Designing Democracies using Digital Identity

In the 19th & 20th centuries, the power to issue legal identity became a state monopoly. Whenever states did not properly apply this power, people suffered. In the poor world, those without proof of identity have been cut off from food rations, public housing and other government assistance. This is why the 1989 UN Convention on the Rights of the Child lists the right to birth registration and to a name second only to the right to life, and hence the aim of a “legal identity for all” is included in the sustainable development goals the UN has set for 2030. The World Bank states that at least a billion people cannot produce a birth certificate, often because the states involved do not care to issue them. Being undocumented means being excluded from the modern economy—or working in the shadows and risking exploitation. Identity is a thus a very important service for citizens if they are to fully participate in the economy and society. In Middle French, *identité* meant the “quality or condition of being the same”. It was not until 1756 that the word started meaning individuality.

The fact that identity is governed by the state raises problems. Identity, like treasury bills, can be **taken away** by the state that issues it. Compulsory identity cards have only been introduced during wartime; efforts to bring them back have been repulsed. Most early states were able to operate with broad identities that broad-brushed villages using intermediaries such as feudal lords, village heads and holy men, or through collective fines or punishment. They had need for specifics sometimes: the Romans, peculiarly famous for organised violence, conducted a census so the state could **keep checks** on young men of fighting age and call them up as necessary.

This issue is worsened by another addition to the world of identity—online authentication. The power holders in the physical world has, online, been taken up by Facebook and Google. Nine out of ten non-Chinese websites that allow their users to log in with the credentials provided by another company use both of them. The economic incentives of the internet mean that these systems, like government bureaucracies, associate identity with ever greater loads of information built up by the data-brokers who manage the flows of data between advertisers, tech firms and consumer companies. The firms which provide identity services have real insight into the personal lives of their users, as states have into the lives of their citizens.

The fingerprint was just the beginning. Today, there are a number of unique identifiers. The scope of biometrics includes recognition by face, gait, retina, ear and more. There are official documents and there are also mobile numbers, social network ids, smartphone device ids and loads of browser cookies. Records of each are largely created separately from each other, and administered by different or competing interests within and outside the state. When reconciled, they can produce detailed images of the persons they identify, accurately locating them based on all sorts of varied coordinates. Thus, the demand for Unique Digital Identity for all.

Smart cities which combine both Digital Commerce and eGovernance are being promoted in a big way. Every citizen is given a Digital Identity and would be able to use it to authenticate any transaction either with respect to payments or banking or governments. Authentication could be done using a smart card or fingerprints or iris scans or using facial recognition. Also, with Internet of Things coming into play, all the various functions of the smart city would receive and share data stored in the digital identity. Machine learning would help analyze the data of all the citizens and use Artificial Intelligence to predict and meet the requirements of the citizens on a real-time basis. Also, the need for efficiency and transparency has shaped a lot of international protocols or treaties to get rid of anonymity over the internet to the extent of breaking encryption. Please find below analysis of some of the sectors which advocate for digital identity given the need to satisfy some international protocols or legal frameworks:-

1. Banking, Financial Services and Pensions

   With money laundering scams on the rise, countries have come up with **Anti-money laundering and terrorist financing** protocols to bring fraudsters and economic offenders to book. So, banks as part of their Know Your Customer norms have to capture all the personal data of their customer in order to make sure he can be tracked in case of default. Also, corporations have to report their Ultimate Beneficial Owners (UBOs) in order to make him or her accountable for the actions of the corporation with respect to servicing of debt. Also, this data has to be shared with tax regulators and law enforcement agencies such as Interpol to act quickly in case of fraud. Persons are sometimes issued blue corner or red corner notices in order to prevent free movement of wanted defaulters across borders. Also, with government paid pensions mainly routed through the banking system, the focus has largely been to verify the customer to whom payment is made. In order to improve methods of authentication, passwords and biometrics have led to much precise recognition technologies such as facial recognition and iris scans. Thus, the combination of digital interfaces, digital storage and authentication brings in the era of **Digital Commerce.**

