COMMENT

On Ethiopia's Digital ID Bill, Data Privacy, Warts and All

DOI http://dx.doi.org/10.4314/mlr.v16i2.8

Kinfe Yilma ♣

Abstract

Ethiopia has been considering a Digital Identification legislation in the past few years. This comment offers a critical analysis of the legislative proposal with a focus on three aspects of the Bill. First, it analyzes the extent to which the Draft Digital Identification Proclamation attends to data privacy concerns associated with digital identification systems. Second, it considers the Bill's approach to the risks of digital exclusion or discrimination that are common in systems of digital identification. Finally, the comment discusses major areas of normative ambiguities that would undermine the effective implementation of the Bill upon its enactment. The submission is that the Bill requires substantial revision before adoption by the legislature.

Key terms

Digital ID · Data privacy · Digital exclusion · Legal drafting · Ethiopia

Suggested citation:

Kinfe Yilma (2022). "On Ethiopia's Digital ID Bill, Data Privacy, Warts and All", 16(2) *Mizan Law Review*: 455-466.

Contents

♣ Kinfe Yilma (PhD), Assistant professor of law, Addis Ababa University.
Email: <kinfeyilma@gmail.com>
ORCID: https://orcid.org/0000-0003-2514-0491

[1] This comment is based on the English version of the Digital ID Bill published on the website of the National ID Program available at: https://id.gov.et/digital-draft-id-law-english-translation-2/

1. Introduction

Ethiopia's most recent 'digital' legislative initiative is the Draft Digital Identification Proclamation (hereinafter, Digital ID Bill or Bill) which has recently been presented to the federal Parliament for consideration. In late October 2022, the Parliament referred the Bill to the relevant standing committees for closer scrutiny.[2] The Bill seeks to achieve a series of objectives, including enabling efficient provision of public services, effective national development planning, and combating crimes committed with the help of multiple identities. Upon its enactment as a proclamation by the House of Peoples' Representatives, the Bill will displace parts of the Registration of Vital Events and National Identity Card Proclamation (hereinafter Proclamation No 760/2012 or ID Card Law).

A notable departure from the existing legislation –i.e., Proclamation No 760/2012– is that the Digital ID Bill envisions identification of individuals as a matter of *right*: a 'right to identity' or a 'right to be identified' [See Art 6 *cum* Preamble]. Indeed, provision of Digital ID is envisioned as a solemn duty of the Ethiopian Digital Identification Institute, a body responsible for the administration of the identification system [hereinafter, the Institute; see, e.g., Art 5)].

In contrast, obtaining a national ID is a duty under the ID Card Law, and failing to do so may lead to liability [See Art 56]. The Bill states that upholding the right of Ethiopian citizens and residents is one of its *raison d'etre*. But this is negated by another provision in the Bill which provides that government or private entities may condition provision of services on possession of digital identity [See Art 11(2) *cum* Art 18(13)]. Moreover, if the provision of a public or private service relies on biometric verification, possession of digital identity will be mandatory.

With digitization of more and more services, possession of digital identity will be more of a duty than a right. In that sense, the notion of a right to identity appears to be an empty promise. As shall be noted later in this comment, the statutory requirements for acquiring a digital ID may be cumbersome or downright impossible to fulfil for certain individuals.

Perhaps another notable departure concerns *scope*. Proclamation No 760/2012 applies only to Ethiopian citizens [See Art 3]. That means aliens but lawfully residing in the country are exempted from the duty to obtain a national ID card. But this changes in the Digital ID Bill which will apply to

[2] Ethiopian Digital ID Draft Law Tabled in Parliament (Ethiopian Monitor, 21 October 2022) <https://bit.ly/3jAb4Gv>.

'anyone residing in Ethiopia' –i.e., to both citizens and residents [See Art 3]. This commentary discusses aspects of the Bill with a particular focus on issues relating to data privacy, digital exclusion and drafting missteps.

