ORF ISSUE BRIEF

JUNE 2020
ISSUE NO. 367

# Building Trust: Lessons from Canada's Approach to Digital Identity

SUNIL ABRAHAM

**ABSTRACT** Both during times of normalcy and crises, governments depend on increasingly digitised identity systems. Such systems, however, have been considered controversial since the use of IBM machines to facilitate the Holocaust. Since then, more contemporary identity systems have tried to ensure that they do not violate citizens' essential rights. This requires multi-stakeholder coordination, a network paradigm, a focus on open standards rather than specific technologies, clarity and predictability on intellectual property, an openness to the latest technological developments, and a commitment to interoperability and compatibility across institutions and entities. Most critically, successful digital identity projects need to build trust. This brief draws lessons from Canada's experience of building a national identity ecosystem.

Attribution: Sunil Abraham, "Building Trust: Lessons from Canada's Approach to Digital Identity," *ORF Issue Brief No. 367*, June 2020, Observer Research Foundation.

**Observer Research Foundation** (ORF) is a public policy think tank that aims to influence the formulation of policies for building a strong and prosperous India. ORF pursues these goals by providing informed analyses and in-depth research, and organising events that serve as platforms for stimulating and productive discussions.

To know more about
ORF scan this code

ISBN 978-93-90159-28-4

© 2020 Observer Research Foundation. All rights reserved. No part of this publication may be reproduced, copied, archived, retained or transmitted through print, speech or electronic media without prior written approval from ORF.

## INTRODUCTION

*"The ultimate crisis that Earth is now facing means that open technology is the unavoidable responsibility that advanced countries have to all humanity."*

- Cixin Liu, The Dark Forest (2008)[1]

The current global health crisis is not because of extra-terrestrials swarming the Earth from outer space, but a 60-140-nm virus occupying the "inner space" of people's bodies. More than two months since the World Health Organization (WHO) declared a pandemic of COVID-19, various measures that have been taken by governments have involved the use of open technology. For example, technology giants Amazon, Facebook, Hewlett Packard Enterprise, IBM and Microsoft have joined the Open COVID Pledge[2] so that any entity can freely use their patents to address the pandemic.

One application of open technology is in establishing digital identity, and governments across the world are using it in two direct ways to flatten the curve:[3] for contact-tracing measures and for issuing immunity passports or certificates. Singapore was the first to make its contact-tracing app open-source, and private sector collaborations like the COVID-19 Credentials Initiative (CCI) featuring 60 digital identity technology providers are producing open, standards-based solutions for immunity certificates.[4]

Indeed, digital identity projects may be considered the "holy grail" of e-governance. Since they build upon the history of citizenship, existing power relationships, and governance cultures within a jurisdiction, there are many avenues for errors. Intangible ingredients of a project—foremost amongst them, trust—take years of flawless execution to build, and a single high-profile mistake can do irreparable damage.

Across the Commonwealth countries is a question that begs to be asked: Which digital identity paradigm is best suited for "normal" situations, and which ones are appropriate for exceptional circumstances? A corollary question is: How do various forms of openness within the digital identity ecology contribute to the resilience of the paradigm?

In India, the digital identity project, Aadhaar, has a single identity provider, the Unique Identity Authority of India that determines if a person is who they say they are. Aadhaar falls within the classic hierarchical, centralised, command-and-control paradigm that is increasingly falling out of favour with technologists across the world because even a single vulnerability can bring the entire e-governance system to a standstill.[5] The network looks like a star, with the UIDAI at the centre and various other actors all connecting to the UIDAI for identification, authentication and authorisation of transactions.

In the UK, following a failed attempt to launch a centralised ID system, the government shifted gears and has adopted a federated approach. Under this approach, between 2013 and 2015 the UK government attempted to establish a competitive oligopoly of identity providers.[6] It started out with nine providers, dropping down to two players over the years. The project ended up with a virtual monopoly and public funding for the project will run out in 2020.[7]

In Australia, the government seems to be moving towards the federated model, even as a single government-appointed identity provider is leading the efforts. Moreover, that government provider myGovID is not being treated at par with private sector providers.[8] Ideally, when competitive oligopoly is being established, the government should only act as a market maker[9] and not a participant in the market.

Canada, for its part, has opted for the federated model like the United Kingdom and Australia, although they are doing things more carefully by prioritising ecosystem development and standards development over technological solutionism.[10] There are many lessons from Canada's approach to implementing digital identity solutions that can help inform projects in other countries, including India. The following paragraphs outline those lessons.