2. Healthcare, Automobiles and Insurance

   Insurance has a very close relation to automobiles and healthcare alike. While different countries have different public healthcare models, private healthcare is mostly linked to health insurance. As per the Bismarck model[1], public healthcare is linked to the employment of the citizen and is financed through social contributions, rather than taxes. Hence, we have health departments working with banks and other government departments to deliver healthcare services. In the Beveridge model[2], healthcare is paid for by taxes, wherein the tax department gets involved. In the American model, public healthcare is only provided to elderly and disadvantaged wherein tax departments get involved along with insurance providers. Corporations citing fraud and harmonization of systems bring in health card solutions with a built-in chip. Also, with medical e-files and e-prescriptions emerging, corporations are also getting into database management in order to help doctors keep track of the patient's medical history and diagnosis.

Automobiles being the order of the day, are linked to automobile insurance as well as the banking system on a real-time basis to automatically pay at toll gates, using digital tachographs to cross borders (in **European Union and North America**) Further, there is good coordination among the transport authorities and banking systems to handle wrongdoing and pay traffic fines. In some countries, even insurance companies work with transport authorities to increase the premium based on the driving behaviour of the driver. Hence, there is a huge database kept with the transport authorities which gets inputs from different players and the information flows out as well. The way in which these systems interact brings in the aspect of **eGovernance**.

3. International Trade and Migration

ICAO, the regulatory authority for global aviation, has called for all new passports to be machine-readable[3] and airports to introduce eGates[4] which would require **biometric authentication**. To illustrate this with an example of United States,the Transportation Security Administration (TSA) published their *Biometrics Roadmap for Aviation Security and the Passenger Experience*, regarding plans to work with Customs and Border Protection (CBP) to introduce increased biometric collection and screening for all passengers, including Americans traveling domestically. Basically, CBP and TSA want to use face recognition and other biometric data to perform surveillance over everyone from check-in, through security, into airport lounges, and onto flights. If implemented, there might not be much one can do to avoid it: the Department of Homeland Security (DHS) has said that the only way once could ensure that their biometric data isn't collected when one travels is to "refrain from traveling."

The roots of this program could be traced to 2016 and 2017 when DHS began ramping up its plans to collect facial images and iris scans from travelers on a nationwide scale. In pilot programs in Georgia and Arizona in 2016, CBP used face recognition to capture photographs of all travelers boarding a flight out of the country and walking across a U.S. land border and compared those photographs to previously recorded photos from passports, visas, and "other DHS encounters." Now, agencies plan to extend this program to all international flights and border crossings. They're also partnering with private airlines and airports to collect and maintain data. The government has said it will retain photos of U.S. citizens and lawful permanent residents for two weeks and information about their travel for 15 years and **retain data** on "non-immigrant aliens" for 75 years. However, there are no restrictions on how long private companies can hold onto the data or what they can do with it.