2. Data Privacy-protective Provisions in the Bill

Digital identification raises privacy concerns as the procedure involves the routine collection, processing, retention –and at times, sharing– of personal data. One can thus readily see that data privacy has been a concern for the drafters of the Digital ID Bill. Yet, the concern does not seem to be adequate. Part V of the Bill –captioned 'Digital Identification, Data Security and Protection of Personal Information'– has provisions offering some baseline data privacy safeguards. At the highest level, the Bill mandates that Digital ID-related data should be kept in secure systems, protected from loss or damage. To that effect, the Institute is required to put in place technical and procedural safeguards [See Art 17].

One should note here, however, the rather vague duty of the Institute to employ a 'strong' information management system, while what makes a system 'strong' [in Art 13(1)] remains unclear. An interesting clause is the requirement that technical protection measures should be commensurate with the legal safeguards [See Art 17(4)]. However, it is not entirely clear what those legal safeguards are –is it a reference to a future data protection law which would embody data privacy principles, data subject rights and governance norms? The clause appears to mandate the so-called 'privacy by design' by which privacy safeguards are baked into technical designs. But there is still a need to bring more clarity to the provision to ease its future application.

Furthermore, the Digital ID Bill provides specific privacy-protective standards highlighted below.

2.1 Data minimization: Data necessary to identify an individual

Reflective of the principle of data minimization, it requires that only data needed for the functioning of the identification system –i.e., data necessary to identify an individual digitally– should be collected [See Art 18(2)]. The Bill further enumerates the type of personal data that should be furnished in the process of registration in the ID system: name(s), data of birth, gender, place of residence, nationality –and in certain cases, phone number and email address of registrants [See Art 7].

Data minimization means that the Institute would not be able to collect other types of personal data, including sensitive personal data like a registrant's religion and ethnicity. Not only are the latter types of sensitive

personal data required in the current legislation –i.e., Proclamation No 760/2016, but also that the ID issuing federal entity can require 'other necessary information' if need be [Art 57(2)]. In current practice, local administrative units in Addis Ababa collect such data which, although not printed in the ID card issued to individuals, are recorded in databases.

Perhaps, this is one area where the Bill moves away from the rather problematic provision of existing law. But there is another provision in the Digital ID Bill where this progressive standard appears to be reversed. Article 16 indicates information that would be displayed in the physical ID cards to be issued to registrants, which may include 'any other information that shall be collected in accordance with subsequent directives' [See also Art 22(M)]. What this clause suggests is that the Institute could by a Directive expand the type of personal data that may be collected and processed in the course of Digital ID registration.

If such a future Directive were to allow registration in the database –and then in the ID card– sensitive personal data like religion and ethnicity, it will not just be reinforcement of current practice but also even worse. As alluded to above, ID cards issued by local administrative units, at least in Addis Ababa, involve collection of religion and ethnicity but those data will not appear in the physical ID cards.

2.2 Prohibition of sharing personal data

The Bill prohibits sharing of personal data to other entities without the 'permission' of the data subject [See Art 18(5) cum Art 18(14)]. Earlier versions of the Bill used the rather common notion of 'consent'. The term 'permission' is defined in the Bill as 'consent given by an individual for their information to be processed for known purposes solely based on the individual's own will' [See Art 2(16)]. In that sense, permission somehow represents consent for purposes of the Bill.

Third parties such as law enforcement and intelligence agencies are also prohibited from collecting, disclosing, distributing, printing, using or transferring data without the permission of the data subject [See Art 18(4)]. However, the framing of this clause is quite vague, and a question can arise whether it means that law enforcement agencies are totally banned, even with court warrant, to seek access to personal data stored in the digital ID system. But this is not necessarily a privacy-protective approach. We return to this point later.

An earlier version of the Bill even banned onward sharing or storage by those entities to whom the data has been transferred with the permission of the data subject [See Art 22(7)]. Existing law prohibits onward transfer of the data to third parties or its repurposing, but it does not prohibit storage by

entities to whom the data was shared [Art 64(2)]. It appears that the Bill is prohibiting third parties such as the Police who secured the data with the permission of the data subject from further disclosing it to other parties. In that sense, the Bill has another progressive privacy-protective clause.