## THE CANADA MODEL FOR DIGITAL IDENTITY

### Multi-stakeholder coordination

To effectively implement networked governance, the first step is to establish consensus and inducement-oriented systems. Gilles Paquet from the University of Ottawa argued as early as 1996 that the governance system is "coordinated much less by coercive and hierarchical top-down pressures than by associative networks of cooperation built on a quid pro quo exchange and on consensus and inducement-oriented systems."[11] The Digital ID & Authentication Council of Canada (DIACC) was established in 2012 as a self-governing entity so that the Ottawa administration, provincial governments and the private sector entities could engage and collaborate on equal footing when designing specifications of an digital identity ecosystem that worked for everyone. Since the Council was working with the aim of establishing trust across the ecosystem, each step was carefully considered, and it took almost four years for the DIACC to produce the overview to the Pan-Canadian Trust Framework (PCTF). Following the approach adopted by Standard Setting Organisations (SSOs) like World Wide Web Consortium (W3C), Institute of Electrical and Electronics Engineers (IEEE) and the Internet Engineering Task Force (IETF), the first version of the model for the framework was released as a consultation draft in March 2019.

The DIACC's approach to developing a trustworthy framework is in stark contrast with India's, which prioritised speedy execution and scaling. From this view, "moving quickly" was seen as a strategic decision because it "doesn't give opposition the time to consolidate."[12] It is also worth noting that voicing and accommodating dissent to identity schemes is a long established tradition in Canada. For example in 2003, Robert Marleau, the country's Interim Privacy Commissioner, made a submission to the Standing Committee on Citizenship and Immigration titled "Why We Should Resist a National ID Card for Canada",[13] urging the Parliament to reject the proposal for the national ID card. Seventeen years later, there is hardly any visible opposition to the work of the DIACC. A key reason is that the DIACC is undermining neither the existing institutions in the identity ecosystem, nor the relationship between citizens and these institutions. Indeed, through the framework, the DIACC is empowering those same institutions by providing a universally acceptable verifiability standard for every person, every organisation, and every relationship. This all-embracing posture emerges from an authentic practice of multi-stakeholder coordination.

## The network paradigm

In countries like India and Kenya, for example, there is a single centralised government agency that assumes the role of identity authority. Canada, for its part, is clear that no single federal government organisation can provide digital identity for all persons within the jurisdiction; rather, there are 14 different "roots of identity" through which persons can establish who they are. Since the turn of the century this approach has been gaining favour within the Canadian research community.

The 2012 *Frontiers of Networked Governance* report published by the International Institute for Sustainable Development provides a good sketch of how it works: "Networked governance strategies based on active-steering are those by which governments or other centralized governance authorities can put in place mechanisms and organizational structures that allow outside agents and organizations to self-organize, within certain boundaries, to inform centralized problem solving."[14] The network paradigm based on the principle of subsidiarity is the best fit for governments with different degrees of federalism. According to Joni Brennan, President of the DIACC, the key to solving for digital identity requires "interoperable networks that will have verifiable data requesters ask for particular attributes to be verified and attribute verifiers to provide that verification."[15] This is inspired by internet architecture where there is no single point of failure.

## Standards not technology

Centralised, government-provisioned national ID programmes usually start by producing software or hardware artifacts. This could be an ID card, software stack, or mobile application. Canada's DIACC has focused purely on the specification of standards with a clear emphasis on open standards. The stress on open standards is evident in the documentation for the framework which explicitly names standards like Tranport Layer Security (TLS) from the IETF and Decentralized Identifiers (DIDs) from the W3C. Apart from international standards, the framework is informed by existing national standards such as "User Authentication Guidance for Information Technology Systems"[16] from the Communications Security Establishment (CSE) of the Canadian government and also makes references to national guidelines and good practices both within and outside the Commonwealth. Two examples of national standards from other countries allow a comparison to the Canadian approach: the "Digital Identity Guidelines" from the National Institute of Standards and Technology (NIST), United States of America and the "Authentication and Credentials for use with HMG Online Services" issued by the National Cyber Security Centre, and the Government Digital Service which is a unit of the Government of the United Kingdom's Cabinet Office.[17]

Just as SSOs have different business models when it comes to access to the standards specification documentation, W3C has free access while ISO has paid access. While the NIST standards are "not subject to copyright in the United States," they do state that "attribution would, however, be appreciated." Under copyright law this will be the equivalent of having a work in the public domain. On the other hand, the UK government has used "crown copyright" which is a restrictive model where "permission must be sought in advance if you want to copy, republish, translate or otherwise reproduce all or any part of the document." Most copyrighted works come with the same restrictions. For the PCTF the DIACC aligns more with NIST since it is "developed as an open public resource, will always be freely available to the public for review and adoption, and is developed under DIACC's transparent and neutral good governance policies and procedures."