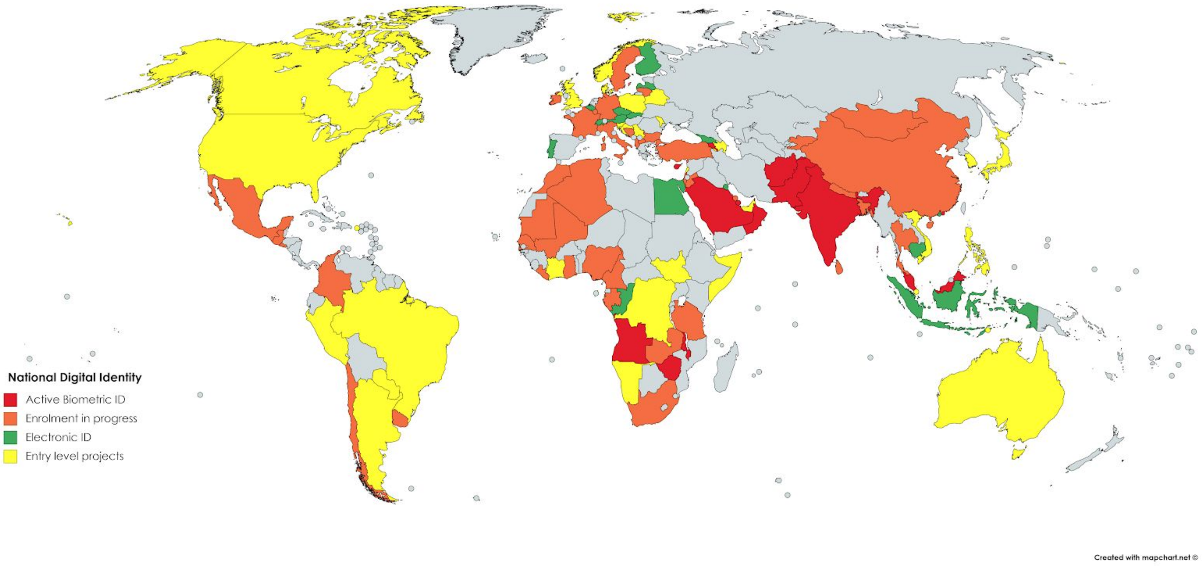
The UN Refugee Agency (UNHCR) has been using databases to collect and manage information on refugees, and has continued to issue refugees with a form of certification of their status. In recent years, UNHCR began deployment of biometric identification systems[5] to register refugees, check their identity and status for aid disbursement. Pilot schemes were initiated in Eastern Africa and Asia in the mid-2000s, and in October 2012, UNHCR announced that it was going to use biometrics in Senegal and South Sudan. A field study conducted by Privacy International in 2008 witnessed large issues being experienced with respect to UNHCR's deployment of a biometric system. The primary concern was the system's reliability: UNHCR had procured a fingerprinting system that was not designed for such huge population, and particularly for those who did not have well-defined fingerprints. UNHCR staff members were unaware of this issue and lacked guidance on how to deploy the system in the field: various field teams were using the system differently, some fingerprinting adults of all ages, young people, and even babies, presuming that the system would work. The system was erratic; it worked sometimes on some refugees, and sometimes it would not work even moments later for the same person. But for UNHCR, it was a perceived success: staff exuded high confidence in the system, and it was considered a useful tool for communicating with host governments that UNHCR was taking fraud seriously.

Digital identification registration systems increase the likelihood that processes become data dependent, and in turn, that implementation is driven by such data. The adoption of biometric technologies means that sensitive personal information of the citizens can be collected and processed rapidly, and decisions can be made with reference to digital identities and aggregated data, the integrity and accuracy of which is difficult to establish or safeguard. Information and data is not purely objective, and discriminatory judgments can become accepted and institutionalised through the use of automated systems. Individuals quickly become reduced to a set of qualitative and quantitative data that may not necessarily represent them or their circumstances accurately. With the advent and introduction of the EURODAC[6] biometric database system for identifying asylum seekers and irregular migrants, submitting to biometric registration has become a compulsory **prerequisite to claiming asylum**. Asylum seekers and refugees are reduced to someone with a ID, whose biometrics need to be verified in order to gain access to, or be prevented from wrongly accessing services. When the biometrics systems do not accurately function, the refugee's status is thereby called into question sooner than the technology. This may lead to the further marginalisation of vulnerable individuals, other human rights violations, and exclusion from vital aid. In September 2013, for example, 6,500 refugees in the Mbera camp in Mauritania were denied access to refugee assistance because of problems with the biometric registration system.

