respect my rights.”

“Consensual Good ID as human rights foundation.”

“Good ID is useful, private, and compartmentalized.”

“Open doors without fear or favor.”

“Easy to obtain, verified, respected, and controlled.”

“Good ID should be reliable, secure, inclusive, transparent, interoperable, and controllable.”

“I decide when to share identity.”

Annex 2: Participants pledges for action

Overall, the shared sentiment established during this closing session features promises and hopes for future collaborations to create Good ID.

"I am committed to real privacy protection. We believe that our narrowly-focused biometrics can be helpful to this process.”

"I will ensure that a checklist of ‘accountability’ is applied in public services.”

“Having worked on digital rights in Thailand, it is my commitment to still represent the voices of the disadvantaged groups especially in building their literacy on digital rights."

“My commitment is to think more about ways that we can build in social value for disadvantaged groups so that it becomes something that people want to pursue and opt into."

“I will bring more security to the platform and allow people to use this system securely."

“. . .I am hoping to use my expertise to help come up with a good design that not only addresses security but also all these issues that are important.”

"As a designer and developer of IT systems I will take transparency logic and apply it in design and definitely I will design the opt-out option.”

“As a technology provider, we will provide technology to implement the Good ID whatever shape or form it may take."

“. . . We have been promoting the NDID model, we will promote it and also support moving this to the next level in terms of ASEAN and other countries so that this can be recognized across borders. With the Internet there are no borders, and a lot of value to be unlocked".

“. . .I can commit to taking the discussions and learnings from the Thai set-up and share them with my colleagues, especially those in other Asian countries."

“As a lawyer and a citizen, I’ll be one voice to make sure that all stakeholders that are involved are held accountable. I will seek to raise transparency using the legislation that we already have.”

"As the head of the legal department. . . I will make sure that the relevant teams in the organization are aware of customer rights, transparency, security, user rights and inclusion. From the consumer point of view, we have to make sure that the consumers know of their rights, and to ensure those ‘features’ for the customer to exercise their rights.”

"As the chief transformation officer . . . looking into data privacy . . . I would also like to raise awareness of the audience of how the NDID will affect them and discuss what we should do to make it a ‘better ID.’”

"We take action from today by opening a public forum to get Thai audiences to understand the issues and to participate in policy-making processes.”

"... my commitment is to help other parts of the world understand another technology on the national digital ID and to help my staff to achieve their commitment.”

"As part of a standards team, I will bring all the aspects we discussed today to provide good guidelines to all the internal processes at my organization.”

Annex 3: Workshop Agenda

09:00 ARRIVE AND REGISTRATION

INTRODUCTIONS

-
- Mrs. Vunnaporn Devahastin, Deputy Permanent Secretary Of The Ministry Of Digital Economy And Society
- Professor Thawatchai Jittrapanun, PhD; Commissioner, National Broadcast And Telecommunications Commission
- Abiah Weaver, Director, Omidyar Network
- Chris Locke, Caribou Digital

MORNING SESSION 1

- Case Studies From The Region
- Discussing Best Practices In Thailand

MORNING SESSION 2

- Improving Transparency, Accountability, And User Engagement
- Making Other Choices And Decisions That Drive Public Trust And Value

12:30 LUNCH

AFTERNOON SESSION

- Designing New Practices For Positive Outcomes
- Finding Ways To Advance Good ID Together

15:20 REFLECTIONS AND CLOSE