2.3 Anonymized personal data and access upon court order

Personal data of (un)consenting individuals may be shared with other entities only where it has been anonymised and that the entities are legally allowed to seek or receive the data [See Art 18(6)]. One notes in this regard how the 'consent' of the data subject is given higher weight in the Bill. Other common legitimate bases of data personal processing –including sharing of personal data, for example, to law enforcement and intelligence agencies– without the consent of data subjects, are not recognized in the Digital ID Bill.

This stands in stark contrast with Proclamation No 760/2012 which not only allows sharing for purposes of law enforcement, intelligence, administrative and social services as well as 'implementation of risk management systems of financial institutions' but also that data may be shared with third parties upon court order [Art 64(1), Art 64(3)]. That simply means a court will not, under the Digital ID Bill, be able to order disclosure or sharing of de-anonymized and de-aggregated personal data needed, for instance, to investigate crimes.

This may be taken to be a privacy-oriented policy choice on the part of the drafters, but it is not necessarily the right choice. There should be a mechanism by which relevant authorities such as the Police may be able to obtain data based on a duly obtained judicial warrant. That way, courts will be incumbent upon to properly balance privacy and other competing values before issuing or denying warrants.

In the absence of such mechanisms, law enforcement and intelligence agencies may resort to other extra-legal or illegal means of obtaining the data. An extra-legal avenue may be efforts by heads of law enforcement and intelligence agencies to force or persuade the heads of the future Institute –who would be appointed by, accountable to and be removed by the Prime Minister–to furnish the data without any independent oversight [See Draft Council of Ministers Regulation Establishing the Ethiopian Digital Identification Commission,[3] now renamed as Institute].

Alternatively, intelligence agencies may resort to hacking –which would generally be unlawful– to secure the data. To prevent such counter-productive outcomes, relevant authorities should be allowed to seek court order for the production of data held in ID databases where data subjects deny permission.

[3] Available at <https://bit.ly/3idTuaX>.

As alluded to above, the Bill purports to repeal the ID Card Law rather vaguely. Article 64 of the Proclamation, which sets out circumstances of disclosure to third parties, including law enforcement and intelligence agencies, is not explicitly revoked. If that is the case, the above highlighted concern might be mitigated as Article 64 would continue to apply. But of course, there is the need for clarity in this regard. How a confidentiality exemption clause in the Bill may be interpreted to allow disclosure is further discussed below.

3. Some Observations on the Bill's Data Privacy Clauses

What have been highlighted (in Section 2 above) are the main privacy-protective provisions in the Bill. But the relationship between the Bill's privacy clauses and a future data protection law is not quite straightforward. An earlier version of the Bill had a provision which stated that once Ethiopia adopts a data protection law proper, the privacy rules in the Bill would cease to apply [See Art 22(9)]. Ethiopia has no data protection legislation, but several Bills have emerged in the past decade including the latest Bill drafted in 2020. And, there is no certainty when the Parliament will adopt data protection legislation. But the concern was that the privacy provisions in that version of the Bill did not provide much safeguards. Hypothetically speaking, protection of data privacy would have remained circumscribed until the data protection bill is enacted.

With this clause now removed from the current version of the Bill, the interplay between a future data protection legislation and Bill's privacy clause becomes even more unclear. In the provision where the Digital ID Bill addresses 'revoked laws', Article Art 21(2) reads: 'any law or procedure or practice shall not prevail over the affairs covered by this Proclamation'. Perhaps, what the drafters hoped to convey in this clause concerns current legislation, but will it apply to future legislation which comes into force before or after the Digital ID Bill? If so, would it mean a future data protection law will not apply when it comes to processing of personal data relating to digital ID? If the answer is in the affirmative, it can be problematic. That is mainly because the Digital ID Bill does not offer much data privacy safeguards, as alluded to above. Indeed, it embodies privacy notions that do not exist in Proclamation No 760/2012. For instance, it offers a definition of key terms

such as 'permission' –albeit, in a slightly vague manner[4]– which is missing in the existing ID legislation.

