POLICY PAPER

Biometric Data in Jordan
Table of Contents

Context

Introduction

Biometric Data Collection and Usage in Jordan

Relevant Jordanian Legal Frameworks

Selected International Examples of Biometrics Regulation

General Data Protection Regulation (GDPR)

The Indian Personal Data Protection Bill - 2018

California Consumer Privacy Act (CCPA)

Policy Options

Criteria/Considerations

Assessments of Policy Options

Recommendations

References
Introduction

Biometric data is unique data, generated from characteristics of humans, may be used to track and profile people across their lives. Generally, biometrics enable automated recognition of individuals or automatic identification. Most used systems nowadays rely on fingerprints, iris scans, face features, voice patterns, and DNA sequences.

Biometric technologies may pose grave threats to privacy and personal security, as their application can be broadened to facilitate discrimination, profiling, geolocalization, and mass surveillance. Biometrics are the “passwords you cannot change”. Indeed, individuals cannot practically generate new face IDs or reissue fingerprints if they do not want to be tracked or if their biometric data got leaked, making such an incident effectively a lifetime risk. Unauthorized or unintentional disclosure of biometric data may lead to identity theft, unauthorized access to buildings or systems by criminals, and any resulting consequences.

A very alarming possibility that biometric data enables is mass surveillance. Powered by artificial intelligence, processing biometrics facilitates real-time tracking and classifying of billions of people, rendering dystopian futuristic predictions into a practically realizable possibility. Accordingly, and in an attempt to mitigate the risks associated with biometrics, calls have been made for permanently stopping all biometric processing in public spaces, and anywhere it has the potential effect to establish mass surveillance. Campaigns like Reclaim Your Face aim to ban all kinds of mass surveillance, believing that facial recognition can and will be used against everybody from governments to corporations.
Based on all that, policies that govern the collection, use, and processing of biometric data today are crucial for our future, and this paper attempts to present and evaluate the current status of biometric data in Jordan, and suggest the best course of action according to global best practices.

**Biometric Data Collection and Usage in Jordan**

The following points give a broad picture of the status quo of biometric data collection and processing in Jordan:

- Biometric data stemming from fingerprints and iris scans is already being implemented into ID cards in Jordan, to serve as an additional means of verification⁴, and plans to integrate biometric chips in passports were announced⁵.

- The practice of collecting fingerprints to monitor employee attendance, arrival and departure times, is a pervasive practice in Jordan. Small companies, big corporations and government entities use (or used to use) such systems on a daily basis. Also, some gymnasiums and other shared spaces utilize fingerprints to authorize entry to them. Yet, it’s worth noting that the government issued instructions that require using alternative methods to fingerprints to monitor employees’ working hours⁶.

- At least one bank in Jordan collect biometrics such as iris scan to identify and verify clients at ATM machines.⁷

- The Office of the United Nations High Commissioner for Refugees (UNHCR) has implemented a biometric program in Jordan that requires refugees to use eye scanners to receive cash assistance,
established through a public-private partnership with the Jordanian company Iris Guard.\textsuperscript{8,9}

➔ Commercial banks are required to use fingerprints or iris scans as valid forms of signatures for people with disabilities, based on the instructions for banking services provided for people with disabilities\textsuperscript{10}.

➔ Foreign residents in Jordan need to submit ten-digit fingerprints and iris scans at a police station according to the instructions for determining the place of residence for non-Jordanians\textsuperscript{11}. Also, the government collects Iris scans of Syrians in Jordan in order to give them cards that can make their access to services easier\textsuperscript{12}.

➔ In 2018, the TRC announced that a biometric system for mobile and internet SIM card registration would be established, requiring users to submit their fingerprints.\textsuperscript{13,14} Yet, no further news about that was published.

\textbf{Relevant Jordanian Legal Frameworks}

Several legal frameworks organize the right to privacy in Jordan. Most importantly, the Jordanian constitution protects the right to privacy in several instances. For example, Article 18 of the Jordanian Constitution emphasizes correspondence and communications secrecy:

"All postal and telegraphic correspondence, telephonic communications, and the other communications means shall be regarded as secret and shall not be subject to censorship, viewing, suspension or confiscation except by a judicial order in accordance with the provisions of the law."
Article 18, though focuses on privacy from a communications secrecy standpoint, emphasizes privacy as a major right of Jordanians and is considered evidence of the importance of privacy in the Jordanian fundamental principles.

