Data Protection And Privacy Laws In MENA:

A Case Study Of Covid-19 Contact Tracing Apps

FEBRUARY 2021

smex.org

ACKNOWLEDGEMENTS

SMEX produced this report based on research by **Joey Shea**, a researcher and analyst specialized in security and political repression. Joey Shea is a nonresident fellow at the Tahrir Institute for Middle East Policy and consults for the World Bank.

The report was edited by **Grant Baker** and **Nerissa Naidoo**. Special thanks **Salam Shokor** for the graphic design, **M. Zidel** for the research support, and **Grant Baker** for the feedback and support.

The report relies on the Cyrilla database, an open database of digital rights law from around the world, as well as Cyrilla's legal research methodology. The research was generously funded by one of Cyrilla's applied research and advocacy grants.

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 February 2021 Publication of SMEX

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

Table of Contents

Executive Summary

This report analyzes data protection and privacy laws in Qatar, Bahrain, the United Arab Emirates, and Kuwait. It also documents the deployment of COVID-19 contact tracing applications in these states. The report compares data protection and privacy legal frameworks in these states with international standards, as well as assesses whether their respective COVID-19 contact tracing applications have implemented adequate privacy preserving mechanisms. Qatar, Bahrain, and the UAE have at least some form of data protection and privacy legislation, while Kuwait is the only jurisdiction surveyed without any data protection law at this time. The laws in the three jurisdictions with data protection legal frameworks broadly resemble international data protection standards, such as the GDPR, with some notable exceptions. These laws are comparable with international data protections laws in terms of their fundamental data protection principles, the rights of data subjects and the legal obligations of data controllers. Importantly, some states diverge from international standards insofar as they grant large exemptions related to national security. These sweeping national security exceptions are most pronounced in Bahrain and Qatar. There is also a notable lack of evidence in most jurisdictions indicating broad enforcement of their data protection and privacy laws and their regulatory authorities are relatively inactive. Furthermore, there is a lack of evidence of people or entities taken to court under these laws. Widespread accusations of sweeping domestic surveillance programs in Qatar, Bahrain, the UAE and Kuwait also raise serious doubts about the extent to which these governments and state security agencies respect and adhere to data protection and privacy principles outlined in the law.

COVID-19 contact tracing apps surveyed within these jurisdictions lack a limited purpose and clear timelines on their deployment and use. There is also a notable lack of transparency in both their technical design and regulatory mechanisms. Finally, the report finds that the more robust a state's privacy legal framework is, the more privacy preserving their app has proven to be.

Introduction

As COVID-19 spread across the Middle East, human rights groups quickly expressed their concern over the threat that coronavirus poses to privacy. Civil society throughout the region feared that the pandemic would provide yet another pretext and justification for sweeping government surveillance and further limiting of rights and freedoms. Of particular concern was the use of technology, mainly mobile device applications, to enhance and expand traditional track and trace programs.

> "COVID-19 tracking applications were identified as posing a significant threat to the right to privacy."

Dozens of organizations signed a statement that "called on all governments not to respond to the coronavirus pandemic with increased digital surveillance" unless a number of conditions were met. These conditions included demands that any surveillance measures be "lawful, necessary, proportionate [...] and justified by legitimate public health measures."[1]

In light of these concerns, COVID-19 tracking applications were identified as posing a significant threat to the right to privacy. Now, months into the pandemic, this report seeks to analyze the regulatory environment in which these applications were deployed and assess whether the initial fears over the loss of privacy were well-founded. Most importantly, this report seeks to understand how legal frameworks across the Middle East have evolved in respect to state surveillance, data protection and privacy; it aims to evaluate whether these frameworks have adequately protected -- or violated -- the right to privacy.

Given the historic health crisis facing the region, these data, privacy and surveillance legal frameworks will be explored through the lens of COVID-19 tracing applications. The fast proliferation of these applications raises important concerns over privacy, data protection, and surveillance. There are legitimate concerns about whether these applications are striking the correct balance between surveillance in the service of public health, while also protecting their users' privacy. Moreover, given the immensity of the crisis, many NGOs and human rights organizations have expressed concern that states will use the crisis to exploit special exemptions and emergency powers in the law to expand state power and track citizens long after the end of the coronavirus.[2] In order to thoroughly address and evaluate these concerns, the legal frameworks of contact tracing applications will be examined, in addition to documenting their deployment and use. This case study will be used as a framework through which to explore broader questions about the health of data governance, data protection, privacy and state surveillance in the Middle East.

Four countries were selected based on the timing of the release of their respective COVID-19 contact tracing application: Qatar, Bahrain, the UAE, and Kuwait. This report includes separate country studies for each of these states that analyze their fundamental data protection principles, the rights of data subjects and the legal obligations of data controllers. Each country study also includes an assessment of the state's COVID-19 contact tracing application and the extent to which the policy framework and design features of the app complies with international standards. The report also includes a summary of findings that assesses regional data protection and privacy trends; a comparative analysis of data principles across jurisdictions, including an assessment of fundamental principles, the rights of data subjects and the legal obligations of controllers; an overview of exemptions and provisions related to national security; and, finally, an assessment of how these applications measure up to international privacy standards.