The current law speaks of 'information specific to an individual' –which might be taken to mean 'personal data'– but no formal definition of personal or biometric data is provided [See Art 64(3-4)]. Moreover, the Bill falls sharply short when it comes to embodying central aspects of data protection legislation. One example is that it does not offer a definition of 'personal data' or 'sensitive personal data'. Although it defines aspects of personal data, particularly 'biometric data', this is not adequate as acquiring Digital ID would require the collection and process of other types of personal data. That said, what the Bill calls 'enrollee information' –i.e., information recorded in the digital ID system, including biometric data– essentially captures the notion of personal data [See Art 2(15)]. However, there appears to be no reason to introduce a rather odd concept in lieu of using the rather common terminology of personal data.

A problematic provision embodied in the Digital ID Bill concerns the notion that data subjects 'own' their personal data collected and used as part of the digital ID system. The current English version of the Bill does not, as such, use the term ownership, which explicitly was mentioned in its earlier version [See Art 22(3)]. But the Amharic text in the latest version still adopts the notion of data ownership. The English and Amharic versions of Article 18(3) read:

> *The subject of the information* collected for the Digital Identification System is the individual themselves; therefore, any verification processes should be done under the permission of the individual. [Emphasis Added]
>
> **በዲጂታል መታወቂያ ሥርዓት የተሰበሰበ ማንኛውም የተመዘጋቢ ግላዊ መረጃ <u>ባለቤት</u> ተመዘጋቢው በመሆኑ፣ በማንኛውም የዲጂታል መታወቂያ አሠራር ሥርዓት ውስጥ አገልግሎቶችን ለማግኘት የሚደረጉ የማረጋገጥ ተግባራት በተመዘጋቢው ፈቃድ ብቻ ሊደረጉ ይችላሉ።** [Emphasis Added]

The word 'subject' is used as '**ባለቤት**' in Amharic. It is to be noted that the Amharic word '**ባለቤት**' may mean 'owner' or 'subject' depending of context of its usage. The word '**ባለቤት**' in Article 18(3) of the Digital ID Bill means 'referred to/what it is about' as in the case of the grammatical reference to 'subject/**ባለቤት**' and object/ **ተሳቢ**'. There is thus the need for clarity in the

[4] The definition of permission does not, for instance, mention whether the consent is one that could be withdrawn at a later stage nor is it clear what one's 'own good will' means. See Id, Art 2(16).

definition of '**ባለቤት**' to avoid the idea of 'data ownership' based on the literal reading of the words which can be a cause for concern.

This should be considered in the light of how –as alluded to above– the Bill envisions consent, or rather 'permission', as the sole basis of processing of personal data. It is now widely accepted that ownership, which inherently carries the right to alienate the data for consideration or otherwise, is a deeply flawed concept in data privacy discourse. At its core, not only that it would lead to loss of control or autonomy over personal data in exchange for meagre 'data price' which often comes in the façade of 'free' services. What data protection legislation essentially does is enable data subjects control their personal data through bureaucratic regulatory processes. That is an area where Proclamation No 760/2012 perhaps embodies a sensible provision which is sharply opposed to the notion of data ownership, and it refers to consent as the sole basis for the lawful processing of personal data.

Article 64(5) of the ID Card Law provides that disclosure of personal data to third parties may be denied even when there is the consent of the data subject where the impugned disclosure would undermine 'public interest'. While data privacy is an individual right, there is arguably a sound public interest in its protection. That 'permission' or consent is defined so ambiguously means data subjects are likely to give permission for disclosure of their personal data, be it under deception or duress. That makes disclosure prohibitions grounded on public interest, questions of what public interest and according to whom regardless sensible. More so, in countries like Ethiopia where digital literacy is too low and state-sanctioned coercion is too common.

Finally, a rather generic rule in the Digital ID Bill envisages an exception to the requirement that data collected and processed as part of registration should be kept confidentially [Art 18(1)]. Under circumstances prescribed in the Ethiopian Constitution and international instruments ratified by Ethiopia, data held in the system may be disclosed to third parties regardless of data subject consent. One way to make sense of this clause is from the perspective of permissible restrictions under the right to privacy. Article 26 of the Ethiopian Constitution guarantees the right to privacy which may be restricted when the requirements of legality, necessity and legitimacy are met.