Also, article 7/ii of the Jordanian constitution stressed on the sanctity of the private life of Jordanians, specifying that any breach must be punishable by the law:

"Every breach of rights and public freedoms or the sanctity of the private life of Jordanians is a crime punishable by law."

Traditionally, fingerprints have been used as an alternative to hand signatures, especially for illiterate individuals. Accordingly, in tens of laws or regulations, especially older ones, law articles refer to “signatures or fingerprints” as ways to prove written consent. This practice, however, started long before automatic biometric processing became readily available.

Civil Status Law of 2001 allows the Department of Civil Status to collect the fingerprints of any Jordanian or resident in Jordan and add them to a database for that purpose. It also permits courts, ministries, official departments and institutions, public commissions, and municipalities to use the collected biometric data, while other entities need the approval of the Minister of Interior affairs before receiving access.

Interestingly, the final draft of the Personal Data Protection law, published by the Legislation & Opinion Bureau, has no explicit reference to biometric data. The draft law defines ‘sensitive personal data’ as a special category of ‘personal data’ and excludes ‘contractual necessity’ as a legal basis for processing for this category of data. Nonetheless, biometric data, despite its sensitivity, is not necessarily regarded as ‘sensitive personal data’ according to its stated definition, and gives room for interpretation in that aspect. Supposedly, the long-awaited-for Personal Data Protection law would tightly defend the personal data of Jordanians, so its failure to protect biometric
data on any level is a signal of the government's lack of awareness of the sensitivity of biometrics or lack of willingness to change the status quo.

Selected International Examples of Biometrics Regulation

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) describes itself as the toughest privacy and security law in the world\textsuperscript{16}. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The regulation was put into effect on May 25, 2018. The GDPR levies harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros.\textsuperscript{16}

GDPR defines biometric data as: “personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data” (Art. 4 [14]).\textsuperscript{17}

Biometric data is classified as a special category of sensitive personal data under GDPR, implying that processing and protecting must proceed under a framework reserved for sensitive personal data generally.\textsuperscript{18} The GDPR also defines biometric data broadly and empowers Member States to pursue divergent protections for biometric data. In many cases, it requires conducting privacy impact assessments before biometrics processing.
providing better protection for individuals from intended or unintended violations.

In this context, it is worth mentioning that because the employer has authority over the employee and the employee is financially dependent on the employer, permission from an employee to an employer in principle cannot be considered as freely given. Accordingly, since employers generally cannot base employees personal data processing on the ground of consent, another legal ground must apply before processing. This means that employers cannot process employees fingerprints, for instance, to use it as a check-in mechanism, just because employees gave their consent. Instead, they need other valid processing grounds such as Legitimate interests (e.g. high security spaces).

The Indian Personal Data Protection Bill - 2018

The Indian personal data protection bill defines biometric data as: facial images, fingerprints, iris scans, or any other similar personal data resulting from measurements or technical processing operations which allow or confirm the unique identification of that natural person. Unlike the Jordanian personal data protection draft law, the Indian counterpart explicitly categorizes biometric data as “sensitive personal data” and thus requires explicit consent (informed, clear and specific) of the data subject before processing them.

In addition, the bill requires the processor to conduct and submit a “Data Protection Impact Assessment” before commencing any large scale biometrics processing. The impact assessment shall contain a detailed description of the proposed processing operation, the purpose of processing and the nature of personal data being processed. Also, it shall assess the
potential harm that may be caused to the data subjects, and detail measures for managing, minimizing, mitigating or removing such risk of harm.

