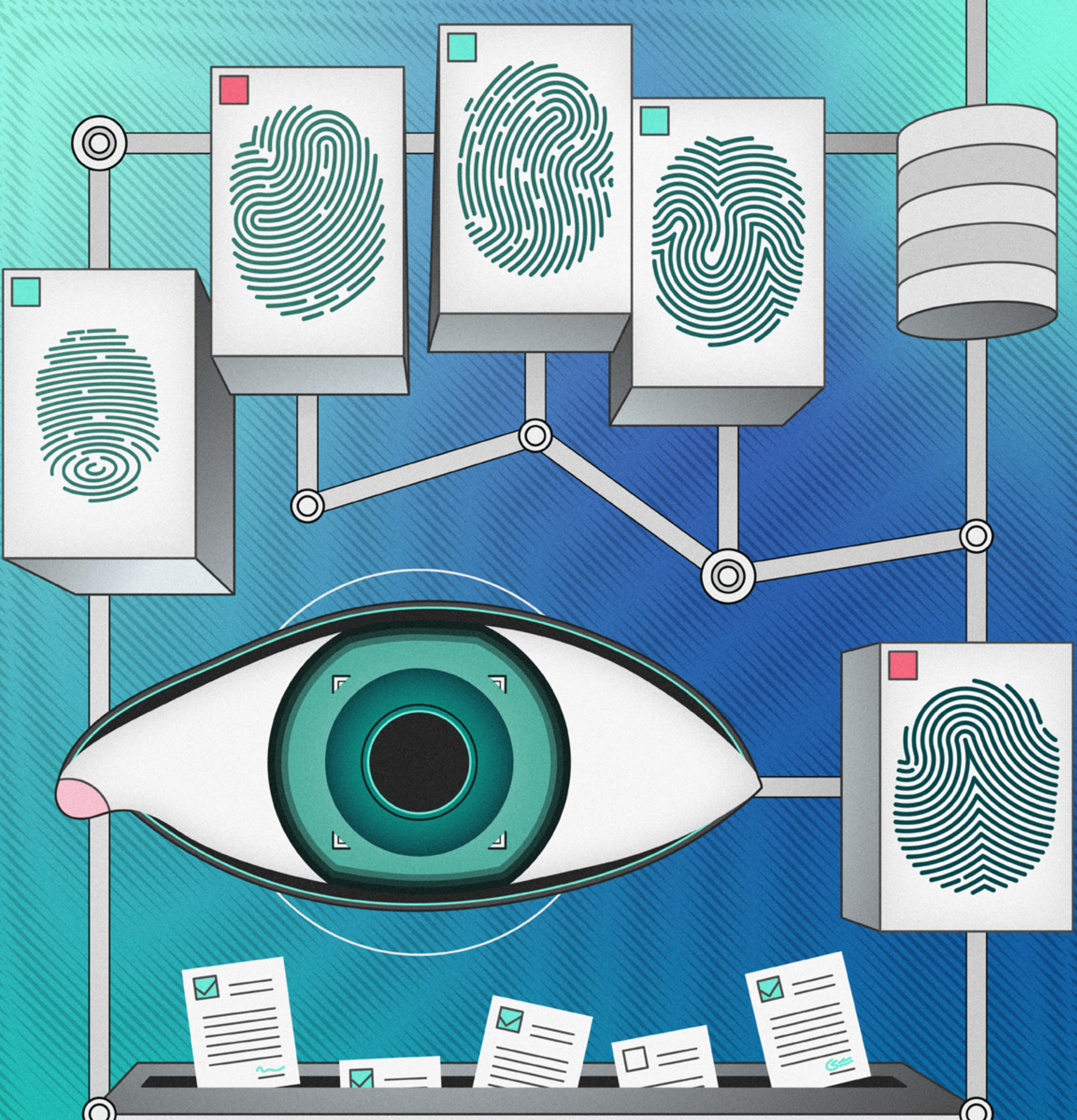

The Future of Biometrics and Digital ID in Lebanon:

Assessing Proposed Systems for Elections and Social Assistance

January 2021

smex.org

ACKNOWLEDGEMENTS

Sacha Robehmed, an independent research consultant, was the researcher and author of this report.

The report was edited by **Grant Baker**, who served as a contributing author, and **Nerissa Naidoo**, who also drafted the initial literature review. Additionally, **Marianne Rahme** provided legal analysis related to data protection and privacy and **Nourhane Kazak** provided copyediting support. **Salam Shokor** designed the cover and the report layout.

The research was generously funded by Privacy International.

All errors and omissions are the responsibility of SMEX.

SMEX is a Lebanese NGO that since 2008 has worked to defend digital rights, promote open culture and local content, and encourage critical, self-regulated engagement with digital technologies, media, and networks across the Middle East and North Africa (MENA).

www.smex.org

A January 2021 Publication of SMEX

Kmeir Building, 4th Floor, Badaro, Beirut, Lebanon

Table of Contents

Executive Summary

In Lebanon, passports, driver's licenses, work permits, residency permits and humanitarian aid all use systems that require biometric data — unique fingerprints and/or iris scans — of citizens, residents, and refugees, which are captured, collected, and stored. In 2017, the newly passed electoral law stated that voters would use "magnetic voting cards"[1] in the upcoming parliamentary elections. (Magnetic cards boast a magnetic stripe, which corresponds to personal information, and they are commonly used as credit cards or for building access cards.)[2] Later in the year, the Cabinet passed a measure to adopt biometric IDs instead of the magnetic voting cards. The new biometric ID would still enable citizens to vote, but it also "serves as an ID, lasts forever and can be used to complete all administrative transactions, whether for social security, at the financial ministry… or anything related to personal civil status."[3]

> " Given the reality of the political and bureaucratic landscape in Lebanon, it's unlikely that benefits of digital ID for citizens, such as efficient service delivery, would be achieved. Yet the risks to individuals' right to privacy are heightened, with insufficient legal frameworks and a history of government data privacy violations. "

The plan for these biometric IDs was not carried out ahead of the parliamentary elections in 2018. However, the Cabinet's amendment hinted at the government's desire to build a national ID system that ties a biometric ID to the provision of services. Given the current economic crisis in Lebanon, the introduction of a biometric voting system seems less likely to come into fruition, but the rollout of the digital ID program for verification and authentication, particularly to support social safety net programs, seems more viable.

Digital and biometric ID is considered by its proponents to offer more efficient service delivery, enhance security, and prevent fraud. The concerns are that digital ID systems may pose privacy and security risks by impinging on individuals' basic rights like the right to privacy; enabling increased surveillance; and potentially being used in harmful ways by malicious actors. There is evidence that digital ID systems are exclusionary — often affecting the most vulnerable people's ability to access government services. Additionally, national digital and biometric ID systems are costly, and often need substantial and reliable infrastructures like internet connectivity and electricity to function.

Given these grave risks and concerns, digital and biometric ID systems should be carefully evaluated to understand if their implementation is the best way forward. Would they solve the problems they are intended for? Are there any less risky alternatives? And if moving ahead with implementation, how can risks be mitigated?

In this report, we aim to both assess the impact of introducing biometric ID on Lebanon's electoral process and highlight concerns about the possibility of developing a digital ID that is attached to the provision of social services, especially given the insufficient safeguards currently in place.

For elections, magnetic voting cards, or biometric ID, would not impact Lebanese electoral fraud, as the challenges are not in creating an accurate electoral roll or in verifying voter identity. Rather, violations have been documented during voting (such as compromised secrecy of the ballot); or in the run up to the election when a party might confiscate an ID card and then return it on election day in exchange for goods or favors.[4] Biometric ID does not combat these kinds of fraud. Another justification given was that magnetic voting cards, or biometric ID, would allow people to vote in their place of residence. International and local election observers nonetheless recommend other measures, such as developing an electoral roll registering voters in their places of residence.

Beyond the elections, other possible benefits of biometric and digital ID systems, including efficient delivery of government services, are unlikely to be realized in Lebanon. There is also concern that a digital ID introduced

[1] Lebanon, *Law No. 44: Election of the Members of the Parliament*, Issued on 17 June 2017, (Official Gazette No.27, June 17, 2017), http://aceproject.org/ero-en/regions/mideast/LB/lebanon-law-no.44-parliamentary-elections-2017

[2] "Magnetic Stripe Card," Science Direct, https://www.sciencedirect.com/topics/computer-science/magnetic-stripe-card

[3] Nicole Hajal, "Report: How does the biometric ID facilitate the voting process?" *Lebanese Broadcasting Corporation International*, September 18, 2017. https://www.lbcgroup.tv/news/d/breaking-news/335830/report-how-does-the-biometric-id-facilitate-the-vo/en

[4] Interview with Aly Sleem, Lebanese Association for Democratic Elections (LADE), July 6, 2020.

to facilitate a social safety net could grow into a broader, national scheme, which could facilitate surveillance and increase civic exclusion. Lebanon's ministries and security agencies also have a history of data leaks, data security breaches, and question marks over data sharing, suggesting weak technical infrastructure and that privacy has not been a priority.

Moreover, current legal frameworks in Lebanon are insufficient to protect individuals' rights when digital ID systems are implemented. The law related to data privacy in Lebanon, the E-Transactions and Personal Data Law, is outdated and does not align with gold standard legal frameworks for data protection, such as the European Union's General Data Protection Regulation (GDPR). While technically it offers some protections, in practice this is not the case. There is no independent data protection authority. This role is instead filled by the Ministry of Economy which has the ability to give third parties access to personal data, or transfer it to foreign states. The E-Transactions Law also makes massive exemptions for government ministries and security agencies and the law has not been enforced.

Given the reality of the political and bureaucratic landscape in Lebanon, it's unlikely that benefits of digital ID for citizens, such as efficient service delivery, would be achieved. Yet the risks to individuals' right to privacy are heightened, with insufficient legal frameworks and a history of government data privacy violations.

Our first goal with this report is to inform future actions of the Lebanese government, international donor governments and organizations working in Lebanon, regarding digital and biometric ID. Secondly, we aim to inform civil society and individuals in Lebanon interested in understanding and learning more about digital and biometric ID specific to our context.

Our recommendations, which we expand on at the end of this report, are as follows:

To the Lebanese government:

1. Fight electoral fraud through electoral reform, not biometric ID

2. Strengthen legal frameworks

3. Ensure sufficient infrastructure is in place

4. Increase transparency around biometric and digital ID procurement and implementation

To international donors:

5. Do not support biometric ID for the purpose of fighting electoral fraud

6. Consult all stakeholders around biometric and digital ID

7. Refrain from excessive centralization of databases

8. Do not mandate digital ID system for provision of social safety benefits

Methodology

The research for this report was desk research and stakeholder interviews carried out between March and October 2020.

We first began with a literature review, building on SMEX's previous research on the subject, to develop a broad understanding of:

- Existing electoral digital ID initiatives in the Middle East and North Africa, including the use of biometric election cards
- Threats, challenges, and advantages faced by groups in the region due to biometric ID initiatives
- The history and use of biometric election cards in Lebanon, and biometric identity initiatives more broadly in Lebanon
- Legal frameworks in Lebanon governing the planned biometric election ID system

We mapped key stakeholders in the private sector, public sector, humanitarian sector, and civil society. We then invited them to take part in a research interview for this project.

This research was planned before the mass protests against the government and banking system that began on October 17, 2019. Since 2019, Lebanon has experienced the devaluation of the national currency, the Lebanese lira (LBP); capital controls; inflation, with food prices and other basic needs soaring; and the Beirut port explosion on August 4, 2020. Based on the information we collected as these events were unfolding, the focus of this project shifted from a more narrow focus on biometric election cards to include digital ID more broadly.

Given the political protests in Lebanon since October 2019, and the COVID-19 pandemic and lockdown which started in March 2020, we chose to focus on private sector actors and international agencies, as opposed to public sector officials. With the deepening economic crisis, and the COVID-19 response, we anticipated that public sector officials would likely be uninterested in discussing biometric ID. Moreover, there was a change in government in December 2019 with a new government forming in January 2020, which resigned in August 2020 following the Beirut port blast. We did, however, reach out to Director General of Civil Status, General Elias Khoury, but did not receive a response.