1 Tahrir Institute for Middle East Policy. "Joint civil society statement: States use of digital surveillance technologies to fight pandemic must respect human rights." April 2, 2020. https://timep.org/press/press-releases/timep-joins-109-organizations-on-digital-surveillance-privacy-and-covid-19-statement/

2 Article 19. "Coronavirus: Emergency powers must be kept in check." March 20, 2020. https://www.article19.org/resources/covid-19-emergency-powers-must-be-kept-in-check/

International Principles for the Use of COVID-19 Contact Tracing Applications

In the early days of the pandemic, civil society organizations, human rights groups, and privacy bodies released a number of guidelines outlining the necessary components for the ethical use and deployment of COVID-19 contact tracing applications.[3,4,5] These frameworks described essential privacy preserving principles that should determine both the technical components of these apps and the regulatory principles governing their use.[6,7,8] These guidelines have been used to assess both the legal frameworks governing the collection and processing of data in the selected states and their respective COVID-19 contact tracing apps.[9,10]

> “Health must always be the starting point for the deployment of COVID-19 contact tracing apps.”

Most importantly, these guides hold that health must always be the starting point for the deployment of these apps. New technologies must only be a small part of a comprehensive response and should not displace non-technical responses. Contact tracing applications must support widespread manual contact tracing campaigns and be deployed only after sufficient capacity for manual tracing and diagnostic testing has been developed.

Human rights standards, in particular data protection and privacy principles, must also be at the forefront of any technological response. Responses must be necessary and proportionate to these ends. The apps themselves must therefore first be proven to serve the purpose for which they are being deployed and there must be evidence that supports their overall effectiveness, including measurable impacts.

Clear and limited purposes for the deployment and use of the app must be articulated before they are introduced. The app should only function in the service of public health and the data that is collected and processed must only be used for this stated purpose. The purpose should also be limited insofar as there is a clearly articulated exit strategy, outlining how long the app will be in existence, under what conditions it will be used, and strict timelines for the deletion of sensitive data.

Governments launching these applications must be fully transparent in regard to how data is collected, what data is collected, how data will be used and with whom it will be shared. The full source code for the apps must be available for scrutiny. Privacy protection must be an integral component in the design features of the app: decentralized storage on individual devices must be used instead of centralized servers, Bluetooth should be used instead of GPS, storage must be secured through encryption, identifiers exchanged between devices must be regularly altered, and only data relevant and limited to the agreed upon purpose should be collected and processed. Data that is collected and processed must be accurate.

User consent and control must be integrated into the app. Governments must therefore not mandate its use, but individuals must be free to voluntarily download and use the application. Users must be able to control their data. Public benefits or access to public or private spaces must not be conditioned on the use of the app. This requirement has important impacts on equity and discrimination, as vulnerable groups may be particularly negatively impacted if access conditions are placed on the app.

3 ACLU. “Government Safeguards for Tech-Assisted Contact Tracing.” May 18, 2020. https://www.aclu.org/other/aclu-white-paper-government-safeguards-tech-assisted-contact-tracing

4 ACLU. “Principles for Technology-Assisted Contact-Tracing.” April 16, 2020. https://www.aclu.org/report/aclu-white-paper-principles-technology-assisted-contact-tracing

5 Ada Lovelace Institute. “Provisos for a Contact Tracing App.” May 4, 2020. https://www.adalovelaceinstitute.org/evidence-review/provisos-covid-19-contact-tracing-app/

6 Ada Lovelace Institute. “Exit through the App Store?” April 20, 2020. https://www.adalovelaceinstitute.org/wp-content/uploads/2020/04/Ada-Lovelace-Institute-Exit-through-the-App-Store-Explainer-for-Government-April-2020.pdf

7 European Commission. “Communication from the Commission: Guidance on Apps supporting the fight against COVID19 pandemic in relation to data protection.” April 17, 2020. https://op.europa.eu/en/publication-detail/-/publication/f8f4dc8b-80a4-11ea-bf12-01aa75ed71a1/language-en

8 European Commission. “eHealth Network , Mobile applications to support contact tracing in the EU’s fight against COVID-19.” April 15, 2020. https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

9 Information Commissioners Office. “COVID-19 Contact tracing: data protection expectations on app development.” May 4, 2020. https://ico.org.uk/media/for-organisations/documents/2617676/ico-contact-tracing-recommendations.pdf

10 Lancet Digit Health. “The need for privacy with public digital contact tracing during the COVID-19 pandemic.” June 2, 2020. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7266569/

National health authorities must be responsible for the deployment of the app. Its use should be accompanied with the passage of primary legislation that governs and outlines strict conditions for its use. Data protection authorities should also be consulted and ensure compliance to data protection principles. An independent oversight body should be created to monitor the apps deployment and data usage.