California Consumer Privacy Act (CCPA)

California Consumer Privacy Act of 2018 (CCPA) defines biometric data as: “an individual's physiological, biological or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity”. CCPA regards biometric data as a type of personal information. Yet, it deals with biometrics more strictly when it comes to consent and security measures.\(^2\)

More specifically, CCPA explicitly excludes biometrics from the definition of publicly available data, which makes processing a publicly available image for purposes of identification prohibited without consent. Moreover, CCPA demands that businesses "maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information".\(^2\) This may imply strict security procedures and practices considering the sensitive nature of biometric data.

Although the state of California does not have any law that focuses specifically on the use or protection of biometric data, Illinois, alongside with 2 other states, enacted the Biometric Information Privacy Act (BIPA), regulating biometric data in a separate legislation that makes violations much more costly to entities.\(^2\) Also, some legislators are pushing for state-level and national-level regulation of biometrics due to the sensitivity and possible severe consequences of processing them.\(^2\)
Policy Options

To better govern biometric data in Jordan, the following options can be followed or implemented (these options are not necessarily mutually exclusive):

➔ **Doing Nothing**: Evidently, we can resort to doing business as usual, without any intervention to change the status quo.

➔ **Banning unwarranted biometrics processing**: Passing a legislation that criminalizes any processing of biometric data unless done by court and/or prosecution decision. (e.g. to resolve an unsolved crime or incriminate a murderer).

➔ **Categorizing biometric data as ‘sensitive personal data’ & providing better protection and guarantees for biometric data processing**: Amending the Personal Data Protection Law draft to regard biometric data as ‘sensitive personal data’ with an explicit reference and a clear definition of biometric data. Also, adding better protections for biometrics processing such as:

  ◆ Developing a biometric data processing framework that processors need to submit to the data commissioner. The framework should include justifications for biometrics processing, privacy impact assessments, and clarification of safety and security measures undertaken for processing.

  ◆ The Data Commissioner authorizes processing of biometric data in cases where more than a specific number of data subjects, say 100, are involved.

  ◆ Consent for biometric data processing ought not be considered freely given in situations where the data subject is
dependent on the processor such as the employer/employee relationship.

➔ **Levying deterrent fines on violations related to biometrics processing**: To force processors to take biometric data processing more seriously in terms of necessity and needed security guarantees, it is vital to amend the personal data protection draft law to levy heavier fines on violations related to biometrics processing.

➔ **Imposing Biometric Tokenization**: Using digital obfuscation methods to transform biometric data to less-sensitive forms called tokens, that have little meaning by themselves and do not convey the original biometric characteristics of original data, obscuring the theft of biometric characteristics. A legislation can allow biometric data processors to store tokens and prevent them from storing raw biometric data, mitigating some privacy and security risks associated with biometrics processing.

➔ **Building Awareness of risks/dangers of biometrics processing**: Adding sections in school curricula/general education programs that explain biometric data and make individuals more aware of privacy and security risks and dangers associated with them.
Criteria/Considerations

The following criteria are taken into consideration in judging policy options:

➔ **Privacy**: The right to privacy is of utmost importance when thinking about biometric data. Any decision should minimize privacy risks, especially those that pertain to (mass) surveillance.

➔ **Digital Security**: Decisions should ensure the digital security for individuals and hinder potential identity thefts exploiting biometric data.

➔ **Innovation**: Decisions related to biometrics should not disproportionately limit innovation. Individuals and companies have the right to innovate and develop technologies that enable human advancement as long as usage risks can be mitigated and negative consequences related to those risks are contained.
## Assessments of Policy Options