We spoke with representatives from digital identity and security companies in Lebanon, Inkript and Intalio; The Graphic Shop, who designed most of Lebanon's digital identity documents; civil society organization the Lebanese Association for Democratic Elections; and teams working on social protection, digital ID, and other issues at the World Bank. Email responses to our questions were shared by Dr. Lina Oueidat, former adviser to the Prime Minister on ICT, and IrisGuard, which provides biometric iris scan technology to the World Food Programme (WFP) and the United Nations Refugee Agency (UNHCR). We also spoke with others who provided background information, but wished to remain anonymous.

We requested interviews with Portuguese company Vision-Box, which provides biometric enrollment units that capture face and fingerprint images for driving licences, WFP and UNHCR, but despite contacting different employees on multiple occasions we did not receive a response for comment.

What are Digital ID and Biometrics?

Identification and authentication are vital to accessing services in our daily lives: registering at school, accessing healthcare, opening a bank account, receiving social security or pension payments, voting in elections, driving, or filing legal claims. Governments often validate this identification, providing citizens (and sometimes non-citizens) with evidence of identity such as birth certificates, social security numbers, national identity cards, passports, and driving licenses.

Increasingly, governments have been proposing or implementing national digital identity programs.[5] Digital ID technology is "speeding up processes that once took a long time, changing what and how data is stored, and unlocking digital services for users."[6] The World Bank describes digital ID as offering "the potential to leapfrog the inefficiencies of paper-based identification systems."[7]

Digital ID has been defined by GSMA, the World Bank, and the Security Identity Alliance, as follows:

> *"Digital identity is a collection of electronically captured and stored identity attributes that uniquely describe a person within a given context and are used for electronic transactions. A digital identity system refers to the systems and processes that manage the lifecycle of individual digital identities."*[8]

Digital identity may include personal data unique to individuals in the form of biographic data (such as name, age, gender, date of birth, address, parents' names) and biometric data, which is extracted from biometric identifiers that are unique to individuals.

Biometric identifiers fall into two categories: physical and behavioral. Examples of physical identifiers include fingerprints, irises, facial recognition, DNA, and other physical traits.[9] Behavioral identifiers describe movement; the most well-known examples are voice recognition, keystroke dynamics, and gait movement (i.e. the way a person walks). When governments purchase and implement biometric ID systems for passports or ID cards, these systems primarily rely on physical identifiers because these are currently more easily recorded than behavioural identifiers. For example, it is much easier to record a person's fingerprint than it is to record the way that person walks.

Biometric identifiers are often used in conjunction with other personal data as part of identification systems. Biometrics are being used by governments at borders, in national ID schemes, and for voter registration; by humanitarian agencies for refugee registration; and by private companies to verify the identity of employees or customers.[10] An organization securing its premises, for example, may use a number of biometric identifiers blended with other information, for instance a license plate recognizer and facial recognition in a parking lot, combined with an ID pass and gait movement at an entrance.[11]

A government would register individuals by collecting biographic and also potentially biometric data. After validating and verifying this data, ensuring there are no duplicate records, it can be used to identify a person as a unique individual, answering the question, "who are you?" The individual would then be enrolled in the ID system, and their data stored on a digital database or registry. A government would then ensure there are no duplicate records verifying and establishing the unique identity of an individual.

A digital ID can also be used for authentication, in other words answering, "are you who you say you are?" Governments would attempt to match a credential like data contained on an ID card, or a data sample such as a fingerprint or iris scan, with an existing record in a database, to authenticate that the person seeking to access

[5] GSMA, World Bank Group, and Security Identity Alliance, *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation,* (Washington D.C.: World Bank Group, 2016), 11. https://openknowledge.worldbank.org/handle/10986/24920

[6] "About," Good ID, https://www.good-id.org/en/about/#section-1

[7] Anita Mittal, *Catalog of Technical Standards for Digital Identification Systems,* (Washington D.C.: World Bank Group, 2018), 1. http://documents.worldbank.org/curated/en/707151536126464867/Catalog-of-Technical-Standards-for-Digital-Identification-Systems

[8] GSMA, World Bank, and Security Identity Alliance, *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation,* 11.

[9] Rawlson King, "What are biometrics?", *Biometric Update,* 2016, https://www.biometricupdate.com/201601/what-are-biometrics-2

[10] "Biometrics", Privacy International, https://privacyinternational.org/learn/biometrics

[11] Interview with Stephanie Azarian, Intalio, July 2, 2020.

services is the same person whose identity was previously registered. A credential like an ID card, license, or passport which stores identifiers in a machine-readable format, might be used to prove identity (i.e. that a person is who they say they are), for instance at a border.

Proponents argue that digital ID can lead to better targeted social welfare programs, more efficient access to government services, reduced corruption, and stronger national security measures. However, critics argue that these benefits are not necessarily ensured by national digital ID systems, and that instead concerns of social exclusion, data protection, and cybersecurity are raised, potentially threatening people's right to privacy and freedom of expression. Without safeguards in place, the sensitive personal data that composes a national digital ID system could potentially be used by malicious actors or governments for surveillance, tracking, and control.[12]

This risk is even greater when this sensitive personal data also includes biometrics, as biometrics cannot be changed or altered. The dangers and potential harms are so great that an international group of civil society organizations, technologists, and digital identity development experts, have called for a moratorium on the collection and use of biometrics.[13]

While biometrics and digital ID are commonly linked, biometrics are not a necessary component of a digital ID system. In an interview, World Bank staff noted that:

> *"Biometrics are not necessarily required for a digital ID system, even though people often equate them with digital ID. There are lots of forms of digital ID systems that do not involve biometrics. Countries are encouraged to carefully consider why and when they are collecting and using this data....The value and appropriateness of biometrics depends on the use case and specific country context."*[14]

The World Bank, however, has funded biometric ID programs in countries like Morocco,[15] where the data protection authority later issued a moratorium on the collection of biometric data.[16]

[12] Access Now, *National Digital Identity Programmes: What's Next?* (May 2018), 2. https://www.accessnow.org/cms/assets/uploads/2018/06/Digital-Identity-Paper-2018-05.pdf

[13] "WhyID," Access Now, https://www.accessnow.org/whyid/

[14] Ibid.

[15] World Bank, "ID4D Overview Brochure," *World Bank,* May 8, 2019. https://id4d.worldbank.org/sites/id4d.worldbank.org/files/2019-05/ID4D_Overview_Brochure_English_20190508.pdf

[16] Chris Burt, "Morocco extends facial recognition moratorium to year-end, proposes biometric authentication service." *Biometric Update,* April 9, 2020. https://www.biometricupdate.com/202004/morocco-extends-facial-recognition-moratorium-to-year-end-proposes-biometric-authentication-service#

What is the Existing State of Digital and Biometric ID in Lebanon?

Like many countries in the world, Lebanon has increasingly updated existing forms of identification into biometric identification. Most of the procurement for and initial implementation of government-issued biometric ID took place between 2013 and 2016.

In 2013, the General Directorate of General Security,[17] responsible for collecting intelligence and issuing travel documents, announced that Lebanese passports would be updated to biometric ones in line with international standards established by the International Civil Aviation Organization (ICAO).[18] The passports are perhaps the most high profile biometric ID project in Lebanon, but the first biometric ID project to be announced was the residency permits, which also began in 2013.[19]

In 2014, Lebanese company Inkript won tenders for five biometrics projects: the temporary residency permit (April), border control (June, with Franco-Dutch company Gemalto which was acquired by French company Thales in 2018), biometric residency permit (August), biometric work permit (August), and the motor vehicle tender, which included biometric driving licenses (December).[20] In February 2015, Inkript was also awarded the tender for the biometric passport.[21] The first biometric ID to be implemented was the work permit, a "smart ID card for foreign workers,"[22] which launched in early 2016. The Lebanese biometric passport was first issued in August 2016,[23] and starting November 1, 2016, General Security announced that Palestinian refugees registered in Lebanon would be issued a biometric travel document.[24] (The previous Palestinian travel document was hand written and had not been machine readable, presenting an additional barrier to travel for many Palestinians registered in Lebanon.)[25] Biometric driving licenses were rolled out from September 23, 2016 onwards.[26] In April 2017, General Security began issuing the biometric residency permit.[27] [28]

The current national ID was first adopted in 1997 and implemented by French company IDEMIA.[29] The current ID card is designed with a personalized 2D barcode, which is an encrypted way to store and read biometric and personal data.

[17] Referred to as "General Security" hereafter.

[18] SMEX, *State of Privacy: Lebanon,* (Privacy International, January 2018). https://privacyinternational.org/state-privacy/1081/state-privacy-lebanon

[19] Interview with member of Inkript leadership team, June 15, 2020.

[20] "News," Inkript, https://www.inkript.com/news

[21] Ibid.

[22] "Lebanese Biometric Work Permit Launching," *Youtube,* December 28, 2015. https://www.youtube.com/watch?v=idnTXfDuJEs&ab_channel=Inkript

[23] "Biometric Lebanese passports issuance," General Directorate of General Security, https://www.general-security.gov.lb/en/posts/182

[24] "The instructions related to biometric passports granted to Palestinian refugees in Lebanon," General Directorate of General Security, https://www.general-security.gov.lb/en/posts/196

[25] Victoria Yan and Hasan Darwish, "Biometric documents for Palestinians," *The Daily Star,* November 28, 2016, https://www.dailystar.com.lb/News/Lebanon-News/2016/Nov-18/381825-biometric-documents-for-palestinians.ashx

[26] "News," Inkript.

[27] Elham Barjas and Hussein Mehdy, *Building Trust: Towards a Legal Framework that Protects Personal Data in Lebanon,* (Lebanon: SMEX, October 5, 2017), https://smex.org/building-trust-toward-a-legal-framework-that-protects-personal-data-in-lebanon-report/

[28] In December 2017, the Ministry of Telecommunications proposed the mandating of biometric registration of pre-paid SIM cards, a plan which was later scrapped. (A previous measure introduced in June 2013 required mobile phone users to register their phones using their passport, but was cancelled in 2014.) For more information see: Lara Bitar, "A Brief History of Personal Data Collection in Lebanon," SMEX, December 16, 2017. https://smex.org/a-brief-history-of-personal-data-collection-in-lebanon/)

[29] Nahla Nasser Dine, "Biometric ID...10.52 Dollars for every Lebanese!" Lebanon Debate, Wednesday 20 September 2017. https://www.lebanondebate.com/news/351304

In January 2019, the Directorate-General of Civil Status updated the procedure for applicants for national ID cards "as part of a wider project to digitize its databases."[30] They stopped receiving national ID applications with ink fingerprints on January 31, 2019. Citizens must go to one of the regional directorate branches and give their fingerprints electronically, instead of submitting fingerprints in ink at the local mukhtar's office, which is usually located in the town they reside in. In other words, biometric data is now collected for the ID card.

While this measure is mandatory for new cards, it is not being implemented in such a way that all citizens are forced to update to the biometric ID card. National ID cards now require a biometric identifier, but the 2019 update currently affects only new IDs and IDs that need to be reissued. Lebanese national IDs do not have an expiration date, and as yet there is no edict in place forcing citizens to upgrade their existing cards. Moreover, the new IDs do not store data in a centralized national system. The biometric data collected is for de-duplication, i.e. ensuring the unique identity of each individual, and not for authentication.[31] While in the longer term this may change, for now it would not be usable in elections or for social security without the mandatory updating of all cards and the development of a data system to accommodate the data.

Biometric ID for Refugees

Besides biometric identification for Lebanese citizens, Palestinians living in Lebanon, and foreign workers, biometric identification is used by international aid agencies serving the approximately 1 million Syrian refugees in Lebanon. The UN's Refugee Agency (UNHCR) and the World Food Programme (WFP) collected biometric identifiers—namely iris scans—to register Syrian refugees arriving in Lebanon, and to verify identity when distributing cash assistance through electronic cards. The technology used to implement this system is provided by Jordanian-British company, IrisGuard.[32]

Existing research has assessed the use of biometric ID for refugee populations, and documented the experiences of Syrians whose biometric data were taken as part of refugee registration in Lebanon.[33] The focus of this report is on the use of biometrics for voting in elections and receiving social assistance, which would likely only impact Lebanese citizens, but these systems would not exist in isolation in the country. Rather it would be part of a wider biometric and digital ID ecosystem. For instance, in 2017 UNHCR was directly supporting General Security to scale up its ability to issue residence permits to Syrians, supporting capacity upgrades in at least 16 centers. Central to this capacity support was "the installation of a complete biometric enrolment and resident card personalization software."[34]

Role of International Actors

International regulations are partly responsible for the shift to biometrics. Up until 2015, Lebanese passports were handwritten and therefore not machine readable. ICAO set a deadline of November 24, 2015 for all of its members to adopt biometric technologies, notifying Lebanon's General Security on December 31, 2012. General Security announced in 2013 that the passport would be updated to a biometric one, and subsequently issued a tender that was awarded to Inkript in 2014.[35] According to Inkript, the driving licenses also conform to international standards under the 1968 Vienna Convention on Road Traffic,[36] although Lebanon is not listed as an official signatory.[37]

[30] "Lebanon to digitize fingerprints for ID applications," *The Daily Star,* January 2, 2019, https://www.dailystar.com.lb/News/Lebanon-News/2019/Jan-02/473089-lebanon-to-digitize-fingerprints-for-id-applications.ashx

[31] Interview with World Bank staff, October 7, 2020.

