Emerging incompatibilities between border crossing and national identification frameworks

Sanjay Dharwadker
Head of Global ID Consultancy Practice, WCC, The Netherlands
Future ID3, Jesus College, Cambridge, 18 – 20 March 2019
Panel: Practical inclusion, or how to walk the last mile

Abstract

Amidst a choice of technologies, diversity of policy frameworks, and emergent priorities, countries that intend to upgrade their identity and identification systems today find themselves drawn into a complex vortex. Apart from the national and foundational perspective within which the tensions between civil registration and identification are situated, border crossing and its international context is yet another area where identity and identification play a dominant role.

Ideas and concepts are being developed independently both nationally and internationally and a further schism is being caused by the independent development of the law and technology in both spheres. Is this a last-mile problem or something fundamental? A few situations are presented that throw light on the issues involved and an attempt is made to imagine the impact and the influences on the future course.

Introduction

Many countries today have multiple, frequently overlapping, identification systems. Often these belong to different arms of the same government and were set up at various points in time to meet diverse objectives.

Significant among them are the system to register and aggregate statistics about vital events such as birth, death, and marriage, also known as civil registration and vital statistics (CRVS). While there are older historical references, CRVS in its modern form has been around for over a century— since 1853 in the UK and since 1902 in the US. Today, every country has a CRVS system, but one in every four persons worldwide do not have their birth registered. Statistics for deaths are even more sparse.

On the other hand, there are more modern national (civil) identification systems that also capture an individual's biometrics. But often such systems do not include other traits of an

identity, such as date and place of birth and names of parents. Such information is often critical to determine an individual's entitlements and rights and their relationship to the State. However, biometrics can ensure that it is the same individual (verification or authentication) and through a more elaborate use of matching a biometric against all others in a system (identification), provide conclusive evidence that an individual is unique and not registered twice, under different names for example.

While biometrics is the key feature of a civil identification system, corroboration is central to civil registration; for example, a notification by a health worker and a declaration by parents, verified by a registrar.

There are also functional subsets of individuals in a country, such as those found on electoral rolls, tax payers, and those who receive state subsidies and pensions. Often, the three—civil registration, civil identification and a functional sub-system—need to work together. For example, civil registration might establish the entitlement to stand for elections and vote (by being a citizen by birth for example), while civil identification might establish (by using biometrics) that it is indeed the same person.

During the last few decades there has been a diversification in the modes of biometrics being deployed, from fingerprints to face and iris as well as signatures, gaits, voice, and somewhat of a final frontier, the use of deoxyribonucleic acid (DNA) that not only identifies a person but also links to their parentage, ancestry, and even ethnicity and race.

Also important to the development of identification systems has been the evolution of identification cards—from paper to plastic and from eDocuments with embedded chips (smart cards and ePassports) to entirely digital identity records.

UN SDG 16.9 – the identity game changer

There has been considerable debate about all this recently, especially since 2015 with the formulation of the United Nations (UN) Strategic Development Goals (SDGs). Among the seventeen goals and its one hundred and sixty-nine constituent targets is 16.9[1], which states 'By 2030 provide legal identity for all including birth registrations'. This is considered integral to goal 16, which states 'Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels'.

Target 16.9, while setting a clear direction, has also generated many apprehensions. Although birth registration is legally endorsed in 196 countries (by signing, endorsing, or ratifying the United Nations Convention on the Rights of the Child, CRC[2], 1989), as stated earlier the records are far from complete and despite the current policy focus, access to funds, and expertise, progress is dismal. Also, there is no universally accepted definition of legal identity and finally, how are we to catch up with 100% birth registration in just over a decade? Like immunization, which has plateaued out at about 85%, has birth registration completeness too reached an empirical upper limit?