Status of National Digital Identity projects

Digital Identity projects are in different phases in close to 50 countries across the world. Some companies are doing entry-level projects. The main phases of digital identity are:

1. Issue of electronic ID i.e. compilation of databases, deduplication and renewals
2. Enrolment of biometric data from citizens in order to move towards digital identity
3. Use of biometric authentication for government services, banking and elections



Entry-level projects in order to lobby for digital identity

Biometric passport: Argentina, Australia, Belarus, DRC, Côte d’Ivoire, Denmark, East Timor, South Korea, Lebanon, Norway, Peru, Poland, Slovenia, South Sudan, UK, USA

Border control: Croatia, Moldova, Namibia, Serbia, Singapore, United Arab Emirates

Driving License: Brazil, Canada, Philippines

Health Cards: Azerbaijan, Puerto Rico

Crime: Paraguay, Somalia

Digital Finance: Japan, Vietnam

Impact of Digital Identity on Freedom of Expression

National security is one of the permissible grounds for limiting the right to freedom of expression. Digital Identity further strengthens the level of detail into which regimes can go. However, restrictions must provided by law. The grounds for restrictions must be specific. That includes the protection of national security, and the restrictions must be **necessary and proportionate**. Principle Six of the Johannesburg principles[7] look for **imminent violence** as a symptom of invoking national security. General Comment 34[8] of UNHRC also follows precise nature of the threat and its **direct connection** with expression. Also, some countries like Saudi Arabia, Greece and Egypt have militarized courts set up to deal with national security.

Amnesty International has condemned the misguided reaction of many governments to national security threats has been the crushing of civil society, the right to privacy and the right to free speech; and outright attempts to make ‘human rights’ dirty words, packing them in opposition to national security, law and order and national values. A development organization said that in 2015, states went **beyond restrictions and funding** to include new efforts to use the law to break contact between Human Rights Defenders and their international partners and supporters.

According to human rights report published in 2012, more than 140 countries have passed **counter terrorism laws** since the attack of 11 September 2001. Human Rights Watch reviewed 130 of those laws and found that all content one or more provisions that opened the door to abuse.

According to the original objective of the legislatures, **glorification of terrorism** clause was meant to punish the organized promotion of existing terrorist act that could bring those listening to them to radicalize or could drive them to commit terrorist act.

The biggest problem as pointed by Lord Chancellor Falconer is that the executive or the legislature decide on the level of the threat and the extent to which exceptional measures are required, so there is **very little for courts to do** expect ask first, do these measures infringe any individual's fundamental human rights; second if they do, is there a justification for the infringement; and third, is the infringement the minimum necessary to protect our democracy?

US Patriot Act[9] disregarded the fundamental principle that government intrusions on civil liberties should be narrowly tailored to avoid unnecessary invasions of constitutional rights. Anti-terrorism provisions which had been adopted in the mid 1990s and those provisions punished the provision of material support to designated foreign terrorist organizations and it added a few more forms of **prescribed material support** including the provision of so-called expert advice or assistance. The US Supreme Court in Humanitarian Law Project vs Holder[10] has also said that its difficult to assess the impact of certain conduct since conclusions are based on **informed judgement**.

Also courts are not able to assess the **proportionality** of the actions taken by the government because it can not or it determined that it can not assess the evidence provided. Another problem with the cases on national security in context of actual insecurity is a **multiplication of charges in cases**. The prosecutorial net is spread very large and should probably not be the object of such charges.

In fact the seriousness of the situation compelled one of the main union of judges in January 2015 to raise the alarm about what it described at **expedite procedures** which are based on a review of the context, rarely of the circumstances and never of the person indicted with glorification of terrorism: not for having organized demonstrations of support for the authors of the attack, nor for having drafted and largely distributed their pitch, but for clamors made while drunk or in anger.

In a number of countries the courts have upheld government's use of anti-terrorism legislation against journalists **reporting on terrorism issues** or indeed against political dissent. At issue are the vagueness of the definition of a terrorist act, the far-reaching restrictions imposed on the right to due process, and the high number of cases in which human rights defenders, lawyers, journalists, even children and political opponents are charged under the anti-terrorism law for the free expression of very legitimate opinions and ideas.