On April 10, 2020, Google and Apple announced the Exposure Notification System, a joint venture to develop an API appropriate for both of their operating systems that would support the development of privacy preserving contact tracing applications.[11] Civil society organizations and data protection authorities assessed the system and found that the proposal "aligned with the principles of data protection by design and default."[12]

Relying on a decentralized protocol and Bluetooth, the Exposure Notification System allows personal data only to be collected on a voluntary basis and prohibits the collection of location data. The UK's Information Commissioner's office assessed the system and found it "supports the development of apps that protect their users' identities."[13] The Commission also found that the protocol complies with the principle of data minimisation and incorporates privacy conscious security measures. However, they also found that third-party developers "may also develop functionality that involves collection of additional data or new uses of existing data."[14]

Each country study will use these international standards as a measure with which to assess each respective COVID-19 contact tracing application.

11 Apple. "Apple and Google partner on COVID-19 contact tracing technology." April 10, 2020. https://www.apple.com/ca/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/

12 Information Commissioners Office. "Apple and Google joint initiative on COVID-19 contact tracing technology." April 17, 2020. https://ico.org.uk/media/about-the-ico/documents/2617653/apple-google-api-opinion-final-april-2020.pdf

13 Ibid.

14 Ibid.

Country Studies: Qatar

As of December 7th, 2020, there have been a total of 139,908 confirmed cases of COVID-19 and 239 deaths in Qatar.[15] A digital contact tracing application, called EHTERAZ, was launched by Qatar's Ministry of Interior as part of the country's efforts to combat the coronavirus. On May 18th, the Qatar News Agency announced that the application would be mandatory for all citizens and residents and the decision became effective on May 22nd.[16]

Privacy concerns have plagued the app since its launch, particularly after Amnesty Tech released a report detailing serious security vulnerabilities. While the vulnerabilities were quickly patched, the issue exposed the personal data of millions of users.[17] Qatar passed a personal data protection law in 2016. However, security forces have been accused of monitoring personal communications, raising doubts about the extent to which the data protection law is respected by security agencies.[18]

Legal Framework Of Data Protection And Privacy In Qatar

Qatar's data protection and privacy obligations are governed by a number of national level laws and sector specific regulations. Qatar's Constitution guarantees the sanctity of human privacy. Article 37 holds that: "The sanctity of human privacy shall be inviolable, and therefore interference into privacy of a person, family affairs, home of residence, correspondence, or any other act of interference that may demean or defame a person may not be allowed save as limited by the provisions of the law stipulated therein."

Other provisions pertaining to privacy and data protection can be found in the Penal Code, Civil Code, Labour Law, Banking law, Electronic Commerce and Transactions Law, Telecommunications Law, Cybercrime Prevention Law, and the 2005 Data Protection Regulations for the Qatar Financial Center.

Qatar's data protection and privacy framework is governed mainly by Law no. 13 of 2016 on the Protection of Personal Data. The law was adopted on December 29, 2016 and lays out the application rules for the processing of data in Qatar. On January 2, 2018, a resolution from the Council of Ministers extended the compliance period until January 29, 2018.

Data Protection Principles

The law outlines how personal data of citizens is protected in Qatar and applies to controllers and processors of data. The Ministry of Transport and Communications is the responsible authority for data protection.

Personal data is required only be processed within the principles of transparency, honesty, respect for human dignity, and acceptable practices, as outlined in article 3.[19] Personal data must be processed honestly and legitimately. The appropriate administrative, technical and material precautions must be taken to protect personal data, as determined by the competent department.[20]

Any person or entity that violates provisions of the law could be subject to a fine ranging between one and five million Qatari Riyals (274,631 to 1,373,155 USD). The penalties for violating provisions of the law are outlined in articles 23 and 24.[21]

The Rights of Data Subjects

Data controllers are obligated to inform data subjects about the processing of their personal data before the processing occurs, including the legitimate purposes for which the controller or any other party wishes to process data.[22]

However, there are broad exemptions that allow personal data to be processed without obtaining consent from the data subject. These exemptions, outlined in article 18, include the following:

15 World Health Organization. 2020. "Qatar: WHO Coronavirus Disease Dashboard." Accessed December 7, 2020. https://covid19.who.int/region/emro/country/qa

16 https://twitter.com/QNAEnglish/status/1262487099145703426?s=20

17 Amnesty International. May 26, 2020. "Qatar: Contact tracing app security flaw exposed sensitive personal details of more than one million." https://www.amnesty.org/en/latest/news/2020/05/qatar-covid19-contact-tracing-app-security-flaw/

18 Freedom House. "Qatar, 2019." https://freedomhouse.org/country/qatar/freedom-world/2020

19 Law number 13 of 2016 on the protection of Personal Data, art. 3 https://www.motc.gov.qa/ar/documents/document/qatar-issues-personal-data-privacy-law-5