The same principle applies in international human rights instruments such as the International Covenant on Civil and political Rights (ICCPR). Should data retained in the Digital ID system be needed for purposes of, say, criminal investigation, the Police could rely upon a law that authorizes disclosure for such purposes to seek disclosure through formal court process. In such cases, the consent or permission of the data subject will not be necessary. Such

plausible interpretations aside, there is a need for clear rules governing lawful disclosure of personal data.

4. Digital Discrimination/Exclusion

A common concern associated with Digital ID systems is the risk of exclusion and discrimination. Individuals who are unable to furnish information or documentation to prove their identity may be denied Digital ID and hence access to key public services. The Bill provides a hint of basic identification tools that would be used for the issuance of Digital ID. Article 7(1) reads:

> [The Ethiopian Digital Identification Institute] shall […] register the individual based on documents that verify individual identification, residence, address, or based on other legally accepted documents, or by human testimonials.

Beside documentation supporting the claimed identity of the individual, testimonials may be used to obtain digital ID. That means individuals without other ID documents such as passports would be able to obtain Digital ID. In that sense, it may reduce the risk of excluding such individuals. But the proviso is framed in a form of discretion to the Institute in that it may be able to deny digital ID where, for instance, the person fails to adduce enough number of witnesses/testimonials or the testimonials appear to be suspicious.

Considering that Digital ID is envisioned as a basis for other types of identification [See Art 6(8)], the discretionary power of the Institute may result in an exclusionary digital ID regime. In a way, this concern is partly addressed by a provision tucked away in parts of the Bill dealing with 'information required in special cases' [See Art 5(B)] where it is provided that presenting one witness who already possesses a Digital ID would suffice when adducing other documentation is impossible. A persistent concern, however, is when the person is unable to present a witness with a digital ID. Similar concern arises regarding the requirement that a minor cannot be registered except through a parent or guardian who already possesses a digital ID [See Art 5(A)]. What if the minor is a child of a migrant, refugee or stateless person who has no Ethiopian Digital ID?

Not entirely clear is also whether the Institute or the body to which its functions may be delegated could reject witnesses present, and under what circumstances. Such points require clarification. Another related concern is that the task of running the Digital ID system may be delegated by the Institute to third parties through a licensing regime [See, e.g., Art 6(9)]. With privatization of a public service, the risk of discrimination and exclusion could be even more pronounced. What this, then, calls for is clarity in subsidiary legislation, especially regarding the circumstances where human testimonials

are permitted and how, thereby circumscribing the discretion of the Institute or its delegate.

5. Drafting Missteps

The question of whether the Bill is necessary or will it ever be effective in practice aside, a closer look at the Bill reveals a myriad of drafting missteps. One relates to the ambiguous way in which the Bill repeals Proclamation No 760/2012. Article 21 of the Bill provides that Arts 55-62 and 'other provisions that pertain to national identification and covered under this proclamation are revoked'. It is not clear whether the latter limb of the provision refers to Articles 63-66 of Proclamation No 760/2012 which deal with themes directly related to data collected in the course of issuing a national ID. Article 64, for instance, sets forth an illustrative list of circumstances justifying disclosure of data to 'other organs' –which might include private as well as public organs. Article 65 requires ID-related information to be protected from breaches or other forms of loss whereas a series of punitive provisions are provided in Article 66. Would the Bill repeal the latter provisions as well once it enters into force?[5]

Other aspects of the drafting oversight concern the way in which certain notions are thrown in with little clarity. This relates particularly to certain bodies envisaged in the Bill: relying parties, client bodies and collaborating entities. What regulatory role that these bodies assume is not entirely clear. Nowhere in the Bill is the meaning and nature of 'collaborating entities' explained. In a provision where they are referred to –i.e., Art 6(5)– they appear to be entities that may run digital ID systems. It is not clear whether these bodies include employers who often have internal systems by which IDs are provided to employees.