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Severe Negative Impact</td>
<td>With the current rate of technological development, leaving the status quo unchanged enables material privacy compromises, surveillance, tracking, and other risks in a way that is difficult to reverse.</td>
<td>Severe Negative Impact</td>
<td>Leaving biometrics unregulated provides hackers or saboteurs the opportunity to steal and exploit biometrics with impunity.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>High Protection Banning biometrics processing and restricting its use to criminal/rights applications makes biometric data far less available and thus less susceptible to privacy abuse.</td>
<td>High Protection Banning biometrics processing and restricting its use to criminal/rights applications makes biometric data far less available and thus less susceptible to digital security abuse.</td>
<td>Paralyzing Innovation Banning unwarranted biometrics processing paralyses developments in the field and prevents the private sector from building biometric-based technologies.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Policy Option 3: Categorizing biometric data as ‘sensitive personal data’ &amp; providing better protection and</th>
<th>Criterion 1: Privacy</th>
<th>Criterion 2: Digital Security</th>
<th>Criterion 3: Innovation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Better Protection Dealing with biometric data as ‘sensitive personal data’ would make it difficult to collect biometric data without justification and</td>
<td>Better Protection Dealing with biometric data as ‘sensitive personal data’ would require processors to provide better security guarantees before</td>
<td>Hindering Innovation Abiding by a strong personal data protection law would require more effort from processors and thus make the</td>
<td></td>
</tr>
<tr>
<td>Policy Option 4: Levying deterrent fines on violations related to biometrics processing</td>
<td>Better Protection</td>
<td>Better Protection</td>
<td>No Material Effect</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Levying large fines on biometric processing violations would incentivize providing better privacy guarantees before processing.</td>
<td>Levying large fines on biometric processing violations would incentivize providing better security guarantees before processing.</td>
<td>Fines amounts can be calculated as a percentage of realized revenues, making the effect of levying them on innovation minimal.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Policy Option 5: Imposing biometric tokenization</th>
<th>Better Protection</th>
<th>Better Protection</th>
<th>No Material Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transforming biometric data into tokens obfuscates its content, making identifying individuals based on it more difficult, enhancing the privacy of individuals.</td>
<td>Transforming biometric data into tokens renders data useless for different applications, making security threats less of a concern.</td>
<td>Tokenization is virtually cost free, and does not require huge efforts to implement in applications, especially with open source libraries.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Spreading awareness about basic concepts, best practices, and short-term and long-term risks associated with biometric data helps individuals make informed decisions about how, when and to whom to provide such sensitive data.</td>
<td>Spreading awareness about basic concepts, best practices, and short-term and long-term risks associated with biometric data helps individuals in being more cautious when it comes to their biometric data, decreasing the probability of security risks.</td>
<td>Spreading awareness about basic concepts, best practices, and short-term and long-term risks associated with biometric data has arguably no material impact on legitimate innovation, at least not in the short term. In the long run, awareness...</td>
<td></td>
</tr>
</tbody>
</table>
campaigns may decrease the number of users of biometric technologies, providing less incentive for innovation.
Recommendations

Based on the analysis of the policy options, and a humble attempt at balancing the benefits and cost for all criteria, JOSA recommends the following policy options:

➔ Categorizing biometric data as ‘sensitive personal data’ & providing better protection and guarantees for biometric data processing: Amending the Personal Data Protection Law draft to regard biometric data as ‘sensitive personal data’ with an explicit reference and a clear and unambiguous definition of biometric data.

Also, the law ought to include better protections for biometrics processing such as:

◆ Developing a biometric data processing framework that processors need to submit to the data commissioner. The framework should include justifications for biometrics processing, privacy impact assessments, and clarification of safety and security measures undertaken for processing.

◆ The Data Commissioner authorizes processing of biometric data in cases where more than a specific number of data subjects, say 100, are involved.

◆ Consent for biometric data processing should not be considered freely given in situations where the data subject is dependent on the processor such as the employer/employee relationship.

➔ Levying deterrent fines on violations related to biometrics processing: To force processors to take biometric data processing more seriously in terms of necessity and needed security guarantees,
it is vital to amend the personal data protection draft law to levy heavier fines on violations related to biometrics processing.

➔ **Imposing biometric tokenization:** Using tokenization and digital obfuscation methods to transform biometric data to non-sensitive forms called tokens, that have little meaning by themselves, obscuring the theft of biometric characteristics. A legislation can allow biometric data processors to store tokens and prevent them from storing raw biometric data, mitigating privacy and security risks associated with biometrics processing.

➔ **Building awareness of risks/dangers of biometrics processing:**
Expanding school curricula/general education programs to add components on digital rights and biometric data, raising awareness of risks and dangers associated with them.
References


2. [No title].

3. Reclaim Your Face: Ban Biometric Mass Surveillance!
https://reclaimyourface.eu/.

4. الآخبار، ف. ر. البطاقة الذكية ستقدم 5 خصائص وخدمات أساسية في مرحلتها الأولى.