20 Ibid. art. 8

21 Ibid. art. 23, 24

22 Ibid. art. 9

- "Protecting national and public security;
- Protecting the international relations of the State;
- Protecting the economic or financial interests of the State; and
- Preventing any criminal offense, collecting data about it or investigating it."[23]

Data subjects are granted the right to consent to the processing of their data and are allowed to withdraw any prior consent. Data subjects have the right to be informed that their data is being processed and the purpose of the processing.[24] They are also granted the right to object to the processing of their data.[25] These rights and obligations are outlined in articles 4 through 6. There are specific consent requirements for sensitive personal data outlined in article 16. It is not permissible to process sensitive personal data, except after a permit is obtained from the competent department.[26]

Data subjects have the right to access and correct their personal data, as per articles 5 and 6. Under article 5, data subjects are able to request that their personal data be corrected. Data subjects must provide evidence of the validity of their access request. Article 6 also provides the right to receive a copy of their data after subjects pay an amount that does not exceed the fee for the service.[27] Article 26 grants data subjects the right to file a complaint with the competent department in the event that a provision of the law is violated.[28]

Legal Obligations for Data Controllers and Processors

Data controllers must provide notice to data subjects before processing their data. Article 4 obliges controllers to obtain a data subject's consent, or another legal basis, before the processing of their data. Controllers must outline the legal reason why they are processing the data and explain how the data will be processed.

Broad exemptions from the consent obligation are outlined in article 19. Controllers are exempted from obtaining consent from their data subjects in the following cases:

1. "Carrying out a task related to the public interest in accordance with the law.

2. Executing a legal obligation or an order from a competent court.

3. Protecting the vital interests of the individual.

4. Achieving the objectives of scientific research that is conducted in the public interest.

5. Collecting the necessary information to investigate a criminal offense based on an official request from the investigation authorities"[29]

There are also exemptions granted to controllers from the obligation to grant access to a data subject. Exemptions include the following: instances where it is necessary for the protection of national and public security, the international relations of the state, the economic and financial interests of the data, or to prevent a criminal offence or collect data in the context of an offence or investigation. These exemptions are outlined in article 20.

Controllers are required to implement proper administrative, technical, and physical precautions to protect the data they are processing, as per article 8. Controllers are also required to verify that the data being collected is "relevant to the legitimate purpose and sufficient to achieve them"[30]. Data controllers are further obligated to take necessary steps to protect against the loss, damage, or any unauthorized or illegitimate access to the data they control. Article 10 also requires that controllers not retain the data for longer than is necessary to achieve the legitimate purposes of the collection.

Controllers must ensure that data will be processed according to the law before disclosing or transferring data to a data processor. They must train the processors in regard to the protection of data and verify that the processors comply. The controller must also verify that the processor has taken necessary precautions to protect and secure the data.

Article 11 outlines obligations for controllers to review privacy procedures, establish management systems, and

23 Ibid. art. 18
24 Ibid. art. 4
25 Ibid. art. 5
26 Ibid. art. 16
27 Ibid. art. 6
28 Ibid. art. 26
29 Ibid. art. 19
30 Ibid. art. 10

report violations. Controllers are obligated to establish a system to receive and process requests from data subjects to access, correct or delete their data.

Controllers must notify data subjects and the competent department in the occurrence of any data breach, if it causes damage to the personal data or the privacy of an individual. Processors are also required to inform controllers of a data breach, as soon as they become aware of it, as per article 13.

COVID-19 Contact Tracing App In Qatar

EHTERAZ was developed and launched by Qatar's Ministry of Interior as an integral component of their overall COVID-19 strategy. The app is meant to "spread health awareness tips and techniques" as well as "protection methods that are necessary to halt the outbreak of coronavirus."[31] The chair of the EHTERAZ Joint Taskforce, Dr Yousef Al Maslamani, said that the app is "playing an important role in keeping Qatar's population safe", particularly after the country entered phase 4 of lifting restrictions.[32] Qatar's health ministry promised that the data gathered through the application is "completely confidential."[33] The app had over 1 million installs on the Google Play store at the time of writing and is available in English and Arabic.[34]

The app uses real-time GPS location tracking and data is uploaded to a central database.[35] Bluetooth contact between two users' devices is also recorded. The GPS function also records the location of the contact and this data is uploaded to the central server.[36] The government has claimed that the data collected through the app is deleted after two months, and that law enforcement do not have access to the data.[37] The application is said to transmit the data to health authorities.