[1] https://www.un.org/sustainabledevelopment/sustainable-development-goals/
[2] https://www.ohchr.org/en/professionalinterest/pages/crc.aspx

Legal frameworks for identification

Significant investments are being made all over the world and brand-new identification systems continue to be commissioned. A case in point is the Aadhaar system in India that has enrolled over 1.2 billion people and is currently being used for thousands of payment and welfare applications. Every day, the system verifies over 35 million transactions and authenticates 24 million biometrics[3]. Using empirical yardsticks, the Aadhaar system is a significant success, but on using a diversity of normative benchmarks, not everyone agrees. Biometric failure for the old and infirm, for example, has been an especially glaring cause of concern on its promise of universal inclusion. The individual constituents that can enroll for Aadhaar, ironically, fall in between conventional classifications—it neither consists of all persons born in the territories of India, nor its citizens, nor its nationals, but temporally defined "residents"; that is, those who have continuously resided in the country for over 182 days. Why this works in the Indian context is the subject of another discussion.

Many countries have updated their civil registration laws to bring it in line with the UNCRC. This is a human rights treaty which sets out the civil, political, economic, social, health, and cultural rights of children and specifically provides for registration at birth and having a name, parentage, and nationality recorded, as stipulated under its articles 7 and 8. However, not all countries have entirely superseded older practices such as the family book which continue to have legal or quasi-legal status. Also, such laws and traditions are read along with judgements passed by various courts on the subject that make both interpretations and exceptions.

The legal framework for civil identification systems seem to originate in at least three different ways. The first is where an existing law (population registration, for example) is amended and every individual on the register is deemed entitled to an electronic record with biometrics. The second is a de novo statute like in India—the Aadhaar[4] (targeted delivery of financial and other subsidies, benefits, and services) Act, 2016. The third is where a country already has the equivalent of an electronic transaction or information technology act, and an amendment is made for applicability to the national population register, that might be stipulated in another act.

A predominant feature of national identification systems is that they originated in the era of information and communication technology (ICT) and therefore also work to transform paper-based registers to electronic identification records—something that also made the deployment of large-scale biometrics possible. Therefore, parts of the legal changes today have been necessary to keep up with the technological change brought about by such deployment.

In some cases, even though the legal position has changed substantially, amendments have only been brought about one step at a time through administrative changes, via orders

[3] https://uidai.gov.in/aadhaar_dashboard/
[4] https://uidai.gov.in/about-uidai/legal-framework.html. This reference provides the text of the Act as well as the Supreme Court judgement of September 2018.

passed at the bureaucratic level and made public in the National Gazette or equivalent of a country.

It is also a matter of perception, evolving with the passage of time, that the shift from paper identification to an electronic chip of a smart card and finally to a digital record is fundamental in nature. Many years ago, such discussions were more involved. Today, the reliability (and irrepudiability) of electronic transactions is viewed with much more confidence.

Birth registration, for example, provides rudimentary data that is necessary (though not sufficient) for legal identity like date and place of birth (*jus soli*) and parentage (*jus sanguinis*). It may also be required for determining entitlements. Thus, while birth registration might be referenced for tasks that could affect an individual decisively, these are few and far between during the lifetime of a person. However civil identification (verification using biometrics) could be deployed multiple times every month: for payments, pensions, rations, and so on. Usage too impacts the legal and technological nature of the systems.

However, there are limits to which such identification systems can be deployed and the first such limit is quite literally the national border, beyond which travel documents like the passport come into play.

Travel documents and identification

What used to be commonly called a *passport* is more correctly referred to now as a *Machine- Readable Travel Document* (MRTD). There were two reasons for this very characteristic change. It was stipulated that after November 24, 2015, handwritten passports would no longer be accepted as a travel document. Instead, they had to be printed using high-security printers and one of the new features would be the *machine-readable zone* (MRZ), from where a scanner could automatically pick up relevant information for processing by a computer, for example at an airline check-in or immigration counter.

Incidentally, the standard selected for the MRZ was not a usual barcode, but a string of characters and numerals separated by chevrons (>). The text printing on a passport is also highly standardized in terms of font[5], size, and spacing, and constitutes the visual inspection zone (VIZ). Part of the VIZ is also a photograph of the passport holder.

A more advanced version (issued by over one hundred and forty countries) is the electronic passport (ePassport) that has an embedded contactless electronic chip. This chip not only carries the text information of the VIZ but also the photograph which is stored in such a way that it can be used for automatic facial recognition. The data stored on the chip consists of a mandatory minimum set and provides space for optional storage. There is even space for yet unimagined future use. An option is already provided is for storing a scanned image of a birth certificate (ICAO Doc 9303 part 10 – LDS or Logical Data Structure).