[32] "Liban Post Case Study," IrisGuard, https://www.irisguard.com/technology/case-studies/liban-post/

[33] For examples, see: Dragana Kaurin, "Data Protection and Digital Agency for Refugees". World Refugee Council Research Paper No. 12 (May 2019) https://www.cigionline.org/sites/default/files/documents/WRC%20Research%20Paper%20no.12.pdf

[34] UNHCR, *Operational Update, Lebanon: 3rd Quarter Update, July - September 2017* (January 2018), 2. https://www.unhcr.org/lb/wp-content/uploads/sites/16/2018/01/UNHCR-2017_Q3_EN.pdf

[35] SMEX, *State of Privacy: Lebanon.*

[36] Interview with member of Inkript leadership team, June 15, 2020.

[37] United Nations, "19. Convention on Road Traffic, Vienna, 8 November 1968," Treaty Series, https://treaties.un.org/pages/ViewDetailsIII.aspx?src=TREATY&mtdsg_no=XI-B-19&chapter=11

Biometric and digital ID systems have also been introduced as part of digital transformation projects. Since 1994, the United Nations Development Programme (UNDP) has supported the Office of the Minister of State for Administrative Reform (OMSAR), and a core pillar of OMSAR's strategy is "the use of ICT tools enhanced and an E-Government portal established."[38] Even in 2007, the vision included a smart card for the national ID card–with an OMSAR presentation showing an image of a card with microchip–which citizens could use to access services.[39] And in late 2018, General Security launched its Vision 2021 strategy for a "paperless organization,"[40] with Intalio (at the time known as Everteam) to digitize their system.

It's also no coincidence that the increased adoption of biometrics has taken place alongside wider geopolitical events, such as the conflict in neighboring Syria and growing government concern about security. Bilateral donors, in particular the United States and the United Kingdom, have supported border management with Syria. The US and the UK, together with other international donors such as China, France, Germany, Italy, Poland, Qatar, Russia, Saudi Arabia, and the United Arab Emirates, have provided increasing financial and technical support to the plethora of agencies that comprise Lebanon's security apparatus since 2011.[41] It is difficult to find details as this information is rarely publicized, but at least some of this funding has supported new digital ID and biometrics systems. The US supported Lebanon's Internal Security Forces with an 11 million USD upgrade to its IT system and biometrics database in 2017,[42] while a Saudi grant is credited as funding the 35 million USD contract for the biometric passports.[43]

Other international donors and financial institutions play a major role too. In 2019, the World Bank was working with the government on a digital economy project, which included building digital ID in Lebanon, and had started an assessment before putting this work on hold when protests started in October 2019. Due to Lebanon's enormous national debt burden and a lack of reforms, most lending and support that Lebanon had been receiving from multilateral institutions like the World Bank and UNDP was halted. Donors have redirected funds towards food aid and emergency relief. WFP expanded its social assistance programme from 15,000 to 35,000 families in Lebanon through the Ministry of Social Affairs' National Poverty Targeting Programme,[44] while the World Bank has a 246 million USD Emergency Social Safety Net project in the pipeline, which includes investments in "social registry/database management."[45] A Central Management Unit (CMU) located in the Presidency of the Council of Ministers (PCM) will house the targeting database.

Role of Private Sector Biometrics Companies

For each form of biometric identification, the relevant government department launches a tender which private sector companies apply for. French company IDEMIA (formerly known as Morpho, and before that Safran Group or Sagem Sécurité) was given the tender for Lebanon's ID cards. IDEMIA has worked to implement a biometric ID system

[38] "Support to Civil Service Reform and Management Capacity of Public Administration - Phase II," UNDP Lebanon, https://www.lb.undp.org/content/lebanon/en/home/projects/SupporttoCivilServiceReformandManagmentCapacityofPublicAdministration-PhaseII.html

[39] Tania Zaroubi, "e-Government in Lebanon: an overview and the action plan," *Expert Group Meeting on ICT Indicators Adoption and Data Collection* (Cairo, February 13-15, 2007) https://www.unescwa.org/sites/www.unescwa.org/files/events/files/021_zaroubi.pdf

[40] Daoud Rammal, "'Vision 2021' Comprehensive Digital Transformation of 'Paperless General Security'," *General Security Magazine, no. 64* (January 2019) 40-42. https://www.general-security.gov.lb/uploads/magazines/64-2/10.pdf

[41] Simone Tholens, "Border management in an era of 'statebuilding lite': security assistance and Lebanon's hybrid sovereignty," *International Affairs, 93, no.4* (July 2017): 865–882, https://doi.org/10.1093/ia/iix069

[42] "New U.S. Government-Funded Biometrics Project Supports International Efforts to Counter Terrorism and Crime," US Embassy in Lebanon, August 19, 2017, https://lb.usembassy.gov/new-u-s-government-funded-biometrics-project-supports-international-efforts-counter-terrorism-crime/

[43] Yassmine Alieh, "Inkript wins biometric passport tender," Lebanon Opportunities, February 23, 2015, http://www.businessnews.com.lb/cms/Story/StoryDetails.aspx?ItemID=4667

[44] WFP, "WFP to assist 50,000 crisis-hit families via national safety net programme", September 22, 2020, https://www.wfp.org/news/wfp-assist-50000-crisis-hit-lebanese-families-national-safety-net-programme

[45] World Bank, *Project Information Document,* Lebanon Emergency Crisis and COVID-19 Response Social Safety Net Project (P173367), October 27, 2020, 6, http://documents1.worldbank.org/curated/en/216001603902307374/pdf/Project-Information-Document-LEBANON-EMERGENCY-CRISIS-AND-COVID-19-RESPONSE-SOCIAL-SAFETY-NET-PROJECT-P173367.pdf

in Morocco, and is perhaps best known for supplying the controversial Aadhar system in India, where they "manage a multi-biometric database of 1.3 billion people."[46]

Apart from the ID cards, Lebanese company Inkript has won every other bid on biometric identity projects. Inkript worked with Franco-Dutch company Gemalto (acquired by Thales in 2018) on the biometric passports with Inkript responsible for programming, software development, and project coordination, while Gemalto made the physical passports.[47] They also collaborated on the border control systems. For the driving licenses, Inkript worked with Portuguese company Vision-Box that provided a desktop technology to capture standardized face and fingerprint images.[48]

[46] "Trusted and legal identity," IDEMIA, https://www.idemia.com/trusted-and-legal-identity

[47] "News," Inkript.

[48] "New Vision-Box Identity Management Solution Introduces Biometric Enrollment for Driver License applications in Lebanon," Vision-Box, March 5, 2018, https://www.vision-box.com/pressroom/press-releases/new-vision-box-identity-management-solution-introduces-biometric-enrollment-driver-license-applications-lebanon

Biometric ID in Lebanese Elections

Prior to 2018, the last parliamentary election was in 2009. Parliament extended its mandate twice, citing failure to agree on the new electoral law and security reasons, until the Electoral law was passed in 2017 along with a third parliamentary extension.[49] The Electoral Law issued on June 17, 2017, introduced proportionality and redefined constitutions. It also included provisions for an election-specific magnetic card, under Article 84.[50] Magnetic cards are cards with a magnetic stripe which contains information, and are commonly used in the banking sector or for building entry.[51] According to the Ministry of Information, the purpose of the magnetic election card was "to allow voters to cast their ballot from anywhere in the country—through so-called magnetic voting cards —rather than having to travel to their district."[52]

> “As the biometric ID proposal encompassed service provision beyond elections, any future biometric or digital ID could be expected to have a similar broad scope. The current focus on digital and biometric ID systems is for social protection programs.”

On September 17, 2017, the Cabinet approved a proposal changing the "magnetic card" in the election law to biometric ID.[53] A media report at the time touted the benefits: while they cost the same as a magnetic card or a biometric voting card—only to be used once—the biometric ID "lasts forever and can be used to complete all administrative transactions, whether for social security, at the financial ministry, to apply for a passport or anything related to personal civil status."[54] The cost of introducing the biometric ID cards was estimated at 134 million USD by the parliamentary committee in charge of budgets.[55] Preparations were made: the graphic designer that worked on the passport and vehicle licenses designed a sketch for the biometric ID which was taken to be printed, but did not hear anything more.[56]

However, there were significant concerns from civil society organizations and election experts as well as some parliamentarians that there was insufficient time to introduce the biometric ID. Doing so would risk disenfranchisement, which would affect the legitimacy of the election results. They also feared that the biometric election card would be used as an excuse to further delay elections[57]—the previous election was cancelled just two weeks before it was scheduled to take place in June 2013, with Parliament extending its mandate multiple times. As the first parliamentary election in nine years, civil society groups and election monitors were understandably wary of potential reasons to postpone again.

These concerns were echoed by the private sector, too. Inkript, the company that had won tenders for all biometric ID in Lebanon so far, was consulted on the magnetic election cards ahead of the 2018 elections. Their assessment was that the time frame was too tight to be able to implement a system. A member of Inkript's senior leadership team said that while the necessary hardware and software could have been rolled out in nine months, the major challenge would have been to register the biometric data of all eligible voters.[58] Although biometric data has already been captured

[49] European Union Election Observation Mission to Lebanon 2018, *Final Report: Parliamentary elections 2018,* (EU EOM, July 2018), https://eeas.europa.eu/sites/eeas/files/final_report_eu_eom_lebanon_2018_english_17_july_2018.pdf

[50] Lebanon, *Law No. 44: Election of the Members of the Parliament.*

[51] "Magnetic Stripe Card," Science Direct.

[52] "Lebanese Electoral Law 2018," Republic of Lebanon Ministry of Information, April 4, 2018, https://www.ministryinfo.gov.lb/en/22598

[53] Joseph Haboush, "Cabinet OKs biometric IDs in upcoming elections" *The Daily Star,* September 18, 2017, https://www.dailystar.com.lb/News/Lebanon-News/2017/Sep-18/419685-cabinet-oks-biometric-ids-in-upcoming-elections.ashx

[54] Hajal, "Report: How does the biometric ID facilitate the voting process?"

[55] Ghinwa Obeid, "Split over biometric voter ID cards lingers," *The Daily Star,* October 27, 2017, https://www.dailystar.com.lb/News/Lebanon-News/2017/Oct-27/424074-split-over-biometric-voter-id-cards-lingers.ashx

[56] Interview with Noha Karanouh Kabbani, The Graphic Shop, July 15, 2020.

[57] Federica Marsi, "Biometric IDs: Ambitious project, razor-thin window," *The Daily Star,* September 19, 2017, https://www.dailystar.com.lb/News/Lebanon-News/2017/Sep-19/419784-biometric-ids-ambitious-project-razor-thin-window.ashx

[58] Interview with member of Inkript leadership team, June 15, 2020.

for the driving license and passport, these documents are not used for voter identity authentication and cover a smaller population than the 3.5 million eligible voters that were registered in 2015.[59]

On March 29, 2018, Parliament amended Article 84 of the Lebanese Electoral Law issued in 2017 so that neither magnetic cards nor biometric IDs were mandatory for the elections held on May 6, 2018.[60] However biometric ID remains on the table for future elections in Lebanon. As the biometric ID proposal encompassed service provision beyond elections, any future biometric or digital ID could be expected to have a similar broad scope. The current focus on digital and biometric ID systems is for social protection programs. This report will examine arguments and concerns for digital and biometric ID, primarily in relation to elections, but also taking a broader approach to consider the proposed expansion to identify and authenticate individuals eligible for social services, particularly social assistance.