Ehteraz was made mandatory for all Qatari citizens, residents and visitors on May 22nd. Individuals can receive a fine of 200,000 QR or up to three years in prison if they do not download and install the app. The app is mandatory for entering many different kinds of establishments throughout Qatar. It is necessary to enter mosques, entertainment and social venues, transportation, parks, corniches, beaches, sports facilities, schools, nurseries, and childcare establishments.[38] Security forces were reported setting up checkpoints throughout the country to ensure that residents and citizens had the app on their phone.[39] Diplomats have been granted exemptions from the use of the app.[40]

In May, Amnesty Tech released a report outlining "serious security vulnerabilities" with the EHTERAZ app.[41] They found a critical weakness in the configuration of the app which would have granted access to sensitive personal data to would-be attackers. Amnesty security researchers were able to view sensitive data such as names, national ID numbers, health status, and location data. The security researchers found that the centralized server into which all of the data is uploaded did not have adequate security measures in place to protect the data. Amnesty Tech informed Qatari authorities of the vulnerability and it was patched.[42]

Assessment

The Ehteraz app has several troublesome features that run contrary to international privacy and human rights

31 Google Play. "Ehteraz – Ministry of Interior Qatar." https://play.google.com/store/apps/details?id=com.moi.covid19&hl=en
32 State of Qatar, Ministry of Public Health. ""Etheraz" Plays Vital Role in Keeping People Safe during Lifting of Restrictions, say Health Officials." September 8, 2020. https://www.moph.gov.qa/english/mediacenter/News/Pages/NewsDetails.aspx?ItemId=274
33 AFP. "Qatar COVID-19 tracing app stirs rare privacy backlash." May 25, 2020. https://gulfnews.com/world/gulf/qatar/qatar-covid-19-tracing-app-stirs-rare-privacy-backlash-1.71675372
34 Google Play. "Ehteraz – Ministry of Interior Qatar." https://play.google.com/store/apps/details?id=com.moi.covid19&hl=en
35 Amnesty International. "Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy." June 16, 2020. https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/
36 COVID19Qatar. "Supreme Committee for Crisis Management announces launch of EHTERAZ – "precaution" mobile application to help contain COVID-1." April 10, 2020. https://covid19qatar.info/supreme-committee-for-crisis-management-announces-launch-of-precaution-mobile-application-to-help-contain-codiv-19/
37 Al Jazeera. "Qatar makes COVID-19 app mandatory, experts question efficiency." May 26, 2020. https://www.aljazeera.com/news/2020/5/26/qatar-makes-covid-19-app-mandatory-experts-question-efficiency
38 State of Qatar Ministry of Public Health. "Controlled Lifting of COVID-19 Restrictions Plan." https://covid19.moph.gov.qa/EN/Precautions-for-lifting-restrictions/Pages/default.aspx
39 Arab News. "Coronavirus tracing app stirs rare privacy backlash in Qatar." May 26, 2020. https://www.arabnews.com/node/1680026/middle-east
40 State of Qatar Ministry of Public Health. "Excluding diplomats from "Ehteraz." July 9, 2020. https://www.moph.gov.qa/english/mediacenter/Announcements/Pages/AnnouncementsDetails.aspx?ItemId=84
41 Amnesty International. "Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy." June 16, 2020. https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/
42 Ibid.

preserving guidelines. These features, combined with far-reaching exemptions outlined in Qatar's data protection law, should raise serious concerns about the right to privacy and data protection in the country.

International guidelines for COVID-19 contact tracing applications hold that these apps must be met with a clear and limited purpose. Qatar issued its requirement that the app be mandatory on May 22nd, without any accompanying guidelines on how long citizens and residents of the country can expect to be made to use the app. The mandatory obligation runs directly contrary to international guidelines on the deployment of these applications.

This mandatory obligation has important implications for equity and discrimination, particularly because access to public and private spaces are conditioned on the use of the app. Many individuals, particularly migrant workers, were not able to afford a phone compatible with the application. There were multiple reports of older mobiles not supporting the application which forced many low wage workers to purchase new phones during a devastating economic period.[43] Individuals also feared the possibility of fines or imprisonment on their way to purchase a phone compatible with the app.

Failure to have the app installed on your personal mobile completely limits movement and access throughout the country. Citizens and residents are not allowed to enter any establishment, from hospitals to coffee shops, without the application. Mandatory use risks shutting out large portions of the population, particularly vulnerable communities, from all sectors of society.

There are also notable transparency issues with the app itself, its regulations for use, and technical design. The source code of the app has not been released and is not available to be fully scrutinized by security researchers, creating further knowledge gaps about how the data is being used and with whom it is being shared. Additionally, users have a limited capacity to control their own data. Qatar also lacks strong regulations on data retention and deletion. The government has said that the data is deleted after two months, but there are no enforceable mechanisms guaranteeing the timely deletion of data, nor are there strict time limitations on data retention under the law. The app also does not adhere to the "privacy protection by design" principle because it uses a centralized server and GSP tracking.

Finally, there have not yet been any cases brought to bear under the law, raising questions about the state's willingness to enforce the provisions of the data protection law.