## Clarity on intellectual property

Some identity projects have resulted in dependencies on foreign proprietary technologies that are at the very heart of the project. This is because proprietary code and patents can be trojan-horsed into e-governance infrastructure including digital identity programmes. To enable co-creation where there is certainty about gratis implementation of the standards, it is important to prevent patent ambush and other intellectual property-based rent-seeking. To accomplish this unlike the royalty free W3C standards, and more like the paid IEEE standards, the DIACC requires patent contributors to sign covenants that grant patent license on fair, reasonable and nondiscriminatory (FRAND) terms or non-assertion covenants. Contributors are also required to "declare at the earliest opportunity, any patents they are aware of which they know" that will impact implementation of the standard. Copyright contributors are expected to grant a worldwide, royalty-free, non-exclusive, transferable copyright license to DIACC. This is a clear example where a government has adopted best practices from global standard-setting organisations for the purposes of implementing its own national digital identity system. Why is Canada so particular about providing this clarity when it comes to intellectual property? It is because of their "open by default policy." While other governments across the world are prevaricating about free and open-source software while simultaneously considering policies that allow for proprietary software in government, Canada has not given up its decades-old push for openness. Canada has pushed its preference for openness both in its domestic policies and also propagated internationally through key research organisations like the International Development Research Network.[18]

In December 2018, the Government of Canada adopted the latest Directive on Management of Information Technology[19] which states that "where possible, use open standards and open source software first." The trust crisis around proprietary contact-tracing mobile applications for tracking COVID-19 is a ringing endorsement of the Canadian approach. Governments today need to be more vehement in their embrace of openness than ever before, given the grip that surveillance capitalists have on contemporary information societies.

## Embrace of the latest technology

The Canadian approach has been bold in terms of making friendly overtures to technological implementations of the latest development in identity solutions—self-sovereign identity. According to Christopher Allen, co-chair of the W3C Credentials Community Group, digital identity technologies have gone through four stages of evolution: Centralised identity; federated identity; user-centric identity; and self-sovereign identity.[20] This brief has so far discussed the first two stages.

The third phase, User-centric identity, is when the user can either register their own ID on their own network infrastructure or by using an identity provider; unlike the second stage, there is no federation. The final stage of self-sovereign identity is where cryptographically, the user controls all relationships with all identity providers and requesting organisations. While self-sovereign identity has not been taken seriously by many other governments, the PCTF has referred  to two standards that are being developed at the W3C and  could be considered components of this paradigm: Verifiable Credentials and Decentralized Identifiers.

Verifiable credentials is a standardised digital representation of both online and offline credentials that prove things about the holder. For example an educational degree, an immunisation certificate, or a driver's license. The document in its entirety and/or its components can be converted into verifiable credentials because the technology allows for atomisation. For example, using verifiable credentials, a driver's license can prove its owner's age without having to reveal the name. Decentralised identifiers involve the use of tokens so that instead of propagating ID numbers across multiple government or private-sector databases which enable surveillance, unique tokens are used for each purpose. This also builds accountability because breaches can be connected to a specific data controller. The W3C standards also allow parts of the Canadian identity ecosystem to be connected to public or private blockchains.

## Interoperability and compatibility

Rather than treating identity questions as a binary dichotomy, Canada treats identities as composite and therefore these questions could have a range of answers.  Emerys Schoemaker of Caribou Digital puts it best when he writes "like an 'identity mosaic', people select and combine identity elements for transactions during the course of everyday life."[21] This means that the new identity solutions should not be introduced as a monopoly, as has so often been the case in traditional e-governance projects.

To use an example from Karnataka—backward compatibility with paper records was eliminated when the architects of the Bhoomi project used legal reform to derecognise the competition to digital land records. Under the Canadian approach, there is no issue if the government or the private sector are not able to afford more up-to-date technology. PCTF author Dave Roberts explaining how they have modified the W3C data model when it came to verifiable credentials, described the project's ambitions as follows: "If we cannot model something as physical and tangible as Marco Polo's letters of introductions to the emperor Kublai Khan, then we have failed because they are credentials too and they exist in the real world."[22] This is quite a high bar when it comes to taking legacy systems along, however this approach has resulted in projects that have been built 40 years ago being integrated into the PCTF ecosystem. However, it will be recognised that these are transactions with different Levels of Assurance (LOA).