[59] International Foundation for Electoral Systems, *Lebanon's 2017 Parliamentary Election Law,* (Arlington: IFES, October 2017) https://www.ifes.org/sites/default/files/lebanons_2017_parliamentary_election_law_final.pdf

[60] Lina Younis, "Parliament Concludes Evening Session, Amends Article 84 of Elections Law Concerning Biometric Card," *National News Agency,* March 29, 2018, http://nna-leb.gov.lb/en/show-news/89619/Parliament-concludes-evening-session-amends-article-84-of-elections-law-concerning-biometric-card

Examining Arguments and Concerns for Digital and Biometric ID

Proponents of biometric ID argue that the main advantage of using biometrics in elections is to combat fraud in voter registration and voter verification. However, neither of these represent the most significant electoral violations during elections in Lebanon. As such, the introduction of digital or biometric ID in elections would have limited impact. The Lebanese Association for Democratic Elections (LADE) has instead put forward other (non-biometric) measures which would safeguard from fraud.

There are also concerns specific to implementing biometrics in Lebanese elections. First and foremost is that the credibility of the election could be diminished. Then there are challenges with infrastructure needed to run biometric voting systems, and the reliability of high-tech election systems. The anticipated costs were budgeted at 130 million USD, while there was also a real potential risk of function creep—the mandated use of biometric ID beyond the initial proposed function of voter ID.

Biometric ID would not fulfill the expected promise of preventing fraud, as most electoral fraud violations could still occur regardless of the ID used. At the same time, the high cost of biometric ID, risk to the credibility of the elections, exclusion risks, and other concerns of using digital and biometric ID in elections outweigh the benefits.

Voter Identity Authentication

During elections, it is important to ensure that the person who is voting matches the person registered to vote. Biometric ID can play a role in ensuring 'one person, one vote.' For example, for voter authentication using fingerprints, "the prints are compared against reference fingerprints stored on an identity document or in a fingerprint database, which enables the owner to be securely authenticated as the holder of the document."[61] Biometric ID is considered more secure as it stores biometric identifiers unique to an individual, for instance fingerprints or an iris scan, that have to correspond with the person presenting the card. However, according to experts, the majority of the issues with the Lebanese electoral system are not related to identity authentication.

> “ Most electoral fraud in Lebanon is not related to challenges of authenticating voter identity, but rather to clientelism and the tactics of political parties to secure votes. ”

In 2017, then Foreign Minister Gebran Bassil proposed the biometric ID be used to prevent voter fraud. He stated: "There are three things being targeted in the new electoral law: the voters' freedom, increasing [voter] participation and forgery."[62] He claimed biometric IDs would make it more difficult for someone to vote with another person's ID card, or a fake ID card.

Leaders in the biometrics industry are less certain about biometric ID's ability to limit fraud. A member of Inkript's senior leadership team told SMEX that he believes biometrics can mitigate certain aspects of election fraud related to voter identity, but acknowledges that biometrics alone cannot combat interference from political parties and other types of fraud:

> *"We can use biometrics to secure the voting operations...[but] you will not be able to eliminate elections fraud. The biometric ID can reduce fraud related to the procedure of voting. However, many illegal interferences might occur by voters or parties in the process of an election."*[63]

Likewise, Thales (the French company which acquired Gemalto, the maker of Lebanon's biometric passports, in 2018) stated in a 2020 report on biometric election systems generally that "until cases of electoral fraud have been demonstrated and quantified, it remains difficult to establish what contribution the use of biometrics would make to the fairness of the ballot."[64]

[61] "Biometric voter registration: trends and best practices," Thales, 2020, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/identity/enrolment/biometric-voter-registration

[62] Obeid, "Split over biometric voter ID cards lingers."

[63] Interview with member of Inkript leadership team, June 15, 2020.

[64] "Biometric voter registration: trends and best practices," Thales.

While electoral fraud is present in Lebanon, when we examine electoral violations they are rarely related to authenticating voter identity. During the 2018 election, more than 7,000 violations were recorded by Lebanese and international observers,[65] with some of the most serious pertaining to secrecy of the ballot. For instance, only 91.99% of polling stations had screens positioned to guarantee secrecy; and party representatives accompanied voters to polling stations or even behind voting screens, pressuring them to cast their vote.[66] According to Aly Sleem, Executive Director of the Lebanese Association for Democratic Elections (LADE), another type of violation his organization has recorded in past elections was political parties confiscating ID cards in exchange for cash gestures or services, and returning the ID on election day to ensure a vote for a particular candidate.[67] These types of electoral fraud could still occur even with biometric ID.

Most electoral fraud in Lebanon is not related to challenges of authenticating voter identity, but rather to clientelism and the tactics of political parties to secure votes. Instead of a biometric card which will be costly to citizens and government, and still vulnerable to electoral violations, LADE recommends two reforms:

1. To give voters the right to vote in polling centers near the location they live in.

2. To create an electoral roll and give voters the right to actively register prior to the elections, so that they can elect candidates in their place of residence

Voter Registration

> “ Civil registry records remain largely paper-based, which can be a challenge. ”

Under Article 26 of the 2017 Electoral Law, voter registration happens automatically, with annual voter lists extracted from Lebanon’s Civil Status Register, which is maintained by the Ministry of Interior and Municipalities under the Directorate General for Civil Status.[68] Under this central directorate, there are regional departments in each governorate, and below that 52 civil registry offices.[69] Civil registry offices hold records of births, deaths and marriage. An extract of the civil status record document (ikhraj eid), derived from the civil registry, is the basis for other identification documents in Lebanon, and is required when applying for the national ID card (hawiya)[70] and passport.[71]

These civil registry records remain largely paper-based, which can be a challenge. Accurate voter registers are essential in ensuring people’s right to vote, and most EU countries extract voter registration data from existing population registers,[72] as is the case in Lebanon. A potential risk to the accuracy of the registers in Lebanon is that civil registry offices across Lebanon often keep these civil status records manually, and the data they hold is not networked.[73] Paper-based records are generally more difficult to update and cross-check, increasing the risk of electoral fraud through “ghost voters” (deceased citizens) or multiple registrations for the same person, allowing multiple votes. This is often used to justify biometricelection systems — at least 45 countries use fingerprints, and Somaliland used iris scans in the 2017

[65] National Democratic Institute, *Lebanon 2018 Parliamentary Elections: Final Report,* (National Democratic Institute, July 2019), 27, https://www.ndi.org/sites/default/files/Lebanon%202018%20Parliamentary%20Elections_Final%20Report%20%28v.3%29.pdf

[66] Lebanese Association for Democratic Elections, *Observation Mission of 2018 Parliamentary Elections,* May 2017, https://lb.boell.org/sites/default/files/uploads/2018/05/180507_prelimreport_overviewen.pdf

[67] Interview with Aly Sleem, LADE, July 6, 2020.

[68] Lebanon, *Law No. 44: Election of the Members of the Parliament.*

[69] United Nations, Department of Economic and Social Affairs Statistics Division, Demographic and Social Statistics Branch, “Status of Civil Registration and Vital Statistics in ESCWA Region,” Technical Report Series, Vol. 1, March 2009, 38. https://unstats.un.org/unsd/demographic-social/crvs/documents/Technical_report_ESCWA_Final.pdf

[70] “ID Express,” OMT, https://www.omt.com.lb/en/services/governmental/id-express-service

[71] “Biometric passport,” General Directorate of General Security, https://www.general-security.gov.lb/en/posts/11

[72] Martin Russell and Ionel Zamfir, “Digital technology in elections: Efficiency versus credibility?” *European Parliamentary Research Service,* September 2018, 2. https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/625178/EPRS_BRI(2018)625178_EN.pdf

[73] EU Election Observation Mission to Lebanon 2018, *Final Report,* 17.

election.[74] Despite Lebanon's civil registry system being largely paper-based, voter registration is not a major fraud concern in Lebanon. The European Union Election Observation Mission in 2018 reported that "confidence in the inclusiveness and transparency of the voter list among political forces and other interlocutors was widespread."[75] It would seem that the current voter list is accurate, and that Lebanon does not face some of the voter registration challenges of other countries that use biometrics for voting.

Voting Location and Increasing Participation

According to the Ministry of Information, the main purpose of the magnetic voting card was "to allow voters to cast their vote from anywhere in the country."[76] In 2017, Baabda MP Alain Aoun (and nephew of President Michel Aoun) told the media "the goal is to let voters vote in their area of residence and [therefore] get better participation."[77]

In Lebanon, voters must vote from their paternal ancestral place of registry, and married women from their husband's registered ancestral place. In practice, this means that in order to exercise their right to vote, people may have to travel (perhaps for several hours) from the urban center where they live, to the more rural location where their family is registered. This applies even if their family may not have lived there for decades or even generations. This is because the electoral register is drawn from civil status records. While there are legal provisions to transfer registration location, in practice these are barely used and transferring registration is a politically sensitive topic in relation to Lebanon's confessional status quo.[78] The 2018 European Union Election Observation Mission to Lebanon recommended that "it would be advisable to implement a system that allows voters to cast ballots in a place where they actually reside."[79] This has yet to happen.

The introduction of a biometric ID would not in and of itself change the voting location; it would just add an additional data point to individuals' existing personal records and ID documents. In other words, it would not transform the civil status record system. It might allow for people to vote in polling mega centers close to their residence, yet their vote would be for the location they are registered in. However, allowing people to vote where they reside does not require a biometric ID.

Civil society organizations such as LADE say that what is needed instead is an electoral roll for voters to register in the area they are eligible to vote in, such as their place of residence, and freely cast their vote in the district where they live rather than returning to their ancestral villages to vote.[80] Introducing biometric cards for elections will not automatically allow for voting from different locations. Rather, a far less costly solution would be the introduction of an electoral roll, allowing people to actively register to vote where they reside.

Credibility and Trust in Election Results

While biometric ID may not address electoral fraud present in Lebanon, it could in fact contribute to eroding voter confidence in the electoral system. Digital ID systems provider Thales notes that:

"In a tense political context, where there is a total lack of trust between the different people involved in the electoral process, biometrics can itself become something of a double-edged sword. It may help to resolve problems with the identification of voters and prevent fraud of a particular type. Still, it cannot, by itself, render an electoral process reliable, credible and transparent."[81]

The technology involved, such as electronic voting software, can be vulnerable to hacking attacks, and suspicions of digital fraud can cast doubt on election results. Given the past challenges of an election even taking place in

[74] "ICTs in Election Database," International Institute for Democracy and Electoral Assistance, https://www.idea.int/data-tools/question-view/738 from Russell and Zamfir, "Digital technology in elections," 2.

[75] EU Election Observation Mission to Lebanon 2018, *Final Report,* 17.

[76] "Lebanese Electoral Law 2018," Republic of Lebanon Ministry of Information.

[77] Marsi, "Biometric IDs: Ambitious project, razor-thin window."

[78] EU Election Observation Mission to Lebanon 2018, *Final Report,* 17.

[79] Ibid, 5.

[80] Interview with Aly Sleem, LADE, July 6, 2020.

[81] "Biometric voter registration: trends and best practices," Thales.

Lebanon, alongside the current distrust of politicians —with protests across the country calling for the resignation of president, the prime minister, and the speaker of parliament since October 2019, and further distrust in the governance system since the August 4 2020 Beirut explosion—the primary concern must be for a reliable, credible and transparent election.

Iraq's 2018 election illustrates the potential vulnerabilities biometric voting systems present, weakening voter confidence in the result. The Independent High Electoral Commission (IHEC) in Iraq introduced a biometric voter registration and election system in order to prevent fraud and improve the accuracy of the voter list for the 2018 parliamentary elections on May 12—held just six days after Lebanon's parliamentary election. While Lebanon was debating magnetic cards and biometric ID in 2017, Iraqi citizens were registering their biometric data including all 10 fingerprints, iris scans, a voice sample, and photo, as well as non-biometric personal data like full name, date of birth and address, which was all stored on a chip-enabled voting card.[82] Civil society was concerned about the privacy of citizens' data, but the IHEC insisted that a security breach was "not possible."[83]

Yet after the poll, intelligence services conducted tests which showed it was possible to hack voting machines and manipulate the results, leading the Iraqi government to call for a manual recount of the vote.[84] In particular, electoral complaints concerned the "Polling Station Count Optical Scanners (PCOS) and Central Count Optical Scanners (CCOS)," which Korean company Miru Systems built as part of their 135 million USD contract.[85] With multiple corruption cases related to the elections, Iraqi citizens were angry at this failure of biometric e-voting, which they had been assured would result in free and fair elections, but had instead wasted public funds and insecurely collected and stored their personal data.[86] As Thales' report on biometric election systems states: "a democratic, reliable and fraud-free electoral process is an essential factor in establishing lasting peace and stability in a country."[87] Yet, Iraq's biometric election system created a disputed election result, damaging voter confidence and eroding trust in the government.