In Syria, there have been many examples over the last six months in 2016 of journalists being imprisoned because they were simply reporting on the fighting happening. Committee to Protect Journalists (CPJ) has identified the major perpetrators of murders of journalist 2015 to be political groups, military officials, government officials, followed by criminal groups and local residents. According to the Reporters Without Borders and I quote here, **"**The Jihadis regard journalists simply as **military targets** to be eliminated. Jihad's targets include not only political leaders, economic infrastructure and military installations but also media personalities and media centers."

Also, some countries target journalists or any person or group in retaliation for **cooperating** with an UN agency or a independent UN expert.

Impact of Digital Identity on Democracy

As evident from the Cambridge Analytica scandal[11], personal data was analyzed to create and purchase highly targeted ads that were used for the 2016 U.S. presidential elections, as well as potentially for other high-profile elections and debates. In countries with authoritarian regimes, digital identity can be a double-edged sword to muzzle political dissent by actively profiling and targeting journalists, bloggers and human rights defenders.

Digital technologies can of course be used in many ways in elections, including new communication technologies such as Whatsapp. Political parties of-late are creating an internet army and trolls to target voters with biased content. There are different misinformation campaigns which include the use of fake news which is spread through social media platforms such as Facebook, Twitter and Whatsapp.

However, my focus is largely on the digital technologies introduced by electoral commissions: those associated with electronic voter registration, voter verification, and results transmission. By creating opaque components that "lead to more efficient development and employment", new technology risks transferring power "away from the many" into the "hands of the few".

A number of other publications have pointed out similar challenges. Joel Barkan states that new technology in Africa often fails because insufficient attention is paid to the broader **management structures** it needs to function. Studies have questioned the cost of digital solutions vis-a-vis the extent to which automation can improve the efficiency of one aspect of the electoral process but leave other major issues, such as voter intimidation, unaddressed. Worse still, digital technology can promote a narrow focus on particular parts of the electoral process to the neglect of the broader political environment and campaigns – a point acknowledged even by some enthusiasts.

While Yard pointed to the way that election technology can empower a small technocratic elite, and Gonggrijp and colleagues have found that digital processes may become a source of **mistrust**. Instead of specifying an arbitrary threshold for "effectiveness", one should check whether there was meaningful improvement – that is, changes in the logistical management and transparency of the process that were sufficient to have impact on the overall quality of the elections – and whether this can be attributed to the use of new technology. Focussing on improvement over time at the country level has the advantage of accounting for the conditions on the ground in each case, rather than seeking to impose an ideal standard.

Finally, a further unintended consequence of the introduction of digital technology that is often overlooked; is it tends to distract opposition parties from focusing on effectively deploying party agents and leads to funds being directed away from the provision of **domestic monitors**, leaving other parts of the system more vulnerable – especially if digital processes break down. Gonggrijp and his colleagues rhetorically lament the backwards state of many electoral processes and worry that "technology has revolutionized so many aspects of our lives – services, lifestyles and living standards but elections have been left behind".

These narratives depict digital technologies as "anti-politics" machines, providing simple technical solutions to complex social and political problems. For example, De Gregorio in "Enfranchising the Disenfranchised[12]." says that for the public and civil society, the technology companies promise to enable "citizens to access services and exercise their rights securely and easily", and for governments and electoral management bodies they offer a vision of panoptical modern stateness: "helping governments manage the civil identity cycle in the increasingly mobile and globalized world of the twenty-first century". For international or bilateral agencies, meanwhile, technologies provide a way to channel electoral support towards procedural issues that may allow them to avoid accusation of partisanship and **neo-colonialism**.

This confidence often extends to the mass public. In Kenya, for example, a nationally representative survey conducted by Ipsos in early October 2017 found that 58% of respondents agreed that “Elections that use digital technology are *always* more free and fair.” This is despite the fact that, as we shall see, the widespread use of digital technology in the presidential poll[13] of 8 August 2017 did not prevent it from being found to be “illegal, null and void” by the Supreme Court.

Biometric technology cannot prevent multiple registration if the data are not audited to prevent duplication, as was evidenced by prevailing and reportedly outrageous biometric multiple registration in Somaliland in 2008. Similarly, an audit ahead of the 2011 elections in the DRC[14] found 700,000 so-called “doublons” – multiple registrations – but officials ruled that “it was too late to clean up the roll”.