5. Jordan to start issuing e-passports.

6. DocuWare.
https://doc.pm.gov.jo/DocuWare/PlatformRO/WebClient/Client/Document?id=55905&fc=7e6f119f-71f4-4ed3-8023-b6a6db8bcb15&orgId=1&Auth=15
5636FC5DC51195F1461C635D1DA51CA4BC194E7CA5649B0654E2A3EB4DEEC7675C
04DA4EB6A51D4FDBBE9EE7A7ABB5018CAC4742BD66A8753F135999C378185B817
71B656A5A2A6E6F3FF76716C0A2D1F38AA59BEE825BDAF85002EC3A059975063D5
6ED2F3C450E79D63B387702B76CD929A07AF90523302FFF74F9F72165A55BDAF1B
4B7A43AC0EAF20908CDA0D8213B1E286EA5A6FA24E0AF057CA98DA0A914EE63E
42C5FD344115194540B9081EB25AC0F84EB0446A6B6C9165509A0F2B01F4D3A2808
4EB87908A935CE0AEEF6BF47422C9FF2C62BB8A06874C637D7A656D485AC68B249
F904D7132.

7. Cairo Amman Bank Launches Bills Payment Service through ATMs.
8. Website.

9. Fatafta, M. Exposed and exploited: Data protection in the Middle East and North Africa.

10. [No title].
https://www.cbj.gov.jo/EchoBusV3.0/SystemAssets/03%20%D8%AA%D8%B9%D9%84%D9%8A%D9%85%D8%A7%D8%AA/%D8%A7%D9%84%D8%AC%D9%87%D8%A7%D8%B2%0%D8%A7%D9%84%D9%85%D8%B5%D8%B1%D9%81%D9%8A/%D8%AA%D9%86%D8%BB%D9%8A%D9%85%20%D8%A7%D9%84%D8%AA%D8%B9%D8%A7%D9%85%D9%84%20%D9%85%D8%B9%20%D8%A7%D9%84%D8%B9%D9%85%D8%A7%D9%8A%20%D9%88%D8%AD%D9%85%D8%A7%D9%8A%D8%AA%D9%87%D9%85/T53.pdf.

11. DocuWare.

12. بطاقة الخدمة الخاصة بالجالية السورية - وزارة الداخلية.
https://moi.gov.jo/Ar/Pages/%D8%A8%D8%B7%D8%A7%D9%82%D8%A9_%D8%A7%D9%84%D8%AE%D9%85%D8%A9_%D8%A8%D8%A7%D9%84%D8%AC%D8%A7%D9%84%D9%8A%9_%D8%A7%D9%84%D8%B3%
13. Website.


15. ديوان التشريع والرأي.
https://lob.gov.jo/?v=1.11&url=ar/DraftDetails?DraftID:10254,AddComment:0,PageIndex:1&DraftTitle:%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%AD%D9%85%D8%A7%D9%8A%D8%A9-%D8%A7%D9%84%D8%A8%D9%8A%D8%A7%D9%86%D8%A7%D8%AA-%D8%A7%D9%84%D8%B4%D8%AE%D8%B5%D9%8A%D8%A9-/--%D8%AA%D9%85-%D8%AA%D9%85%D8%AF%D9%8A%D8%AF-%D9%85%D8%AF%D8%A9-%D9%86%D8%B4%D8%B1%D9%87-%D8%B9%D9%84%D9%89-%D8%A7%D9%84%D9%85%D9%88%D9%82%D8%B9-%D8%A7%D8%B1%D8%A8%D8%B9-%D8%A7%D9%8A%D8%A7%D9%85-%D8%B9%D9%85%D9%84-%D8%A7%D8%B1%D9%81%D9%8A%D8%A9.

16. What is GDPR, the EU’s new data protection law?

17. Art. 4 GDPR - Definitions - GDPR.eu.

18. Website.

19. [No title].

20. [No title].

22. California Consumer Privacy Act (CCPA).

23. Public Act 0994 95TH GENERAL ASSEMBLY.


(2020).