The current versions of the passport chip are designed for one-time data that is written, stored, and then locked on the chip. However, a new version of the standard provides for

[5] The font specified is OCR-B, designed by Adrian Frutiger in 1968 and especially suited for optical character recognition by computers and related equipment.

the first time that a part of the chip memory can be dynamically updated and is likely to be first used for electronic recording of entry and exit at each border. There are many more details of the new emerging standards that require a lengthy discussion.

The usual passport booklet size is ID-3, which is 125 × 88 mm (4.921 × 3.465 in), which is also the B7 format. Passports have categories like diplomatic, ordinary, official, emergency, and convention for stateless persons. Countries also recognize passports in the ID-1 (credit card) size which is 85.60 × 53.98 mm ($3_{3/8}$ × $2_{1/8}$ in), often under a regional arrangement like the European Union or ECOWAS in West Africa. The ID-1 size is the most common ID card size, used for credit cards, driver's licenses, and civil identification cards wherever these have been implemented. Electronic chips can be embedded in both ID-3 and ID-1 documents.

It is this entire plethora of technologies, sizes, and categories that falls under the broad definition of an MRTD, for which uniform standards are stipulated by the International Civil Aviation Organization (ICAO) that are binding on its Member States being signatories of the Chicago convention. In its final form, the standard is found in ICAO Doc 9303[6] that has twelve parts. ICAO is supported by means of a memorandum of understanding with the ISO[7] whereby such standards are formulated by experts under various ISO sub-committees and working groups. These are then forwarded to ICAO for review, acceptance, and publication.

The Travel Visa

Superimposed on the primary travel document, the MRTD, is a secondary travel document, the Travel Visa. This standardized sticker pasted on a passport page is stipulated as a specific requirement, usually between countries. An MRTD is universal; on its front page, every country includes a statement to request unhindered travel across international borders. However, the travel visa often qualifies this by imposing additional conditionalities and restraints. Currently there is no standard for an electronic version of a Travel Visa. However, countries have innovated by introducing services like Visa On Arrival as well as electronic travel authorization. Travel Visas belong to the realm of national legislation as well as regional arrangements like the Schengen across European countries. The Travel Visa in its current form originated around the same time as the Passport; that is, just after World War I, around 1920.

Advance Passenger Information (API)

The twenty-first century has seen yet other travel conditionalities being imposed; key among them is Advance Passenger Information (API). Introduced soon after 9/11 as a counter-terrorism measure, its legal moorings rest on a United Nations Security Council (UNSC) resolution that resulted out of its 4385th meeting[8] on September 28, 2001. As per official records, the meeting lasted barely five minutes (convoked 21:55 and adjourned 22:00) and

[6] https://www.icao.int/publications/pages/publication.aspx?docnum=9303
[7] The corresponding ISO Sub-committee is the ISO/IEC JTC 1/SC 17 - Cards and security devices for personal identification and working group ISO/IEC JTC 1/SC 17/WG 3 Identification cards - Machine readable travel documents.
[8] https://www.un.org/press/en/2001/sc7158.doc.htm

thus gives little indication about the discussions and considerations that went into this announcement.

API allows countries to create watchlists and refer to a central international database hosted by Interpol with its headquarters at Lyon, France. The UNSC resolution prima facie allows a destination country to effectively prevent a passenger from boarding a flight and entering their territory. Among the databases is that of Stolen and Lost Travel Documents (SLTD) which currently contains nearly 60 million entries.

Even within the travel sector, the emergent contradictions were immediately overwhelming—a passport that ostensibly allows unhindered border crossing, a Visa that limits the duration, dates, and purpose of visit, and finally an API command that might prevent you from embarking on the trip altogether.

In all cases, the identity of the individual and its comparison to data that States might have in their databases were of paramount importance. Matching of identities thus becomes central to the mechanisms by which the related processes were implemented.

API is a relatively new topic. The principal legal reference can be found in the Chicago Convention annexure 9, amendment 19 (2004)[9]. Since then there have been updates via Amendments 21 (2008), 22 (2010), and 24 (2012). The provisions of API are presented in its entirety in a new chapter in the latest edition (chapter 9 of Annexure 9), which has four sections: (a) General, (b) API and iAPI (batch and interactive API), (c) ETS (electronic travel systems) and (d) PNR (passenger name record). It must be noted that electronic data interchange was first given legal recognition in ICAO operations via Amendment 16 (1995).