Iraq's deployment of biometric voter registration in the 2018 elections should also serve as a warning about the likelihood of the Lebanese government introducing biometric ID linked to voting in the future. Iraq previously attempted to deploy biometric voter registration ahead of the 2014 parliamentary elections, contracting Spanish company Indra to develop a biometric system and 22 million corresponding ID chips.[88] The company was ultimately not able to produce the system on time, but it did produce an electronic voting system, which was rife with issues. There were "discrepancies in the tallying of votes by voting machines,"[89] which were primarily reported in the Kurdistan Region of Iraq and Kirkuk. These issues with the biometric voting system in 2018 mirrored issues with electronic voting Iraq faced in 2014.[90] The IHEC and the United Nations Assistance Mission for Iraq (UNAMI) published a tender in February 2017, which was eventually awarded to Miru Systems and Indra.[91] After the botched introduction of biometrics in the 2018 parliamentary election, Iraqi lawmakers have once again stated that biometric voter registration will

[82] Emna Sayadi, "FAQ: Elections in Iraq – what will happen to the biometric data of voters?", Access Now, July 20 2018, https://www.accessnow.org/faq-elections-in-iraq-what-will-happen-to-the-biometric-data-of-voters/

[83] Ibid.

[84] AFP, "Iraq orders probe after voting machines fail hacking test," *Arab News,* May 25, 2018, https://www.arabnews.com/node/1309716/middle-east

[85] Hussein Rikar, "Iraq Election Body Feared Effects of Recount, Member Says," *Voice of America,* May 19, 2018, https://www.voanews.com/middle-east/iraq-election-body-feared-effects-recount-member-says

[86] Sayadi, "FAQ: Elections in Iraq."

[87] "Biometric voter registration: trends and best practices," Thales.

[88] National Democratic Institute, *MENA Voter Registration - Iraq,* (Washington D.C, NDI, October 2015), https://www.ndi.org/sites/default/files/MENA%20Voter%20Registration_EN_Iraq.pdf

[89] Ahmed Rasheed, Raya Jalabi, Ahmed Aboulenein, "Exclusive: Iraq election commission ignored warnings over voting machines - document," Reuters, August 5, 2018 https://www.reuters.com/article/us-iraq-election-exclusive-idUSKBN1KQ0CG

[90] National Democratic Institute, *MENA Voter Registration - Iraq.*

[91] "Tender No. 1/I/P/2017 Electronic Voter Cards for IHEC-Iraq," UN Global Marketplace, https://www.ungm.org/Public/Notice/53832"https://www.ungm.org/Public/Notice/53832

be a critical component of the proposed parliamentary elections in 2021.[92]

Infrastructure

A huge challenge in Lebanon is the infrastructure needed for a biometric ID system to work. This was another criticism levelled in 2017—that Lebanon lacks the adequate internet and reliable, constant power supply, needed to ensure the reliability of technology needed to verify biometric ID in elections.[93] Each polling station (there were 1880 polling centers containing 6793 polling stations in the 2018 election)[94] would need constant electricity and connectivity to enable the card readers and computerized system used to electronically authenticate voters' biometric ID.

Examples from other countries can illustrate the infrastructure challenges. Nigeria's high tech 2015 election costing 200 million USD faced many technical problems, which led to delaying the election by 6 weeks and extending the voting period.[95] One of the key challenges was with the fingerprint identification reader machines used to validate voter ID cards. According to reports, "critics believe that the effectiveness of the device may have been impaired through its 'epileptic' power supply"[96] with backup batteries not supporting the machine for the 12 hours needed on voting days.

There are ways to mitigate infrastructure challenges, such as using an offline list from a digital electoral roll that works without an internet connection instead of accessing a database online, and having printed lists as a paper back-up in case electronic equipment fails.[97] But the risk is that a biometric system with Lebanon's unreliable infrastructure may combine to cast doubt on the credibility of an election. If a power outage caused polling stations to go offline which would pause or delay voting using digital or biometric ID, this might create suspicion about the fairness of the process, and thus the accuracy of the election results.

Reliability

Introducing biometric ID does not mean that identification and verification are completely reliable, as for some people, "standard" biometric identifiers cannot be found or matched, which may exclude those individuals.

> “ Populations that may be in greatest need of accessing services may have more difficulty doing so. ”

For instance, in Venezuela, the biometric system was unable to match 11% of voters' fingerprints with their voter registration records. Pakistan decided not to use fingerprint scanning in their 2018 elections after experiencing a similar failure rate in testing.[98] The medical condition adermatoglyphia, a loss of fingerprints, is problematic for biometric ID systems requiring mandatory fingerprint scans.[99] In Lebanon, this condition affects 2.8% of those aged 25-64, and 8.5% of those aged 65 and older, with women 3.75 times more affected than men.[100] Adermatoglyphia is more likely to affect those who have worked in manual occupations and come into contact with irritants, with the study noting that "housewives, hairdressers, nurses, workers with

[92] Chris Burt, "Iraq draws closer to biometrics-backed elections in 2021 with 16M voter cards issued," *Biometric Update,* November 16, 2020, https://www.biometricupdate.com/202011/iraq-draws-closer-to-biometrics-backed-elections-in-2021-with-16m-voter-cards-issued

[93] Marsi, "Biometric IDs: Ambitious project, razor-thin window."

[94] National Democratic Institute, *Lebanon 2018 Parliamentary Elections: Final Report,* 12.

[95] Rawlson King, "Nigerian election successful despite biometric voting hiccups," *Biometric Update,* April 7, 2015, https://www.biometricupdate.com/201504/nigerian-election-successful-despite-biometric-voting-hiccups

[96] Ibid.

[97] Russell and Zamfir, "Digital technology in elections," 7.

[98] Ibid, 4.

[99] Nuraiz Sarfraz, "Adermatoglyphia: Barriers to Biometric Identification and the Need for a Standardized Alternative." *Cureus* vol. 11, 2, February 8, 2019, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6456356/

[100] Roger Haber, Josiane Helou, Joelle Korkomaz, Maya Habre, Antoine Ghanem, and Roland Tomb. "Absence of fingertips with focus on dermatological etiologies: national survey and review." *Clin Dermatol* 3, no. 1 (2015), 22, https://www.researchgate.net/profile/Roger_Haber/publication/281274814_Absence_of_fingertips_with_focus_on_dermatological_etiologies_National_survey_and_review/links/55de081508ae79830bb58369.pdf

repeated exposure to cement, cutting oils, or abrasive"[101] are mainly affected.

For those voters whose fingerprints could be matched on election day, this would likely cause confusion and delays. At its worst, it could mean certain people—who tend to be older, female, or work in manual occupations—would be excluded through the identity authentication process, or have their identity questioned in a way that might dissuade them from voting. This disenfranchisement and civic exclusion would violate their right to vote. At the very least, an alternative (non-biometric) process would need to be in place as a backup.

> “ Populations that may be in greatest need of accessing services may have more difficulty doing so. ”

For other services beyond elections, if biometric ID systems relying on fingerprints are implemented, it would likely result in exclusion of people whose fingerprints cannot be read, with and older people, women, and manual workers at higher risk of exclusion. Ultimately, populations that may be in greatest need of accessing services may have more difficulty doing so.

Legal Identity

Proponents of digital ID argue that it allows people to access social services they are entitled to. World Bank publications, for instance, claim that:

> *"For individuals, proof of legal identity is necessary to access rights, entitlements, and services. Without it, they may face exclusion from political, economic, and social life.For governments, modern identification systems allow for more efficient and transparent administration and service delivery, a reduction in fraud and leakage related to transfers and benefits payments, increased security, accurate vital statistics for planning purposes, and greater capacity to respond to disasters and epidemics."*[102]

People have a right to prove who they are and have a legal identity; legal identity is even part of the United Nations' Sustainable Development Goal 16.9, which strives to ensure that people across the world have a legal identity by 2030.[103] Identification allows people to claim and access services like education, healthcare, or pensions.

Critics of digital ID though, note that legal identity does not necessarily mean digital ID, and argue that people should be able to access services regardless of their ID status. Moreover, Sustainable Development Goal 16.9 is essentially concerned with civil registration, as it specifically mentions birth registration, which does not require a digital ID.

Exclusion

Rather than being able to more efficiently access rights, entitlements, and services, people who are not able to register for and access digital and biometric IDs could be excluded from both elections and other services.

> “ Even with sufficient lead time, digital ID systems can still exclude the most vulnerable and marginalized in society, especially when first being introduced. ”

One of the fears expressed in 2017 was the potential disenfranchisement of voters if cards could not be rolled out to all voters in time before the 2018 elections.[104] Even with sufficient lead time, digital ID systems can still exclude the most vulnerable and marginalized in society, especially when first being introduced. Elderly or disabled people are at risk of being overlooked if digital ID rolls out, as they may not be capable of traveling l to the office where registration is taking place. (It's worth noting that civic exclusion is already present in the electoral system, with most polling stations offering inadequate access and therefore not permitting citizens with disabilities to vote with dignity.[105]) If someone does not have the economic means to pay for transport to the registration office, or the literacy level to fill in forms, they would be less likely to have access to a new digital ID.

[101] Haber et al,"Absence of fingertips with focus on dermatological etiologies," 24.

[102] Mittal, *Catalog of Technical Standards for Digital Identification Systems,* 1.

[103] "Legal Identity Agenda," United Nations Statistics Division, https://unstats.un.org/legal-identity-agenda/

[104] Marsi, "Biometric IDs: Ambitious project, razor-thin window."

[105] National Democratic Institute, *Lebanon 2018 Parliamentary Elections: Final Report,* 21.

Moreover, transgender people in Lebanon already face obstacles accessing ID documents that match their gender identity—which in turn limits their access to basic services like housing, health care, and employment.[106] Threats to their physical safety and security may prevent trans people from going in person to a registration office, while systemic violence and discrimination by state officials may deter trans people from applying for a digital ID.

The universal and mandatory nature of most digital systems can be particularly challenging to those less able to register for and access digital ID. At the same time, some of the most vulnerable people in society are both the least able to access digital ID, and most in need of the services connected to digital ID.[107]

Costs

The high cost of digital and biometric ID systems is a concern, particularly as Lebanon is in a deep economic crisis and reliant on international donors. In 2017, anticipated costs of Lebanon's biometric ID cards and biometric electoral system varied from an estimated 40 million USD[108] to 134 million USD.[109] The Director General for Civil Status, General Elias Khoury, had estimated to the World Bank that overhauling the national ID cards to a digital ID would cost 20-25 million USD.[110] Globally, costs of digital ID vary considerably, but it is "rare to have a system that costs less than 2 USD per person when taking into consideration all the costs of investment and ongoing maintenance,"[111] noted the World Bank staff. A focus on expensive and high-tech systems by the ID industry is concerning, particularly if the infrastructure and capacity in a country is not as high-tech. The World Bank staff continued that:

> *"Some governments tend to focus on technology rather than the purpose of the ID system and the specific types of services or transactions that it will be useful for. For example, while smartcards may be the appropriate solution in some cases, they are not necessarily a great investment in every context and for every purpose. The use of smart cards typically requires card readers at the point of service. If smart cards are meant to be used as transaction authenticators or for people to log into e-government services using a pin or a biometric, this won't always be feasible in many developing countries, as card readers are not available everywhere nor do all people have computers at home."*[112]

" Lebanon's economic crisis raises the question of who would pay for digital or biometric ID systems, and what financial dependencies this might create. "

Since these cost estimates for biometric election cards and digital ID, Lebanon's economic situation has worsened significantly. Lebanon's economic crisis raises the question of who would pay for digital or biometric ID systems, and what financial dependencies this might create. In 2009 the UN Secretary General noted that:

> *"Some processes are more costly per voter than others; and some of the poorest countries in the world have chosen some of the most expensive electoral processes and technology. [...] I am concerned about techniques and systems that might cause a State, in the conduct of its own elections, to be financially dependent on donors, or technologically dependent on specific vendors for extended periods."*[113]

[106] Rasha Younes, "'Don't Punish Me for Who I Am': Systemic Discrimination Against Transgender Women in Lebanon," Human Rights Watch, September 3, 2019, https://www.hrw.org/report/2019/09/03/dont-punish-me-who-i-am/systemic-discrimination-against-transgender-women-lebanon

[107] Vrinda Bhandari, *Governing ID: Use of Digital ID for Delivery of Welfare,* (Centre for Internet and Society India, July 2020) https://digitalid.design/evaluation-framework-case-studies/welfare.html and "Exclusion and identity: life without ID," Privacy International, December 14, 2018, https://privacyinternational.org/long-read/2544/exclusion-and-identity-life-without-id

[108] Marsi, "Biometric IDs: Ambitious project, razor-thin window."