43 AP. "Coronavirus: Qatar contact-tracing app exposes divide between rich and poor." June 11, 2020. https://www.middleeasteye.net/news/coronavirus-qatar-contact-tracing-app-exposes-divide-between-rich-and-poor

Country Studies: Bahrain

As of December 7, 2020, there have been 87,929 confirmed coronavirus cases and 341 deaths in Bahrain.[44] Bahrain's eGovernment Authority launched the "BeAware" contact tracing application as part of the state's overall plan to combat the spread of the coronavirus. In addition to contact tracing, the application provides updates and information about COVID-19 and Bahrain's public health response. A Bahraini government spokesperson said: "The app plays a vital role in supporting Bahrain's 'Trace, Test, Treat' strategy and has helped to keep Bahrain's Covid-19 death rate at 0.24%. 11,000 individuals have been alerted through the app and prioritized for testing, of which more than 1,500 have tested positive."[45]

Amnesty Tech released a report in June 2020 warning that Bahrain's app was one of the most privacy invasive apps in the world.[46] While Bahrain passed a data protection law in 2018, the government and security forces are believed to continue to monitor the personal communications of citizens.[47]

Legal Framework Of Data Protection And Privacy In Bahrain

Data protection and privacy in Bahrain is primarily governed through Law no. 30 of 2018, the Issuance of the Personal Data Protection Law. In addition to this law, several provisions in other laws and decrees comprise Bahrain's data protection and privacy legal framework. Bahrain's Constitution guarantees the confidentiality of communications, except where provided by the law. Article 26 of the Constitution states: "The freedom of postal, telegraphic, telephonic and electronic communication is safeguarded and its confidentiality is guaranteed. Communications shall not be censored or their confidentiality breached except in exigencies specified by law and in accordance with procedures and under guarantees prescribed by law."[48]

Other privacy relevant provisions are found in the Consumer Protection Law, the Cybercrime Law, the Penal Code, the Labour Law, and the Financial Institutions Law, among others.

Most importantly, Bahrain's data framework is outlined and defined in the Law no. 30 of 2018 on the Issues of the Personal Data Protection Law. The effective date of the law was August 1, 2019; all natural and legal persons had to fully comply with its provisions by this deadline.

While the law outlines the establishment of a Data Protection Authority, this body has not yet been created. The Ministry of Justice, Islamic Affairs and Endowments is currently acting as the data protection authority until it is established. On September 29, 2019, decree No. 78 of 2019 came into effect and appointed the Ministry of Justice to this role.[49]

Data Protection Principles

The Personal Data Protection Law outlines specific responsibilities for data processors, data controllers, as well as rights for data subjects. The processing and treatment of personal data must be fair and legitimate, as per article 3. The data must be collected only for a specific and clear purpose and it must not be subsequently processed in a manner inconsistent with this original purpose.[50]

After the purpose for the collection of data has been completed, the data must not remain in any identifiable form that allows for identification of the data subject. Data stored for long periods must be preserved in an anonymized form and, if possible, encrypted.

The law applies to natural persons residing or working in Bahrain, in addition to legal persons who have a place of business in Bahrain. It also applies to both natural and legal persons who process data using means that exist in Bahrain. The law details large exemptions and does not

44 World Health Organization. "Bahrain: WHO Coronavirus Disease Dashboard." Accessed on December 7, 2020 https://covid19.who.int/region/emro/country/bh

45 BBC News. "Coronavirus: Alarm over 'invasive' Kuwait and Bahrain contact-tracing apps." June 16, 2020. https://www.bbc.com/news/world-middle-east-53052395

46 Amnesty International. "Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy." June 16, 2020. https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/

47 Freedom House. "Bahrain, 2019." https://freedomhouse.org/country/bahrain/freedom-world/2020

48 Constitution of the Kingdom of Bahrain, art. 26 http://www.nihr.org.bh/en/MediaHandler/GenericHandler/documents/download/1-%20Constitution%20of%20the%20Kingdom%20of%20Bahrain.pdf

49 Al Tamimi and co. "Ministry of Justice, Islamic Affairs and Awqaf entrusted with the tasks and competences of Personal Data Protection Authority." October 9, 2019. https://www.tamimi.com/news/ministry-of-justice-islamic-affairs-and-awqaf-entrusted-with-the-tasks-and-competences-of-personal-data-protection-authority/

50 Kingdom of Bahrain, Law number 30 of 2018 on the Issuance of the Personal Data Protection Law, art. 3

apply to data processing carried out by an individual for personal and family matters. The law also does not apply to processing operations related to national security issues undertaken by the Ministry of Defense, the Ministry of Interior, the National Guard, the National Security Service or other security services in Bahrain.[51]

Personal data is defined as "any information of any form related to an identifiable individual or information that, directly or indirectly, identifies an individual's formal, physiological, mental, cultural, or economic characteristics, or his social identity." Sensitive personal data is given a separate category and is defined as any information relating "directly or indirectly, to an individual's racial or ethnic origin, political or philosophical views, religious beliefs, union affiliation, criminal record or any data related to health or sexual status."[52]

Article 27 establishes the Personal Data Protection Authority. The authority has financial and administrative independence and it is tasked with monitoring compliance with the law.[53] Data Protection Monitors, or data privacy officers, are defined according to article 10, and must assist data managers in exercising their rights and duties stipulated under the law. Data officers and supervisors must be approved by the Data Protection Authority.[54]

Penalties for violating the law range from fines between 1,000 and 20,000 dinars or imprisonment of up to one year.