As stated earlier, the legal mandate for API and the power to prevent an individual from boarding a flight is drawn from UNSC resolution 1373 (2001)[10], followed by amendments, clarifications, and expansion of scope via 2178 (2014)[11], 2309 (2016)[12], 2322 (2016)[13], and 2396 (2017)[14]. The authority to make these applicable to UN Member States, and therefore ICAO Member States, is based on the power vested in the United Nations Security Council (UNSC) via article 39 of chapter VII of the UN Charter. How this is to be implemented depends on the member countries; a national law for the purpose has been recommended. However, each country must have a Passenger Information Unit (PIU) and these already have an interoperable data interchange system connected to airports.

Like API, which is initiated when a passenger checks in to a flight, a framework has also been envisaged for the passenger name record (PNR) which has a much longer trail, starting with the purchase of a ticket as well as any other related transactions that might include car hire and hotel reservation, and therefore has a wider footprint of an individual identity.

The powers of the UNSC to legislate and the implications of international legislation have been actively discussed in recent years. A significant paper on this subject has been written

[9] https://www.icao.int/Security/FAL/Pages/Annex9.aspx
[10] Ibid. UNSC meeting 4385, refer above.
[11] https://www.jstor.org/stable/10.2979/indjglolegstu.24.1.0309?seq=1#page_scan_tab_contents
[12] https://www.un.org/press/en/2016/sc12529.doc.htm
[13] https://www.un.org/counterterrorism/ctitf/en/sres2322
[14] https://digitallibrary.un.org/record/1327675?ln=en

by Stefan Talmon[15]. Other reference material can also be found (cf. Jane E. Stromseth and others)[16] and is of interest.

Over four billion passengers embark on a flight annually. While many flights might be made by the same individual, it represents the fact that an astonishing half the world's population can be moved annually around the globe, if required.

More than a billion people in about 140 countries hold the latest generation of electronic passports (eMRTDs) worldwide that enables them to travel across national borders. As described earlier, the eMRTD is a robust document that has become increasingly difficult to fake or copy. With this, the once thriving industry of counterfeit travel documents has been reduced to a trickle, and the focus has shifted to persons assuming false identities to obtain genuine travel documents. This has exposed obvious weaknesses in how MRTDs are linked to national identification systems. The authorities have had to shift their attention to evidence of identity (EoI), and this brings the MRTD's relation to breeder documents and national identity documents into sharp focus.

In practical terms this means that at the time of an MRTD application (especially the first time), a more thorough examination is made of breeder documents such as the birth certificate. However, this poses challenges such as establishing authenticity, which often falls back on the process of attestation, or the passport issuing authority needing to consult the birth registration authority. If the birth certificate is issued by an indirect authority such as a school principal, this leads to further difficulties. It has been stressed that death records also be checked before issuing an MRTD to ensure that a dead person's identity is not stolen for the purpose.

To overcome such limitations, passport issuing authorities have put other supporting and reinforcing processes in place, such as checking the individual's *social footprint*[17]: the trace of an individual's existence that can be pieced together by looking at, for example, educational records, employment records, addresses, utility bills, and bank statements. Every State could devise its own methodology for the purpose. This is another example of an empirical process supporting a normative one.

Digital Identity, increasing overlap, and overdependence on encryption

Another topic where national and international identification converge is digital identity. The World Bank's identification for development program (ID4D)[18] and inter alia other UN bodies recommend a digital identification framework. Similarly, MRTD standards bodies are already discussing a digital travel credential (DTC). There are parallel discussions at the various ISO bodies for other identification documents such as driver's licenses. The standardization

[15] THE SECURITY COUNCIL AS WORLD LEGISLATURE By Stefan Talmon, 2005, University Lecturer in Public International Law and Tutorial Fellow, St. Anne's College, University of Oxford.
[16] Georgetown University Law Center, 2003. Scholarship @ GEORGETOWN LAW. Jane E. Stromseth. This paper can be downloaded for free from: http://scholarship.law.georgetown.edu/facpub/1686
[17] This is not to be confused with the use of the term in the context of environmental studies, where social footprint has come to mean the spread of one's carbon footprint as a consequence of one's social interactions.
[18] http://id4d.worldbank.org/research

extends to technologies, devices, electronics, and software. Finally, a cross-functional standards body on "virtual identity" has recently been initiated[19].