The four levels currently being envisioned are: LOA1 or "little or no confidence", LOA2 or "some confidence", LOA3 or "high confidence", or LOA4 or "highest confidence". The approach is, as Tim Bouma points out, in line with the latest thinking from the FATF who in their most recent guidance on digital identity,[23] recommend that governments, "Apply appropriate digital ID assurance frameworks and technical standards when developing and implementing government-provided digital ID. Authorities should be transparent about how the jurisdiction's digital ID system works and its assurance level."[24]

## Soft infrastructure of digital identity

The most important determinant for successful adoption of digital identity is the prevalence of a culture of trust, which has to be built slowly and iteratively. The first step towards building trust is getting different stakeholders to understand one other. Joni Brennan, Tim Bouma and Dave Roberts and other contributors to the PCTF are focusing on semantic interoperability. Twenty-one standardised trusted processes have been developed in a consultative manner so that they can be mapped on to existing business processes across the government and in the private sector.

A conformity criteria has also been developed that enables independent assessments and certification of trusted and interoperable systems within the ecosystem. This means that "Canadians will be able to choose any partner, use any device on any platform, to access any service they need."[25] It also implies that a user is not compelled to use a device, platform, service or partner that they do not trust. Under this federated approach, when trust is damaged within the ecosystem, only some partners and citizens will be negatively affected. Interoperability prevents an erosion of trust across the ecosystem. It is precisely this soft infrastructure associated with the PCTF that will make the Canadian ecosystem more resilient to future crises.

To be sure, the PCTF is not perfect and there are many areas where improvement is required. One such aspect is in ensuring agency and consent during the use of facial biometrics. However, the forward-looking approach of the Canadian government has resulted in many interesting products and services. For example, a soon-to-be launched "Known Traveller Digital Identity" service by a company called Vision-Box will enable paperless biometric immigration between the Netherlands and Canada. The implementation partners are Air Canada, KLM Royal Dutch Airlines, Amsterdam Airport Schiphol, Toronto Pearson International Airport, and Montréal-Trudeau International Airport.

Another interesting development is Owl, a technology provider that has enabled remote e-KYC using zero-knowledge protocol, with zero data retention and end-to-end encryption that combines multiple data points such as driver's license, health card, and social insurance records in real-time. More recently, seven of Canada's major financial institutions – Bank of Montreal, Canadian Imperial Bank of Commerce, Desjardins, National Bank of Canada, Royal Bank of Canada, Scotiabank, and Toronto-Dominion Bank—launched the Verified.Me service that allows these institutions to act as identity provider for a fee when users want to use government services.

## CONCLUSION

It is important for other countries in the Commonwealth to closely monitor developments and best practices in Canada and see if they can be adapted into their own national digital identity projects. The Commonwealth Digital Identity Initiative, launched by GSMA's Digital Identity programme in partnership with the World Bank ID4D programme and Caribou Digital, provides one such forum for learnings and discussions.

As COVID-19 makes it clear, it is not sufficient to solve the digital identity and trust challenge within national borders. Solutions need to have global compatibility and interoperability, since many of the basic rights of citizens are also afforded to non-citizen residents and even illegal immigrants; states need to honour them under international law.

Governments should pay heed to the fact that only those solutions, services and products that win the people's trust will succeed. Despite all the right moves by the Singapore government, for instance, only one-sixth of its citizens have downloaded their contact-tracing app.[26] Governments should declare success only when opposition to digital identity projects end. They need to build trust so comprehensively that the people themselves become champions of the digital identity ecosystem.

*(The author thanks Jyoti Panday for her assistance in completing this brief.)*

## ABOUT THE AUTHOR

**Sunil Abraham** is Endowed Professor for Digital Policy and Design Practices, ArtEZ University for the Arts, The Netherlands.