The Rights of Data Subjects

Data subjects have the right to be informed about the processing of their data by the data controller. Processing data without the consent of its respective data subject is prohibited; consent or another legal basis is required for the processing of both personal and sensitive data.[55] Consent must be written, explicit, clear and specific to the data being processed. Data subjects have the right to withdraw this consent at any time and have the right to object to the use of their data for marketing purposes.[56]

Data subjects have the right to access their data, free of charge. The rules and timeline for a data subject's right to access are outlined in article 18.[57] Data subjects also have the right to correct, block and delete their personal data. If the processing is in contravention to the law, or if the data is incorrect or incomplete, data subjects have the right to correct, block or delete this data. Corrections to data must also be provided to the data subject free of charge.

Legal Obligations for Data Controllers and Processors

Controllers are obligated to inform data subjects as to the collection and processing of their data. This notice must include the data manager's name, address, field of activity or profession, and the purpose of the processing, as well as any other important information that is necessary to ensure that processing is fair to the individual.[58] These provisions are outlined in Article 17. Controllers must first obtain explicit consent, or another legal basis, before processing personal data. Controllers are obligated to respond to requests by data subjects to correct their data. The controller must respond to the request within ten days, unless there is a legally acceptable justification.[59] Data controllers must abide by certain security requirements in the processing of personal data. Appropriate technical and organizational security measures must be implemented to protect against unintended or unauthorized destruction, loss, change, access, disclosure or alteration. State of the art technological protection methods must be undertaken to protect against any risks that come with data processing. These security measures must be made available for review by concerned authorities. Controllers must also take the proper measures to ensure that their chosen processor provides sufficient security measures to protect the personal data.[60]

> "The law does not apply to any data processing undertaken by Bahraini security agencies such as the Ministry of Defense, the Ministry of Interior, the National Guard, the National Security Service, or any other security service."

51 Ibid. art. 2
52 Ibid. art. 1
53 Ibid. art.27
54 Ibid. art. 10
55 Ibid. art. 4, 5
56 Ibid. art. 24
57 Ibid. art. 18
58 Ibid. art. 17
59 Ibid. art. 23
60 Ibid. art. 8

The law prohibits controllers from transferring data outside of Bahrain, except under specific conditions. The Data Protection Authority can grant permission to a cross border transfer on a case by case basis or to jurisdictions that offer adequate protections. These conditions are outlined in detail via articles 12 and 13.[61] Controllers are also obligated to notify and register with the Data Protection Agency before beginning any automated processing, as outlined in articles 14 through 16. The controller is exempted from registering with the Data Protection Agency if they appointed a data protection officer. Controllers are still required to notify the data protection within three days of appointing the data protection officer.[62]

Shortcomings

The law grants significant exceptions and exemptions to security authorities. Most importantly, the law does not apply to any data processing undertaken by Bahraini security agencies such as the Ministry of Defense, the Ministry of Interior, the National Guard, the National Security Service, or any other security service. The public prosecution, investigating judges, and the military prosecution do not have to provide notice of data processing to individuals.

There are no obligations outlined in the law that require the controller or processor to notify the data subject, or any other party, of a data breach. There are also no specific guidelines for the deletion of data. Encryption of personal identity is only a suggestion, not mandatory.

While the law was passed recently, the Data Protection Authority outlined has still not yet been established. The Ministry of Justice, Islamic Affairs and Endowments was appointed to the role of the data protection authority on September 20, 2019, but there has still yet to be financial allocation for the establishment of the DPA.

COVID-19 Contact Tracing App In Bahrain

Bahrain's government launched its COVID-19 contact tracing app, BeAware, at the start of the pandemic. It is designed to play "a vital role in supporting Bahrain's "Trace, Test, Treat" strategy" and to help facilitate the work of the National Task Force for Combating the Coronavirus.[63] The government has said that the app kept the country's death rate at 0.24% and that "11,000 individuals have been alerted through the app and prioritised for testing, of which more than 1,500 have tested positive."[64] Government statements have claimed that the app uses AI and big data to monitor COVID-19 cases. BeAware is available in six languages: Arabic, English, Urdu, Hindi, Bengali and Persian.[65]

The app was developed by Bahrain's Information and eGovernment Authority and is under this authority's jurisdiction. It was ready for beta testing within six days and was launched throughout the country only a week later.[66] As of September 15, the government announced that the app has had more than 1 million downloads.[67] As of October 2020, the Google Play store shows that the app has over 100,000 downloads.[68] The app requires IOS 11.0 or later.[69]

The application is voluntary and users must register with a national ID number. It relies on GPS technology to live-track the location of its users. Individuals are informed of the use of GPS technology on the app before its download and use. The app uploads the user's location data to a central server.[70]