Technical standardization is often done in isolation, with little attention to its impact on the associated legal framework (and vice versa). It is assumed that good technological innovation will find a place in the legal world too. So often, the actual harmonization between the two is through an ad hoc patchwork of amendments, ordinances, and gazette orders. These often sit on top of Acts that were formulated many decades ago, or even borrowed from the colonial era. Conversely, there is also patchwork implementation of changes on technical standards to accommodate an existing legal framework. However, recent work on the DTC has involved two simultaneously constituted committees, one for policy and one technical, that work in tandem. One of the first issues to have engaged the two in lively discussion is how a DTC may originate (from the MRTD?), who can issue it (the original issuer?), and who could store, transmit and use the digital record. Such detailed discussion is yet to pick up momentum for civil (national) identification systems and even more so for civil registration.

While nothing might change immediately (moving from hand-written passports to MRTDs took twenty years), constant evolution is expected as the function of API increasingly overlaps with that of the DTC and the electronic Visa that of API. Despite each of them taking on entirely new forms, they are likely to continue serving their existing functions well into the foreseeable future.

This is somewhat like the transformation in electronic payments from card to digital, where currently both coexist seamlessly, and most account holders transact using cards as well as on the internet without feeling the difference.

For identification, it is anticipated that both phenomena will persist—a stepwise transformation in the document mode, agency, privacy, and ownership. At the same time, there might be systems that will directly debut into the digital era, like Aadhaar.

There is no doubt that going digital involves significant (if not overdue) dependence on encryption and decryption (via deployment of public and private keys, for example). Supposed solutions such as the blockchain too heavily depend on encryption. In general, principles of encryption have remained the same over many decades (most of the work on RSA was published by 1977). However, its implementation parameters, such as the key length, have had to keep pace with faster computing capacities, which still continue to double every few years. The first of the new-generation hyper-fast and hyper-capacity computers that use *quantum computing* are already in use. It has been expected that this technology would make current encryption practices obsolete[20]. However, recent research[21] has been more optimistic, and encryption is likely to endure well into the future. At the same time, break-ins are disturbingly frequent, not only by insiders and rogue entities, but via systematic State interference as well[22].

[19] ISO/IEC JTC 1/SC 17/SG 2 - Virtual ID and related technologies.
[20] https://www.cryptomathic.com/news-events/blog/quantum-computing-and-its-impact-on-cryptography
[21] https://techbeacon.com/security/waiting-quantum-computing-why-encryption-has-nothing-worry-about
[22] https://www.information-age.com/nation-state-hacking-long-history-123464181/

It must be noted that eMRTDs continue to be protected and their authenticity validated using a Public Key Infrastructure (PKI).

The broader identity situation

The broader identity situation for an individual in daily life is diverse. It covers governments, institutions, companies, associations, clubs, and social media, among others. Looking at just the government requirements, it could require considerable effort to conclusively establish how these could be made compatible with one another.

Let us take the example of biometrics. Are the biometrics of a civil identification system and an MRTD compatible? If the modes are different, fingerprint and face for example, compatibility would not even be feasible. Even if the mode is the same, the biometrics might still be incompatible due to a variety of reasons, both technical and commercial.

Equally important, it might happen that a country's legal framework does not provide for biometrics under one system but allows for them under another. This is legal incompatibility. There could also be operational, organizational, and administrative incompatibilities.

Similar considerations apply for the biographic details of a person. These are currently the center of much debate, also in part due to the dynamics unleashed by current political trends in some parts of the world.

Current problems in biographics

In some sense, biographics is a loose term applied to the textual details pertaining to an individual identity. It might include names (surnames/family names, first names, middle names, aliases and variations) as well as allied details such as sex, date of birth, place of birth, and in many cases, address.