As David Harvey[15] has argued, “all manner of social actors (corporations, entrepreneurs, and various branches of government, most particularly the military) endow technology with causative powers to the point that they will uncritically – and sometimes disastrously – invest in it in the naive belief that it will somehow provide solutions to whatever problems they are encountering”

Nonetheless, it is important to pinpoint that in states with a history of corruption, some of the support for digitization may be mendacious – motivated more by a desire to open up fresh windfall gains than to improve the quality of elections.

Moreover, this funding challenge often generates a complex triangle of economic relations between the donors who finance new technology, the government or electoral officials who procure it, and the international companies that provide it. In this set of relationships, donors can gain by using their leverage to ensure that key contracts go to businesses that operate in their jurisdiction, companies can gain by generating large profits, and officials can benefit by requiring kickbacks to process a contract.

First, problematic procurement processes can lead to poorly qualified companies getting contracts that they are ill-equipped to fulfil. Second, faulty procurement procedures often require the process to be conducted a second time, delaying the purchase of equipment so late that it cannot be effectively piloted. Third, corruption scandals that involve – or are believed to involve – electoral officials, can dramatically undermine public confidence in the broader electoral process, as in the cases of Kenya and the DRC described above.

References

1. An excerpt from correspondent T.R. Reid's upcoming book *The Healing of America: A Global Quest for Better, Cheaper, and Fairer Health Care*, to be published by Penguin Press in the summer of 2009.
2. https://www.pbs.org/wgbh/pages/frontline/sickaroundtheworld/countries/models.html
3. ICAO: Specifications for the Security of the Design, Manufacture and Issuance of Machine-Readable Travel Documents https://www.icao.int/publications/Documents/9303_p2_cons_en.pdf
4. ICAO: Trip Guide on Border Control Management https://www.icao.int/Meetings/TRIP-Jamaica-2017/Documents/ICAO%20TRIP%20Guide%20on%20BCM-For%20validation-16-11-2017.pdf
5. UNHCR Biometric Identity Management System https://www.unhcr.org/protection/basic/550c304c9/biometric-identity-management-system.html
6. EURODAC Regulation https://ec.europa.eu/home-affairs/what-we-do/policies/asylum/identification-of-applicants_en
7. Human Rights Library, University of Minnesota http://hrlibrary.umn.edu/instree/johannesburg.html
8. UNHRC General Comment No. 34 on Article 19 of ICCPR https://bangkok.ohchr.org/programme/documents/general-comment-34.aspx
9. US Patriot Act https://it.ojp.gov/privacyliberty/authorities/statutes/1281
10. Case Analysis, Global Freedom of Expression, Columbia University https://globalfreedomofexpression.columbia.edu/cases/holder-v-humanitarian-law-project
11. Cambridge Analytica scandal https://www.alphr.com/politics/1008854/cambridge-analytica-facebook-what-happened
12. Enfranchising the Disenfranchised – the Case for Election Technology by Paul DeGregorio, former chair of US Election Assistance Commission http://www.thefutureofelections.com/

13. Kenya Presidential Election 2017
https://www.pri.org/stories/2017-09-04/kenya-declares-presidential-election-results-invalid-null-and-void-and-has-set
14. Democratic Republic of Congo 2011
https://www.telegraph.co.uk/news/worldnews/africaandindianocean/democraticrepublicofcongo/8830144/UK-pays-22.5-million-for-questionable-Democratic-Republic-of-Congo-election.html
15. Harvey, David (2003) "The Fetish of Technology: Causes and Consequences," Macalester International: Vol. 13, Article 7.
https://digitalcommons.macalester.edu/macintl/vol13/iss1/7/?utm_source=digitalcommons.macalester.edu%2Fmacintl%2Fvol13%2Fiss1%2F7&utm_medium=PDF&utm_campaign=PDFCoverPages