[109] Obeid, "Split over biometric voter ID cards lingers."

[110] Interview with World Bank staff, October 7, 2020.

[111] Ibid.

[112] Ibid.

[113] United Nations, *Strengthening the Role of the United Nations in Enhancing the Effectiveness of the Principle of Periodic and Genuine Elections and the Promotion of Democratization,* (Report of the Secretary General, August 14, 2009), 10, www.un.org/ga/search/view_doc.asp?symbol=A/64/304.

It is difficult to find data on costs of existing biometrics projects in Lebanon, and even more so to understand who is funding these. (As mentioned earlier, Saudi Arabia funded the biometric passports in 2015,[114] and the US government supported Lebanon's Internal Security Forces in 2017 with a 11 million USD upgrade to its IT system and biometrics database[115]—but these are rare examples of publicly available information on funding.) Biometric ID, indeed any kind of digital ID update, would have to be funded by international donors.

Function Creep

The Cabinet's decision to transform the "magnetic voting cards" to biometrics IDs, tied to a number of other social administrative services, raises concerns that the collected personal information could be used for purposes beyond their initial scope, a phenomenon commonly known as function creep. For example, the Directorate General of Civil Status could give security agencies access to the data, putting vulnerable people at risk.

> “ If a digital or biometric ID is installed as part of establishing the database for the social safety net programme, it is critical to ensure that the database and related ID's purpose is limited and well-defined. ”

A news report from the time of the announcement of biometric IDs in elections informed viewers that unlike the "magnetic card" which would be for one-time voting use, the biometric ID would be used not just for elections, but for other government services like claiming social security, for personal civil status matters, and one day even for e-gate border crossing.[116] Inkript noted that biometric election cards are not mandatory according to international legislation, unlike the biometric passports. Investing in a complex and costly system for one-time voting use would be a waste of resources, so "it would be a better investment to issue a new biometric ID card, which may be used for e-government applications."[117] However, broadening the mandate of the "magnetic voting card" to biometric ID, and linking it to additional services, poses further threats to civic inclusion and privacy.

Ministries have been actively working on biometric ID for multiple purposes. On April 19, 2018, "the cabinet approved an item related to the Ministry of Social Affairs regarding the biometric card for the social services centers,"[118] according to Pierre Abu Assi, the Minister of Social Affairs at the time. The World Bank had also been working on a digital economy project for Lebanon, which would have allowed people to access social services and make payments online.[119] There was significant interest and buy-in including from the Ministry of Interior and OMSAR, who met with the World Bank in September 2019 before nation-wide protests began in October 2019, the Ministry of Interior holds the civil registry and databases for elections, passports, national ID, and driving licenses. The digital economy project is currently stalled due to Lebanon's economic crisis, changes in government, and COVID-19 pandemic.

Instead, the World Bank is planning an "Emergency Social Safety Net" project which envisages the development of a national social registry for data management. In December 2020, Michel Aoun, the Lebanese president, announced that Lebanon is currently negotiating a 246 million USD loan from the World Bank in response to the economic crisis, which will finance the Emergency Social Safety Net.[120] A key part of the Emergency Social Safety Net project in the pipeline is to build out infrastructure, including a reliable social registry.

In the near future, it is likely that the driving force for digital ID in Lebanon would be social safety net programs and social services, rather than elections. If a digital or biometric ID is installed as part of establishing the database for the social safety net programme, it is critical to ensure that the database and related ID's purpose is limited and well-defined.

[114] Alieh, "Inkript wins biometric passport tender"

[115] "New U.S. Government-Funded Biometrics Project," US Embassy in Lebanon,

[116] Hajal, "Report: How does the biometric ID facilitate the voting process?"

[117] Interview with member of Inkript leadership team, June 15, 2020.

[118] "Cabinet Approves Public Sector Working Hours," *National News Agency,* April 19, 2018, http://nna-leb.gov.lb/en/show-news/90238/Cabinet-approves-public-sector-working-hours

[119] Interview with World Bank staff, October 7, 2020.

[120] "France and UN rally aid for Lebanon, urge political reforms," *The Daily Star,* December 3, 2020, https://www.dailystar.com.lb/News/Lebanon-News/2020/Dec-03/514978-france-and-un-rally-aid-for-lebanon-urge-political-reforms.ashx

Centralization and Efficiency

Proponents of digital ID argue that it allows for more efficient service delivery, so that governments are better able to identify and deliver services to those who should be receiving them.

When it comes to efficient service delivery, the vision for proponents of digital ID is often a centralized system. A digital ID that is used for multiple services could potentially provide ease of use for citizens and minimize bureaucracy. Critics argue that centralization does not necessarily lead to greater efficiency and less bureaucracy. This vision seems unrealistic in Lebanon currently. Such comprehensive service delivery would require cooperation and collaboration across ministries, which seems unlikely given Lebanon's fractured political landscape and recent frequent changes in ministers. In the last 20 years, as the administrative reform ministry OMSAR has attempted to modernize government, it has faced challenges including resistance to change, a refusal to share information, and incompatible systems and processes.[121] Severe budget cuts in ministries in 2020, particularly UNDP stopping funding units in government ministries including OMSAR,[122] are an additional barrier to implementing the kinds of systems and data architecture needed.

There have been issues with databases for delivering government services. In an interview, World Bank staff noted: "The current systems make it difficult to digitally verify or authenticate people's identity or specific attributes, because the civil register is not digitalized, and the national ID system is closed and not accessible. Furthermore, there is no nation-wide digital infrastructure for people to securely authenticate who they are, either via the national ID card or some other method."[123] In an attempt to remedy this issue, the World Bank's 246 million USD Emergency Social Safety Net (ESSN) tasks the recently created Inter-Ministerial Committee for Social Affairs with oversight of the database, a Central Management Unit (CMU) in the Presidency of the Council of Ministers with hosting the database, and the Ministry of Social Affairs with the "technical implementation," but it is not clear if the database will be fully centralized.[124]

Moreover, there are more pervasive issues with social assistance distribution in Lebanon that may render the World Bank's plan ineffective, demonstrated by criticisms of the government's response to the pandemic and the August 4 Beirut Port explosion. According to a recent Siren Analytics report, aid distribution by the Lebanese government in 2020 "raised concerns in regards to the transparency, impartiality, and efficiency of the aid distribution process, tarnishing the overall credibility of state-driven response"[125]—but it is not clear that the implementation of a digital ID system would remedy these pervasive concerns. The report found that different ministries had contradicting numbers for the number of families in need of aid and in some cases were using outdated data, and highlighted bias, lack of impartiality, and data privacy concerns in assessments and distribution.[126] Although Siren Analytics has partnered with a government oversight body, Central Inspection, to launch the Inter-Ministerial Platform for Assessment, Coordination, and Tracking (IMPACT) which collects data from local municipalities and ministries to streamline service delivery—and they have a vested interest in promoting IMPACT over existing data systems—these issues are noteworthy. The introduction of a digital ID system might help mitigate some of these service delivery inefficiencies, but longstanding transparency and data privacy issues would likely persist, further jeopardizing people's sensitive data.

Privacy

The privacy and security of individuals' data is the main risk of biometric and digital ID systems, as a member of Inkript's senior leadership team noted:

> *"The main risk is about privacy protection. Today when we deal with any identification system or any system*

[121] Najib Korban, "OMSAR ICT Achievements," *First National Digital Government Conference, Grand Serail Beirut,* May 4-5, 2017, http://digitalgovernment.omsar.gov.lb/Presentations/ICT_Presentation.pdf

[122] Interview with World bank staff, October 7, 2020.

[123] Ibid.

[124] World Bank, *Project Information Document,* Lebanon Emergency Crisis and COVID-19 Response Social Safety Net Project.

[125] Siren Analytics, "Aid Distribution in Lebanon: An Assessment, November 2020, 8, https://www.sirenanalytics.com/files/Aid-Distribution-November-2020.pdf?id=100

[126] Ibid.

> *that is storing personal data, the main concern would be the privacy issues. But that is not related in my opinion specifically to biometrics. It is related to any personal information."*[127]

Digital ID, as systems which may be used for multiple services, can more readily enable tracking and surveillance and they are vulnerable to cyber security attacks, potentially infringing rights like freedom of expression and the right to privacy. According to digital rights non-profit organization Access Now:

"The problem is accentuated in countries with a lack of comprehensive privacy and surveillance frameworks, compromised institutional standards, and weak independent enforcement. In such countries, financial incentives become stronger for governments and private businesses to delay and dilute privacy and data protection standards, while enabling risky digital identity programmes."[128]

Furthermore, biometric data is an even riskier category of personal information. This is because biometric indicators are immutable—irises and fingerprints cannot be changed if data is hacked or leaked. Biometric data poses a higher security risk, as the damage done by leaks and hacks cannot be repaired and thus it's difficult to restore sanctity to biometric-based ID systems.[129]

Most critics of national digital ID systems highlight that one of the biggest risks to data privacy and security is the aforementioned centralization of large quantities of sensitive personal data, as governments collect and store data on a central database. By virtue of its centralization, it facilitates the sharing of sensitive data between third parties, and can be more readily used for surveillance and tracking of citizens.

Yet, the decentralization of registry databases in Lebanon also facilitates a lack of oversight and can lead to security vulnerabilities, endangering individuals' privacy. As Inkript staff noted, digital identity system providers like their company do not collect data themselves —rather, they provide tools for government customers to protect citizens' data.[130] The ministry or security agency that collects the sensitive personal data stores it. Without clear legal and technical frameworks in place, data may be shared, leaked, and is vulnerable to cyber security attacks and surveillance. As this section explores, the Lebanese government is not able to adequately protect people's data.

Data Sharing

It is unclear to what extent the government shares data between ministries or agencies, or receives data from aid agencies. In 2014, there were fears that the iris scans that UNHCR collected during refugee registration were shared with the Ministry of Social Affairs, after comments from then Social Affairs Minister Rashid Derbas saying that they had the iris scans of Syrian refugees on the record. He later clarified that "while the government didn't currently have the biometric data, it was working with UNHCR to 'establish a system that would turn the data over to General Security.'"[131] He continued: "'Why wouldn't they [UNHCR] give it to us, they are working on Lebanese territory.'"[132] At the time, UNHCR staff rejected the idea that data would be shared with the government.[133] While there has not been any known sharing of biometric data between UNHCR and government agencies, this example demonstrates a disregard for data privacy, particularly from the Ministry of Social Affairs (which leads the implementation of social safety net programs, where digital ID is most likely to be introduced in the near future).

Data Leaks & Management Issues

The Lebanese government has had a number of issues protecting personal data over the past few years, including data related to elections. During the 2018 parliamentary elections, Lebanese embassies in the Netherlands and the United Arab Emirates (UAE) circulated Excel sheets

[127] Interview with member of Inkript leadership team, June 15, 2020.

[128] "WhyID," Access Now

[129] Ibid.

[130] Interview with member of Inkript leadership team, June 15, 2020.

[131] Elise Knutsen and Meris Lutz, "Lebanon seeking refugee biometric data: Derbas," *The Daily Star,* May 30, 2014, https://www.dailystar.com.lb/News/Lebanon-News/2014/May-30/258268-government-has-refugee-eye-scans-derbas.ashx

[132] Ibid.

[133] Ibid.

containing full voter records to all registered voters in those countries.[134] The personal information in the spreadsheets in both the UAE and the Netherlands included each voter's full name, mother's name, father's name, gender, date of birth, religion, marital status, and address. In November 2017, the Lebanon Diaspora Vote website, which was used to register voters from abroad, also tracked cookies of all users without asking for consent. Both of these examples demonstrate the government's lack of competence in handling sensitive voter information, and disregard for data privacy The introduction of biometrics would only create greater risk to citizens by adding further personal identifiers.