MRTDs need to cater to the diverse name and surname conventions across ICAO's 192 Member States and hence to a somewhat generic data structure. However, individual Member States might have their own, more specific data structures and even regional variations. These do not automatically map onto one another and thus require manual intervention. This problem has been especially compounded by the advent of the API system, which compares names in MRTDs against names in watchlists. In many cases where the system failed to apprehend likely suspects, this can be attributed to name mismatch. An institutional mechanism is likely to be set up soon to address this issue.

The two bodies that exert often opposing pulls on such issues are ICAO[23] and the International Air Transport Association (IATA). The former is responsible for security and national border integrity, and the latter for the commercial interests of an industry group that is approaching USD one trillion annually (airlines alone are 800 billion). ICAO wishes to

[23] Reference is also made to WCO (World Customs Organization) that regulates cross-border commerce via all modes of transport: air, sea and land. WCO is also the custodian of the API regulation for this reason. Please refer http://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/api-pnr.aspx

ensure that not a single one of the four billion annual border crossings pose a threat to any of its Member States. However, IATA wish to ensure that the existing expensive infrastructure (runways, airports, and airplanes among others) are more optimally utilized.

Issues around gender

One of the issues that erupts sporadically in various States is the signification of an individual's sex or gender. This is causing conflict in the record keeping (impact of difference in current sex status vis-à-vis at birth) and has required the intervention of courts. Currently, States do not agree on a common globally acceptable strategy. In some States, individuals have gone to court citing declaration of sex or gender as a privacy issue. However, this often has implications for other stakeholders, that include even data architects and border police. API for example uses sex as a search parameter. At the same time, there is a move in some countries for sex to be optional information on an MRTD.

Recent spurt in the use of mononyms

As reported at the end of 2018[24], there has been a perceptible increase in the use of mononyms in MRTDs (I am John in lieu of John Goldsmith and I am Kabir and not Kabir Ahmed). Early analysis has shown that this is more predominant in countries that are potential sources of immigrants and in countries that are reinforcing their policies regarding caste, class, religion, ethnicity, and other factors related to identity. Somehow names embed such information and it can be provisionally concluded that adverse policies are leading to such strategies. These further compounds the MRTD-to-watchlist matching problem for API.

Why is the name important?

Systems like the API have immense stakes in international security and thus carry enormous weight to influence the rules of national civil identification and even civil registration systems. Already ICAO envisions as part of its evidence of identity (EoI) strategy that MRTD issuance be more closely linked to civil registration systems, for example. This might happen even before birth registration achieves its universality as envisaged under SDG 16.9. There are no answers as to how an MRTD might be issued to a person who has no birth registration record, and what would be the final arbitration of a name in such cases.

At the local level and outside the context of the MRTD, such situations already occur. Zimbabwe nationals who immigrate to South Africa for work find it easier to do so by changing their names altogether, from ones that might reveal their *Ndebele* origin to common *Venda* names that are more readily accepted as South African. Similarly, in India individuals often switch to caste-neutral surnames or name suffixes such as *Kumar.*

[24] https://www.icao.int/Meetings/TRIP-Symposium-2018/Documents/RAADGERS.pdf. Please note: FNU stands for First Name Unknown and LNU for Last Name Unknown.

Is this a problem that can be resolved in some practical way? The reasons for altering a name can be seen to fall into two major categories: first, security and second, removing possible difficulties in migration, whether economic or humanitarian.

Linking various identification systems

There are obvious advantages to maintaining a link among identification records pertaining to the same individual in the various systems. While it is a topic of another discussion, it does not seem a good idea to fuse all the identification databases together, simply for the practical difficulties it might cause: among those born in the country are residents, nationals, eligible to vote, etc. The primary difficulty here is how the multiple ownership of such issues can be managed in a coherent manner.

In the realm of technology, two approaches—hierarchical and network-based—can help resolve conflict. It is important to understand how these approaches might work and what impact these would have on the arrangement of the various identification systems with respect to one another.

Privacy is another issue that tends to hold back the linking of diverse identification systems on the grounds that it prevents or at least inhibits the power that such systems could impart to a surveillance state or a totalitarian state.

Yet another aspect is the dichotomy between legal and physical identity. Further, legal identity itself needs to address two separate notions, that of the natural person and the legal person.