## ENDNOTES

1. Cixin Liu, *The Dark Forest* (London: Head of Zeus, 2018).
2. "About – Open Covid Pledge," accessed June 3, 2020, https://opencovidpledge.org/about/.
3. 'Flattening the curve' is a term which medical experts use in times of health emergencies—it is the idea of slowing a virus' spread so that fewer people need to seek treatment at any given time.
4. "Covid Credentials Initiative : Home," Covid Credentials initiative : Home, accessed June 3, 2020, https://www.covidcreds.com/.
5. "Cybernetica Case Study: Solving the Estonian ID-Card Case," Cybernetica, December 13, 2017, https://cyber.ee/news/2017/12-13/.
6. Edgar A Whitely, "Trusted Digital Identity Provision: GOV.UK Verify's Federated Approach" (Center for Global Development, November 2018), https://www.cgdev.org/sites/default/files/Trusted-Digital-ID-Provision-govuk.pdf.
7. Bryan Glick, "Three More Identity Providers to Withdraw from Troubled Gov.uk Verify Programme," ComputerWeekly.com (ComputerWeekly.com, August 23, 2019), https://www.computerweekly.com/news/252469110/Three-more-identity-providers-to-withdraw-from-troubled-Govuk-Verify-programme.
8. Patrick Scolyer-Gray, "Australia's National Digital ID Is Here, but the Government's Not Talking about It," The Conversation, January 27, 2020, https://theconversation.com/australias-national-digital-id-is-here-but-the-governments-not-talking-about-it-130200.
9. "Government in Markets: Why Competition Matters – a Guide for Policy Makers," Government in markets: Why competition matters – a guide for policy makers § (2009), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/284451/OFT1113.pdf.
10. Evgeny Morozov, *To Save Everything, Click Here: the Folly of Technological Solutionism* (New York: PublicAffairs, 2014).
11. Gilles Paquet, "States, Communities and Markets: the Distributed Governance Scenario," accessed June 3, 2020, https://doi.org/10.20381/RUOR-1269.
12. Shriya Mohan, "'Demonising of Aadhaar Is Irresponsible'" (The Hindu BusinessLine, March 10, 2018), https://www.thehindubusinessline.com/blink/cover/demonising-of-aadhaar-is-irresponsible/article21987575.ece.
13. "Why We Should Resist a National ID Card for Canada," Why We Should Resist a National ID Card for Canada § (2003), https://www.priv.gc.ca/media/1310/submission_nid_030918_e.pdf.
14. Gabriel A Huppé, Heather Creech, and Doris Doris Knoblauch, "The Frontiers of Networked Governance" (International Institute for Sustainable Development, February 2012), https://www.iisd.org/sites/default/files/publications/frontiers_networked_gov.pdf.
15. Canada's Digital ID Framework - Joni Brennan, DIACC, YouTube (Payments NZ, 2018), https://www.youtube.com/watch?v=ahsWWTWI2HM.

16. “User Authentication Guidance for Information Technology Systems,” User Authentication Guidance for Information Technology Systems (2018), https://www.cse-cst.gc.ca/en/node/2454/html/28582.

17. “Good Practice Guide No. 44 Authentication and Credentials for Use with HMG Online Services,” Good Practice Guide No. 44 Authentication and Credentials for use with HMG Online Services (2015).

18. Matthew L. Smith and Katherine M. A. Reilly, *Open Development: Networked Innovations in International Development* (Cambridge: The MIT Press, 2014).

19. “Archived [2020-03-31] - Directive on Management of Information Technology,” Archived [2020-03-31] - Directive on Management of Information Technology (2009), https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=15249.

20. Christopher Allen, “The Path to Self-Sovereign Identity,” Life With Alacrity, April 25, 2016, http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html.

21. “Identities: New Practices in a Connected Age” (Caribou Digital Publishing, 2017), https://www.identitiesproject.com/wp-content/uploads/2017/11/Identities-Report.pdf.

22. Tim Bouma, “Definitely Identity: Definitely Identity E9 Pan-Canadian Trust Framework with Dave Roberts on Apple Podcasts,” Apple Podcasts, February 2020, https://podcasts.apple.com/ca/podcast/definitely-identity-e9-pan-canadian-trust-framework/id1496565155?i=1000466706784.

23. “Guidance on Digital Identity” (FATF, 2020), https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf.

24. Tim Bouma, “Looking Ahead in 2020” (Medium, January 3, 2020), https://medium.com/@trbouma/looking-ahead-in-2020-830afa372878.

25. Tim Bouma, “IMSC Pan-Canadian Trust Framework Executive Summary,” April 1, 2019, https://medium.com/@trbouma/imsc-pan-canadian-trust-framework-executive-summary-5c89a72e06b5.

26. Clara Chong, “About 1 Million People Have Downloaded TraceTogether App, but More Need to Do so for It to Be Effective: Lawrence Wong,” *The Straits Times*, April 1, 2020, https://www.straitstimes.com/singapore/about-one-million-people-have-downloaded-the-tracetogether-app-but-more-need-to-do-so-for.

ORF OBSERVER RESEARCH FOUNDATION

**Ideas • Forums • Leadership • Impact**

20, Rouse Avenue Institutional Area, New Delhi - 110 002, INDIA
Ph. : +91-11-35332000 Fax : +91-11-35332005
E-mail: contactus@orfonline.org
Website: www.orfonline.org