In 2017, journalists from Al-Jadeed gained access to the leaked personal data of all citizens and residents who own a car in Lebanon. The data was "unencrypted and unprotected,"[135] suggesting that personal data may not be stored in a secure way by the Traffic, Trucks, and Vehicle Management Authority. Moreover, vehicle registration data is leaked annually, including "private and personal data such as the registered car owner's full name, along with their date and place of birth, registration number, place of residence, cell number, and home phone number."[136] This is all the more concerning as vehicle registration data may be easily linked to driving license data, and other databases which store biometric data.

Cybersecurity Breaches

Then there are examples of cybersecurity breaches. In 2019 at a panel at the American University of Beirut, Major Marc Sawan, head of the Internal Security Forces' Digital Forensics and Cybercrime Unit, gave an example of a hacking attack over 2017-2018, resulting in at least 80 governmental sites being hacked. We do not know if any citizen data was compromised in this attack or others.

In 2018, researchers also uncovered "Dark Caracal," a cyberespionage campaign originating from General Security and targeting military personnel, enterprises, medical professionals, activists, journalists, and lawyers based in Lebanon and 20 other countries.[137] The huge quantities of stolen data, 80 gigabytes, were discovered by researchers on an unsecured open server. Once the server was found, researchers could just browse through it to access the data, no hacking needed.[138]

Concerns for Digital and Biometric ID

These examples demonstrating extensive security breaches, data leaks, insecure servers, and surveillance of citizens, are worrying when considering the sensitive and immutable personal and biometric data stored by government ministries and security agencies. Adding to this concern, we do not know how sensitive personal data is stored by government ministries collecting it, and what the policies are for managing data, such as who is given access. Clear data management policies that are enforced would help to minimize the risk of data sharing, leaks, or security breaches by nefarious actors.

Adding to this is the position of private sector companies providing biometric technologies, who tend to absolve themselves of responsibility for citizens' and residents' data privacy and security. Companies we spoke with were clear that they provided the technology and the tools, but that the contracting government or humanitarian actor bore responsibility for the data. Eva Mowbray, Director of Marketing for IrisGuard, which provides iris scan technology to UNHCR in Lebanon, claimed there are "no risks related to the operation in Lebanon since there is no data stored inside the country at all, [and] the UNHCR systems are managed and maintained by UNHCR outside the region, eliminating the possibility of data breaches and abuse."[139] While we were not able to reach UNHCR for comment, there are always risks when collecting huge quantities of data; and we have already explored the data sharing demands on UNHCR made by the Minister of Social Affairs in 2014.

[134] "Lebanese Embassies Expose the Personal Data of Registered Voters Living Abroad," SMEX, April 6, 2018. https://smex.org/lebanese-embassies-expose-the-personal-data-of-registered-voters-living-abroad/

[135] Barjas and Mehdy, Building Trust, 15.

[136] Ibid.

[137] Lookout & Electronic Frontier Foundation, *Dark Caracal: Cyber-Espionage at a Global Scale,* January 18, 2018, https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf

[138] Kaveh Waddell, "Who Is Selling Hacking Subscriptions to Governments?" *The Atlantic,* January 19 2018, https://www.theatlantic.com/technology/archive/2018/01/lebanon-hacking-subscription/551009/

[139] Email exchange with Eva Mowbray, IrisGuard, June 10 2020.

Yemen: Biometric elections, international actors and data risks.

Yemen offers an example of multinational aid funding companies to implement a multi-million dollar biometric ID system for elections with dubious privacy standards and without sufficient safeguards in place.

Yemen was set to launch a biometric voter registry for the 2014 election, funded by Sweden, Saudi Arabia, the United States of America, the United Kingdom, Denmark, Japan, Turkey and the European Union, with support from the United Nations Development Programme (UNDP) and the International Foundation for Electoral Systems (IFES).[140] In 2013, three companies from Belgium, France, and the Netherlands were invited to showcase their technologies.[141] UNDP reported that system tests were carried out at two elementary schools in Sanaa, where "more than 100 boys and 100 girls participated in the mock exercises in order to test the equipment in a 'real life' setting."[142] However, it seems strange to test a biometric ID system for elections on children who are too young to vote and would not be the ones actually registering; they do not accurately reflect the voting population. More worryingly, the mock registration of elementary students is concerning as the test would have involved collecting biometric data such as fingerprints and images of the faces of minors. The UNDP report does not mention if and how the informed consent of these children and their parents was obtained prior to testing. Nor does it state what was done with the biometric data after the test. Was it deleted, or did these private companies keep the personal data of 200 Yemeni children? If the data was retained, how has it since been used?

It seems likely that one of the three companies which tested technology was Gemalto, the Franco-Dutch company also responsible for Lebanon's biometric passports, as Gemalto was selected in late June 2013 for the procurement and technical support of Biometric Voter Registration kits.[143] In 2014, American company M2SYS announced that its software was selected as the biometric voting platform, funded by USAID.[144] However, it is unclear if this was a complementary or replacement system to Gemalto. A pilot was rolled out in May 2014 for what was set to be the first biometric voter registration system at scale in the region,[145] but Yemen's 2014 election was postponed due to violence, and has yet to take place. Even during the testing phase, the case of Yemen's biometric election ID demonstrates a combination of international donors' and private sector companies' disregard for privacy, all the more reprehensible as it involved minors.

[140] "Testing biometric voter registration kit - The future of elections in Yemen," UNDP Arab States, June 17, 2013, https://www.arabstates.undp.org/content/rbas/en/home/presscenter/articles/2013/06/17/testing-biometric-voter-registration-kit-the-future-of-elections-in-yemen.html

[141] Ibid.

[142] UNDP Yemen, *Support to Elections during the Transitional Period (SETP II) - Annual Progress Report 2013,* https://info.undp.org/docs/pdc/Documents/YEM/SETP%20II%20Annual%20Report%202013.pdf

[143] Ibid.

[144] "M2SYS Technology Deploys TrueVoter™ Biometric Voter Registration Software Solution In Yemen" M2SYS, August 19, 2014, https://www.m2sys.com/m2sys-deploy-truevoter-yemen-biometric-voter-registration-solution/

[145] UNDP, "Yemen's Election Commission Rolls out Biometric Voter Registration Pilot," *Reliefweb,* May 10, 2014, https://reliefweb.int/report/yemen/yemens-election-commission-rolls-out-biometric-voter-registration-pilot

Legal Frameworks

Lebanon's current legal frameworks are not robust enough to support the introduction of digital and biometric ID for the purpose of verification or authentication. The main data protection framework, the E-Transactions and Personal data Law has many shortcomings. While it provides some oversight, it fails to adequately protect individuals' personal information, concentrating power with the executive branch of government, especially the Ministry of Economy and Trade. The law does not offer the same safeguards that are standard in current international data protection legislation.[146] Moreover, there is no evidence that the law has been actively implemented. At the same time, a number of other decrees and decisions threaten to exclude vulnerable populations, including refugees and migrant workers. The introduction of digital and biometric ID for elections or social services, without adequate legal protections, stands to both jeopardize people's personal data and leave out more vulnerable members of the community.

Data Protection

Lebanon's data protection regime, or lack thereof, does not adequately safeguard citizens' and residents' data. Weak legal frameworks often result in digital ID systems that are vulnerable to leaks and hacks, and can jeopardize the sanctity of individuals' personal data. For instance, without strong data protection laws, or an independent data protection authority, political parties could potentially access election data and learn sensitive information, such as who individuals voted for. Furthermore, the mandatory nature of many biometric identification programs leaves every citizen exposed if governments, or the private companies they have contracted with, mismanage them.

International guidance from GSMA, the World Bank and the Security Identity Alliance, on implementing biometric ID stresses the importance of having sufficient legal frameworks and protections in place:

> *"Countries that choose to adopt digital identity systems must have robust legal and technical frameworks for data protection and privacy. Missteps in handling citizen data can erode trust in government and decrease the value of the system, threatening revenues and the efficiency gains derived from personal data applications."*[147]

> " The World Bank described the data protection provisions in the E-Transactions and Personal Data Law as not yet sufficient to meet global standards on data protection. "

Yet, Lebanon's current legal and technical frameworks for data protection and privacy are anything but robust. The main legal framework governing data use in Lebanon is the E-transactions and Personal Data Law, initially proposed in 2004, and eventually passed in September 2018. The law does not meet current best practice in data protection regulations partially because it is based on a regime that was applicable in 2004 in France—European Legislation from 1995—which was replaced by the General Data Protection Regulation (GDPR) in 2016. In an interview, the World Bank described the data protection provisions in the E-Transactions and Personal Data Law as "not yet sufficient to meet global standards on data protection."[148]

The E-Transactions and Personal Data Law in theory offers some data protections. Individuals whose data is being collected have the right to be informed about purpose (Article 87), right to review (Article 86), right to object, right to access their data (Article 99), and right to amend incorrect or incomplete data (Article 101).[149] Those collecting data are also required to share information when collecting data about the nature of the processing (Article 88), and the period during which personal data will be retained (Article 90).[150]

[146] SMEX, "An 'Ugly' New Data Protection Law in Lebanon," October 11, 2018, https://smex.org/an-ugly-new-data-protection-law-in-lebanon/

[147] GSMA, World Bank, and Security Identity Alliance, *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation,* 14.

[148] Interview with World Bank staff, October 7, 2020.

[149] *Law No. 81 Relating to Electronic Transactions and Personal Data,* issued on October 10, 2018, https://smex.org/wp-content/uploads/2018/10/E-transaction-law-Lebanon-Official-Gazette-English.pdf

[150] Ibid.

In practice, these limited protections offered by the E-Transactions and Personal Data Law would likely not apply to a newly introduced digital or biometric ID system, due to the exemptions granted to the executive branch, and the lack of enforcement of the law.

The law does not establish a standalone data protection authority, placing this responsibility with the Ministry of Economy and Trade.[151] This means that the data protection authority is not an independent oversight body, but rather a part of government, and this authority is concentrated in just one ministry, which increases the risk of abuses of power and arbitrary decision making. Lacking checks and balances, the data protection role of the Ministry of Economy and Trade leaves the data of Lebanese citizens and residents vulnerable.[152]

The law requires a permit or license to process personal data, except in cases outlined in Article 94. This also gives the Council of Ministers, the Ministry of Justice, and the Ministry of Economy and Trade the right to exempt entities from authorization and licensing procedures.[153] In current plans proposed by the World Bank, the Emergency Social Safety Net registry database would be housed in a unit within the Presidency of the Council of Ministers. One of these ministries could decide to exempt themselves or whichever ministry was managing a new digital ID system, from the regulations outlined in the law—the Council of Ministers could potentially exempt itself.

Article 97 gives the Ministries of Defense, Interior and Municipalities, Justice, and Health, the authority to give licenses related to data under their jurisdiction. For example, the Ministry of Defense can give licenses in cases concerning "external or internal security of the state," which is not defined by the law. Effectively, the government could claim that a digital ID system used for authenticating identity concerns the internal or external security of the state and it would not be subject to the law. The law also gives the Ministry of Economy and Trade the ability to give third parties access to data and to transfer it to foreign states (Article 95). For private companies implementing biometrics, their clients are the government ministry, security agency, or aid agency contracting them, not the citizens, residents, or refugees, whose personal data is being collected. Therefore, there is virtually no accountability for private companies working with the government.

The E-Transactions law has not yet been enforced and it is even less likely that it would be applied to government agencies. When the law was passed in 2018, sources in the Ministry of Economy and Trade told SMEX that there had been no preparation to implement the law.[154] With budget cuts across the government, the possibility of enforcement and a real data protection authority appears slim.

When asked about current legal frameworks, a member of the senior management team of Inkript, which implements biometric ID systems, said:

> *"The law is not enough. It requires decrees and additional administrative decisions to have a concrete framework for data protection; something similar to GDPR, where people can access their data, correct it, and where you have a very viable auditable system regarding the handling of personal data in line with the regulations."*[155]

Given these shortcomings, if the government were to adopt a biometric election ID or a more comprehensive digital ID, the current data protection law should be replaced.

[151] Myriam Mehanna, "Notes on the Electronic Transactions Law: Freedom of expression at the mercy of the Public Prosecution" The Legal Agenda, May 31, 2019, https://www.legal-agenda.com/article.php?id=5625

[152] SMEX, "An 'Ugly' New Data Protection Law in Lebanon"

[153] *Law No. 81 Relating to Electronic Transactions and Personal Data.*

[154] SMEX, "An 'Ugly' New Data Protection Law in Lebanon."