As all three aspects are so central to the identification narrative, it is important to revisit the reasons why they are there in the first place. It also helps assess whether the mutual impact of the various identification systems is fundamental in nature or only incidental, and inter alia whether each system can resolve issues without causing an irretrievable conflict or breakdown in another.

Legal and philosophical basis of privacy

Going beyond the fact that many countries have enacted privacy laws and others are in the process of doing so, it is equally important to look at the underlying basis for the emerging legal framework and stepping back a little more to look at the philosophical basis of privacy.

The essential modern discussion[25] on the public and the private spheres and privacy itself is found in the Enlightenment philosophers, such as Locke, Mill, and Kant. Also, the evolution of privacy law has been different in the common law and civil law traditions. It is also important to read the works of later philosophers who have given shape to privacy in the information age, and this includes Richard Posner (privacy as a commodity) and Luciano Floridi (information and privacy). Ironically, philosophers attempting to broaden the understanding and extend the meaning and justification of privacy have also reexamined the work of Spinoza (ontology and adequate knowledge) in recent years.

[25] Janice Richardson, Law and the Philosophy of Privacy, Routledge, London & New York, 2016.

Privacy as an issue in common law probably first appeared in an 1890 article in the *Harvard Law Review* (Warren and Brandeis) which stated that tort law could be invoked, and individuals could sue to protect their privacy. The issue then too was technology, related to the use of the newly invented Kodak camera that provided an easy means for so-called yellow journalism.

However, on the continental side, privacy evolved out of progressive decoupling between contract law and the Christian tradition. Especially for marriage, even the Napoleonic code maintained a firm connection between holy sacrament and contract that continued to marginalize women. This list is by no means complete and involves scores of other scholars who have addressed the subject of privacy from various angles.

The fact that marital rape was first criminalized only around the 1970s[26] reflects this asymmetry. Besides to gender, such discussions have also been extended to class and race as well as for the individual as an employee, consumer, and citizen, demonstrating the close relationship between privacy and inequality.

In this light, what are the alternatives? On the one hand, both technology and law must make it impossible for identification information to be shared. Its commodification may only be extended to the individual, who might choose to share it and in the capitalist age, be its sole and rightful beneficiary. On the other hand, as in Iceland, all identification-related data could be made uniformly public by using a publicly known personal identification number (Kennitala). In such a situation, identification data attracts no premium. However, all strategies in between are imperfect solutions that can either be exploited by the State or its representatives for rent seeking, or by the individual to derive unfair advantage.

Luciano Floridi, a contemporary contributor to this subject (2006 onwards) characterizes human beings as informational animals (as opposed to rational, political, or symbolic animals) that coexist with artificial intelligence in a singular infosphere. Such a concept helps us re-frame the identity of an individual through the various means described above, that is: the uniqueness of the body itself via biometrics (locus), corroboration of vital events and the social footprint (time dimension), and finally travel (space dimension). Somehow, these also represent the body, mind, and consciousness of an individual and even though somewhat composite, seem to provide a coherent model of an identity. Depending on particular use, specific aspects of all this could be deployed.

To conclude this section, we come back to why Richardson recommends a re-look at Spinoza. Kant, Locke, and Mill (drawing upon Descartes) base their identity model on the classical mind-body dualism which sets off epistemological arguments such as what is more "primary", birth registration or civil identification (mind or body). Spinoza provides a continuum across both and also imagines identity to be ontological instead. The actual arguments are long-winded as philosophical arguments tend to be and there are the usual references not stated here.

On privacy, three and a half centuries ago, Spinoza foresaw what we have encountered today in the informational age. Some elements of identity will need to be private, and others could well be public. This is especially highlighted in the sporadic discussion around the complex issue of public disclosure of unique identification numbers (UINs). The UIN itself is

[26] Except for the Soviet Union, which passed a law in 1922 that was sustained by some of the socialist bloc countries even after the break-up.

not the carrier of private information. In earlier times, it would lead you to paper records that actually hold the private information. Today, the UIN will need to be accompanied by a biometric (as in Aadhaar) or by an identification card (as in US Social Security).