Regarding 'relying parties' for instance, it is not straightforward whether these entities are envisioned as providers of identity verification services. Article 12(3) states that they 'need to get permission from the Institute before they *receive* verification services' while preceding sub-articles suggest that these bodies indeed are verification service providers. Yet 'consumer bodies' are defined in Article 2 as entities licensed by the Institute to provide identity verification services [See also Art 18(9) where 'client bodies' are alluded to as verification service providers; Cf Art 15(1)]. It is also confusing as to

[5] Note also that by mandating the registration of first name, father's and grandfather's names as opposed to last names of Ethiopian nationals, the Bill also essentially repeals the Ethiopian law of names regulated by the Ethiopian Civil Code of 1960 Arts 32-46. See Art 7(3(A)) of the Bill.

whether consumer and client bodies are different entities. Even if they are the same bodies named mistakenly, it remains unclear whether they are different from relying parties. Such glaring drafting missteps should be corrected.

Ambiguities of other types can also be observed in the Digital ID Bill. One relates to the powers of the Institute to take "legal measures". The Institute may take such measures, for instance, when digital IDs are acquired through fraudulent means or when registrants attempt to register twice [See Arts 8(9) cum Art 14(1)]. But what such legal measures constitute is not clear –are these references to fines, cancellation of digital ID or referral to criminal prosecution? In the absence of clarity on the discretion of the future Institute, it may open the door for measures that may be cumbersome or undermine individual rights.

Another problem in the Digital ID Bill is that it relegates a great deal of legislative matters to subsidiary legislation, i.e., Directives to be issued by the Institute [See Art 22(2)]. The concern is that the legislative power of the Parliament will be usurped thereby abrogating democratic principles. Left with broad legislative discretion, the unelected officials of the Institute will be able to wield unaccountable powers. Such tendencies of relegating major and substantive matters to subsidiary laws of regulators is becoming commonplace in Ethiopia. A good case in point is the Communication Services Proclamation No 1148/2019 which reserves significant legislative power to the Ethiopian Communication Authority. The Digital ID Draft Proclamation, which is slated to be adopted by the House of Peoples Representatives soon, should not go down that undemocratic path.

6. Final Words

A few months have passed since the federal Parliament forwarded the Digital ID Bill to its standing committees. Chances are that the Bill might soon be presented before the plenary for final deliberation and enactment. But it is vital that due consideration be given to issues flagged in this comment before it enters the statute book. In particular, it should not be adopted before the data protection bill and the establishment of a robust national data protection authority. The Parliament had held a forum to seek public comment on the Bill in mid-November 2022. Media reports indicate that neither of the concerns flagged in this comment, particularly those relating to data privacy, appeared to have drawn enough attention.[6] The overall apathy towards privacy

[6] See ብሔራዊ ዲጂታል መታወቂያ (EBS TV, 15 November 2022): <https://www.youtube.com/watch?v=IUR2u2tDBNY>.

and data protection in the country may partly be liable for this state of affairs.[7] But with the growing digitization of public services and the inevitable use of digital ID in the process, it is imperative that the data privacy implications of digital identification systems are taken seriously.

List of legislation

1. Draft Digital Identification Proclamation (English Version 1.0, 2021).
2. Draft Digital Identification Proclamation (English Version 2.0, 2022).
3. Registration of Vital Events and National Identity Card Proclamation (hereinafter Proclamation No 760/2012, *Federal Negarit Gazeta*.
4. Civil Code Proclamation No 165/1960, *Negarit Gazeta*.
5. Draft Council of Ministers Regulation Establishing the Ethiopian Digital Identification Commission (Amharic Version, 2022).
6. Communication Services Proclamation No 1148/2019, *Federal Negarit Gazeta*.
7. Draft Digital Identification Proclamation (Amharic Version, 2022)

---

[7] For more on this *se*e, Kinfe Yilma, 'Data Privacy Law and Practice in Ethiopia' (2015). 5 *International Data Privacy Law*.