[155] Interview with member of Inkript leadership team, June 15, 2020.

Tunisia: civic activism to safeguard privacy

In Tunisia, a draft law was initiated and developed during 2016-2017, which proposed replacing the identity cards with a chip-enabled biometric one. However, civil society activists questioned the vagueness of the bill, arguing that it threatened the right to privacy enshrined in the constitution. They asked questions like:

- “What kind of personal data will be stored in the encrypted part of the new identity card?
- What institution is charged with determining which personal data are stored, and if personal data are stored, exactly how long will it be stored for? Is there a limit to how long the information is retained?
- Is there any kind of procedure that government authorities must undertake to gain access to a database that contains the personal data of millions of citizens?
- How is the database secured?
- How come the law does not mandate the creation of an independent commission to address these questions?”[156]

They also noted the high cost and lack of actual benefit to Tunisians, without safeguarding privacy. In 2018, civil society and the national data protection authority persuaded lawmakers to adopt amendments “to ensure that if it did pass, the bill would protect citizens’ data and their right to consult and rectify their own information.”[157] With these changes, the Ministry of Interior dropped the proposed bill. It’s been speculated that possibly “they could not move forward without giving the unnamed company access to citizen data.”[158]

[156] Wafa Ben-Hassine, “Tunisia’s ‘Aadhaar’? Read the draft law for a dangerous new ID, now in English,” Access Now, 30 August 2017, https://www.accessnow.org/tunisias-aadhaar-read-draft-law-dangerous-new-id-now-english/

[157] Emna Sayadi, “Biometric ID vs. privacy: Tunisians win on privacy! But it’s not over yet,” Access Now, January 11, 2018, https://www.accessnow.org/biometric-id-vs-privacy-tunisians-stood-privacy-not-yet/

[158] Sara Baker, What to Look for in Digital Identity Systems: A Typology of Stages, (The Engine Room, 2019) 6, https://www.theengineroom.org/wp-content/uploads/2019/10/Digital-ID-Typology-The-Engine-Room-2019.pdf

Discrimination

Beyond the issues with the legal framework for data protection, there are a number of other legal issues that could disenfranchise some of the most vulnerable people in Lebanon in the event that a digital ID system tied to service provision was introduced. Even if the system only initially serves Lebanese citizens, as we detailed above, these systems always pose the risk of function creep.

For example, in 2019, only 22% of Syrian refugees in Lebanon above the age of 15 had legal residency, which General Security and the Lebanese government have made progressively harder to acquire, according to a Vulnerability Assessment of Syrian Refugees in Lebanon.[159] Although UNHCR has supported General Security to expand the residency system (including "the installation of a complete biometric enrolment and resident card personalization software"[160]) the percentage of Syrians not holding a residency permit has increased from 2018.[161] This was due to factors like the cost of registration, entering through an unofficial border crossing, and the challenges of finding a Lebanese sponsor.[162] With less than a quarter of Syrian refugees in Lebanon maintaining residency permits, any digital ID system used for verification or authentication would almost certainly exclude them.

Likewise, the oppressive Kafala system, which ties migrant workers' legal status to their employment status, also presents significant challenges. Although they may hold a biometric work permit, migrant workers are excluded from the protections of the labor law, and instead their employment is regulated through the Standard Unified Contract which provides little protection.[163] Specifically, the contract allows employers to terminate a contract for arbitrary reasons and only allows a worker to terminate a contract if they are not paid for three months or if they face physical or sexual abuse.[164] However, in cases where they do face abuse, the burden of proof resides with the worker, and they must provide forensic evidence or an investigation from the police or the Ministry of Labor. These contracts are also often signed in Arabic, which many of the workers cannot read, so they may not be aware of the limited protections afforded to them.[165] Ultimately, the ability of these workers' employers to exert control over their legal status could prevent migrant workers from accessing any services tied to a digital ID.

Transgender people could also face legal discrimination if the government rolled out a biometric ID tied to voting or social assistance. Currently, the only way for trans people to change their gender is through the courts, which can be both lengthy and costly. Moreover, courts often only agree to change an individual's gender marker if they have undergone surgery.[166] Without an easier avenue for officially changing their gender, trans people could be barred from voting or accessing social assistance.

Other populations, including Palestinians and people who identify as LGBTQ, could also face discrimination, especially if there is no clarity around how data is stored and shared.

[159] UNHCR, UNICEF, WFP, *VASyR 2019: Vulnerability Assessment of Syrian Refugees in Lebanon,* December 23, 2019. https://data2.unhcr.org/en/documents/details/73118

[160] UNHCR, *Operational Update, Lebanon: 3rd Quarter Update, July - September 2017,* 2

[161] UNHCR, UNICEF, WFP, *VASyR 2019.*

[162] Ibid, 34.

[163] "Statement of 'My Work, My Rights' Network on the Standard Unified Contract," Anti-Racism Movement Lebanon, October 23, 2020, https://armlebanon.org/content/statement-%E2%80%9Cmy-work-my-rights%E2%80%9D-network-standard-unified-contract

[164] Amnesty International, *Their House is My Prison: Exploitation of Migrant Domestic Workers in Lebanon,* April 2019, https://www.amnesty.org/download/Documents/MDE1800222019ENGLISH.pdf

[165] Ibid.

[166] Rasha Younes, "'Don't Punish Me for Who I Am': Systemic Discrimination Against Transgender Women in Lebanon."

Conclusion & Recommendations

With digital and biometric ID, as with all technology, we need to ask: why do this at all? What problem is the government trying to solve with digital or biometric ID? Are there other ways to solve this problem? What are the risks, and are they worth it?

The introduction of a biometric ID for elections would not address the electoral issues currently facing Lebanon, and may even exacerbate existing problems. The dilemmas Lebanon faces related to voter registration, authentication, and place of voting, would continue to exist even with biometric ID because they require broader political reforms. As cases from other countries show, introducing biometric ID may cast doubt over election results, diminishing trust and credibility. Additionally, the introduction of a biometric ID comes with high costs and it is unlikely that Lebanon's electricity and internet infrastructure could sustain such a system. The proposal of a biometric ID also presents the risk of function creep and could push the state to consider tying an increasing number of its services to digital ID.

Already, it appears that a digital ID system linked to social services could be introduced in the near future, even though concerns around infrastructure, reliability, exclusion, and privacy would still apply. The privacy concerns are particularly worrisome as time and time again, Lebanese ministries and agencies have failed to protect the personal data of citizens and residents. With a weak legal framework in place, there is no guarantee that a digital or biometric ID would protect individuals' privacy, and could potentially facilitate the sharing of their personal data across state agencies or expose personal data to malicious third parties.

Based on the findings of our research, we propose key recommendations for the Lebanese government and international donors concerning the possible introduction of any future digital or biometric ID including for social assistance.

Recommendations to the Lebanese Government

1. Fight electoral fraud through electoral reform, not biometric ID

Implementing a biometric ID system and using biometric or magnetic elections cards will not tackle the kinds of irregularities seen in previous elections. Worse still, using biometric IDs to register voters beforehand, and authenticate their identity on election day would likely exclude some people, particularly from marginalized groups. Lack of reliable infrastructure combined with the technical complexity of biometric ID could cast doubt on the credibility of the election, diminishing confidence in the results.

- The Lebanese government should not introduce biometric ID for future elections.

- Instead, the government should legislate for and implement election reforms recommended by civil society and election observers recommend, such as creating an electoral roll and allowing voters to elect candidates in their place of residence.

2. Strengthen legal frameworks

Current legal frameworks, notably the E-Transactions and Personal Data Law, offer insufficient data protections. Before any new digital ID is introduced, including for social assistance programs, Lebanon must introduce stronger legal frameworks for data protection and against discrimination and exclusion.

- The Lebanese government should strengthen the law by nullifying the current data provisions in the E-Transactions and Personal Data Law and replacing it with a stand-alone data protection law which aligns with the General Data Protection Regulation (GDPR) and other relevant international frameworks. Given the gaps with the current Lebanese law, and the compliance burden of a law like GDPR, particularly during the current economic crisis, it may make sense to look to countries like Georgia and Armenia to adopt an interim data protection law. However, Lebanon should establish any such interim data protection regime with eyes on bolstering it and eventually aligning with GDPR standards.

- The Lebanese government should push for more administrative decisions and decrees to create a concrete framework to protect personal data, such as:

    - Establish an independent data protection commission or authority.

    - Limit the exemptions granted to the executive branch, including the Ministry of Interior and Municipalities, Ministry of Defense, and the Ministry of Health.

- The government should adopt and enforce anti-discrimination legislation and other measures to ensure that no one is denied services on the basis of their gender identity or legal residency status, and to ensure that services are accessible by means other than digital ID.

- Contracts should hold private sector companies implementing digital and biometric ID accountable to citizens and individuals whose data will be collected, not just the government ministry or security agency collecting the data. Private sector companies' obligations should go beyond just providing digital and biometric ID for government clients.

3. Ensure sufficient technical infrastructure is in place

Before introducing any digital ID for social service provision, the Lebanese government must ensure that it has the proper infrastructure to support such a system. Namely, Lebanon needs improved supply of and affordable access to electricity and WiFi, not just in Beirut, but across the country, otherwise these systems could discriminate against vulnerable people. Similarly, international donors should not press for the introduction of new, technologically advanced systems before the government has ensured that the technical infrastructure is in place to sustain such a system.

4. Increase transparency around digital and biometric ID procurement and implementation

There is little publicly available information on how biometric data is stored by the government, and who it is shared with, both within Lebanon (i.e. other government ministries and security agencies) and internationally (by security companies). Procurement processes and contract award information are not easy to find or access, and it is often unclear who is funding these projects. Improving procurement transparency would demonstrate value for money and help fight corruption.

- The Lebanese government should make public calls for proposals, tenders, and contract amounts, including information about funding sources due to both the high cost of digital ID and the sensitive nature of the data that these companies have access to.

- When holding sensitive personal information, the Lebanese government should share privacy policies publicly so the public can better understand what obligations the contractor has to the government and vice versa.

- The Lebanese government should share information on data processing procedures for all identification (i.e. how all our personal data including biometric data is collected, stored, used, published and shared).

- International organizations seeking digital ID as part of their projects, should demand best practices in procurement and data collection, storage, management, sharing, security, and protection.

Recommendations to International Donors

In addition to requiring the Lebanese government to abide by the recommendations in the previous section, international donors proposing digital ID for a social safety net program or any other purpose, should also:

5. Refrain from supporting biometric ID for the purpose of fighting electoral fraud in Lebanon

International donors should insist on election reform recommendations put forward by civil society and election observers, instead of supporting a biometric ID system as the answer for Lebanon's vast electoral issues.

6. Consult all stakeholders around digital and biometric ID

International donors should consult citizens and residents in Lebanon, particularly those that might be disproportionately affected by digital or biometric ID, such as elderly people, disabled people, LGBTQI people, Palestinians, Syrians, and migrant workers. Civil society organizations should also be consulted. Engagement of all stakeholders is vital, to listen to people who will be the 'end users' or recipients of digital ID.

International donors should:

- Produce a publicly available impact assessment, outlining the risks, before any digital ID or biometric ID is introduced.

- Hold consultations with 1) civil society organizations and 2) people whom the ID is intended for, particularly those who are more likely to be adversely affected by digital or biometric ID.

7. Refrain from excessive centralization of databases

Although there are undoubtedly issues and redundancies with government databases in Lebanon currently, centralizing these databases should not be touted as a fix-all solution. Efforts towards centralization are often costly and technically complicated. More importantly, given Lebanon's extremely weak legal framework for data protection, centralization would pose further privacy risks. Instead international donors should:

- Conduct an audit to identify any redundancies in the system and work to eliminate these instead of pushing for centralization of all databases

- Invest in digitizing the civil register

8. Do not mandate digital ID system for provision of social safety benefits

Given the infrastructural and political challenges facing Lebanon, as well as the privacy concerns and data protection risks, citizens and residents should have the choice to not hold a digital or biometric ID in order to access government services. The most vulnerable members of society are the most likely to be excluded by digital and biometric ID, facing greater barriers to register for digital ID or prove their identity (such as adermatoglyphia.) As such, digital ID should not be mandatory to access any government services, and particularly social assistance. People must always have another way to access these crucial services.