What must remain private and what can be public with respect to identity and identification data? Perhaps this needs to be further debated and researched. Also, the way privacy is transacted may need to be reviewed. A closer look at online notice and consent forms, for example, as Richardson explains, has prompted opinions that, "these function as a behavioral technique in a neo-liberal setting, in which privacy as a commodity is exchanged". This has even been the way forward for enforcing the EU's General Data Protection Regulation (GDPR) especially for organizations and States. How well these protect the individual is still to be tested.

Conclusion

To conclude, it seems useful to look at the national as well as international context of identity together as one single continuum. No doubt, the multiple systems (civil registration, identification, and MRTDs) will need to coexist in a composite model due to their mutually exclusive nature, akin to dimensions of space and time. However, this might have both foreseen and unexpected consequences. Some of these are described below.

Biographic data of the same individual may continue to differ, and these differences will need to be properly noted, especially when names of the same individual are not identical. Also, while States continue to grapple with sex and gender indicators in their wider context, this subject too might continue to cause confusion. This will require effort at the national level, to harmonize between civil registration and identification for example, and at the international level, where all States will need to first recognize and then set out to find a common framework to address the same. Both names and gender are culturally sensitive, which can put them at odds with digital identity solutions, which look for binaries and objective categories. Finding common ground continues to be challenging.

Given these shortcomings in biographics, biometrics will continue to become more important and offer the objectivity that systems require. Thus, commensurate analysis is required of the problems that identity and identification systems set out to address, and whether biometrics can effectively contribute to this. Some of the current pilot trials, like the Happy Flow[27] project for airports, make it possible for individuals to be identified entirely through face recognition, with no other documentation or process required for airport entry, check-in, baggage, security check, immigration and boarding at departure, and similar processes at arrival.

The move towards digital identity makes more systems look like one another or capable of offering each other's functionality, as shown in the example of the DTC, eVisa, and API. Thus, more systems will tend to collapse and fuse into one another. However, this poses other problems, two of which are extremely important: privacy and ownership. Some paradoxical situations might arise, like the same data being private in one system (civil identification) and public in another (electoral roll).

[27] https://news.schiphol.com/aruba-happy-flow-pilot-project-a-complete-success/

In defense of multiple systems, it can be said that these should address as many diverse aspects of an individual as possible and avoid stereotyping as well. This excerpt of a review of "Identity and violence: the illusion of destiny" by Amartya Sen[28] sums up the identity problem of our time:

In this penetrating book, Nobel Laureate Amartya Sen argues that we are becoming increasingly divided along lines of religion and culture, ignoring the many other ways in which people see themselves, from class and profession to morals and politics. When we are put into narrow categories the importance of human life becomes lost.

Through his lucid exploration of such subjects as multiculturalism, fundamentalism, terrorism and globalization, he brings out the need for a clear-headed understanding of human freedom and a constructive public voice in Global civil society. The hope of harmony in today's world lies in a clearer understanding of our sheer diversity.

Identity systems therefore, above all, must help preserve diversity.

Not everyone will be virtuous in using identity and identification data. Not only the State, but even the markets provide extreme examples such as racial profiling (through using family names, address, etc.) for real estate sales strategies. The importance of this example is that this calls for regulation in the *use* of identification data and not the data itself.

Finally, it is meaningful to examine the original objective that we set out with. An individual is extremely vulnerable before the powers of the State and the corporation. Every process tends to create further asymmetry of information. Where does the individual stand then and how can identity and identification systems support her?

The plethora of systems that an individual encounters throughout her life needs to be confronted together and not in isolation. Unfortunately, today there is no mechanism that enables this. National and international stakeholders have virtually no interoperability on the subject. Power is always at play in the constitution of "who we are" and unless there is proactive action on this front, this constitutive ability that needs to be deployed to create a more equitable interdependence will not lead to the imagined greater autonomy for the individual.

As shown by the advent of API, all such constructive initiatives can be thwarted, and the individual placed at the vagaries of a poorly performing algorithm that could impact her national identification record of a lifetime.

A first step in the right direction is to look at all this together, preclude hierarchy and tolerate diversity, because her best chance is in manifesting her inner and outer self effectively, and in as many ways possible.

[28] https://www.penguin.co.uk/books/558/55882/identity-and-violence/9780141027807.html