The app will notify individuals when "they are approaching a location where an active case has been detected, or if they were in close proximity with an active confirmed case."[71] The app also provides national information about the spread of COVID-19, as well as updates on new government measures to combat the virus. The government claims that location

61 Ibid. art. 12, 13
62 Ibid. art. 14, 15, 16
63 BBC News. "Coronavirus: Alarm over 'invasive' Kuwait and Bahrain contact-tracing apps." June 16, 2020. https://www.bbc.com/news/world-middle-east-53052395
64 Ibid.
65 Kingdom of Bahrain, eGovernmnet Apps Store. "BeAware Bahrain." https://apps.bahrain.bh/CMSWebApplication/action/ShowAppDetailsAction?selectedAppID=321&appLanguage=en
66 Ali Al Qaed, Mohammed, Al Arabiya. "Bahrain's 'BeAware' coronavirus app has saved lives: Here's how." August 13, 2020. https://english.alarabiya.net/en/views/news/middle-east/2020/08/13/Bahrain-s-BeAware-coronavirus-app-has-saved-lives-Here-s-how
67 Bahrain Information and eGovernment Authority. "Information & eGovernment Authority announces jump in government app August & eservices." September 15, 2020. https://www.iga.gov.bh/en/article/information-and-egovernment-authority-announces-jump-in-government-app-august-and-eservices
68 Google Play. "BeAware Bahrain." https://play.google.com/store/apps/details?id=bh.bahrain.corona.tracker&hl=en_US&gl=US
69 Apple Store. "BeAware Bahrain." https://apps.apple.com/app/id1501478858?mt=8
70 El Sherif, Ahmed. "Bahrain, Kuwait and Norway spark privacy concerns." June 19, 2020. https://www.mobihealthnews.com/news/emea/covid-19-tracing-apps-bahrain-kuwait-and-norway-spark-privacy-concerns
71 eGovernment Apps Store, Kingdome of Bahrain. "BeAware Bahrain." https://apps.bahrain.bh/CMSWebApplication/action/ShowAppDetailsAction?selectedAppID=321&appLanguage=en

data older than six weeks old is automatically deleted. Users are also said to be granted the right to request their data be deleted from the system at any time.

The Minister of Health issued a decision requiring all self-isolating people to wear a Bluetooth bracelet which can be paired with the app. A warning will be sent from the monitoring station if individuals are more than 15 meters away from their phone.[72] Location data from this bracelet, along with other diagnostic data, is uploaded to a central server. Officials from the Ministry of Health are also able to randomly request verification pictures that must include faces and bracelets from individuals in quarantine.[73]

Penalties for not wearing the bracelet or complying with quarantine include imprisonment for 3 months and/or a fine of between BD1,000 and BD10,000 (2652 to 26,520 USD), as per public health law no. 34 of 2018. Tampering with the Bluetooth bracelet is also considered a violation. Once the mandatory fourteen-day quarantine period has been completed, users are allowed to turn off the GPS tracking on the app.[74]

The privacy policy for the application is not specific to the app but, instead, is a generic privacy policy outlining the terms and conditions for how all data is processed and controlled by the Information and eGovernment Authority.[75] The policy states that the legal basis for processing individual's data is outlined in Law No. 30 of 2018 on the Issuing the Personal Data Protection law. Furthermore, it explicitly states that the Information and eGovernment Authority "may be required to disclose personal data in response to legal requests by government authorities, including meeting national security or law enforcement requirements."[76]

The government has said that "there is an established relationship of trust between Bahrain's citizens and residents and the government" and this trust has been "an important ingredient of the Kingdom's ability to deploy technology in their COVID-19 response."[77] The government has also stated publicly that the application "ensures the privacy of users through fully automated processes, implemented without any human intervention whatsoever, in addition to providing data encryption and user privacy" but does not provide any further details on what these privacy measures are.[78]

> "The application lacks the necessary technical safeguards for the protection of privacy, while the law grants far-reaching exemptions to security authorities."

The application was criticized for being connected with a television show, called "Are You At Home?", which used the BeWare App to access telephone numbers of unsuspecting Bahrainis to check whether they were following the government's advice and remaining at home. Every day, the television show would choose ten random numbers and call to check if the individuals were at home; if they were, they won a prize. Enrollment in the show was automatic and mandatory at first. Later, there was a feature added to the app allowing individuals to opt out of participation.[79]

Assessment

The technical components of Bahrain's contact tracing application, as well as the country's broader legal infrastructure, raise concerns about the protection of the right to privacy. The application lacks the necessary technical safeguards for the protection of privacy, while the law grants far-reaching exemptions to security authorities.

In an important investigation by Amnesty Tech, Bahrain's app was named as one of "the most alarming mass surveillance tools" in all of the applications surveyed.[80] The

72 Information and eGovernment Authority. "The iGA begins distribution of electronic bracelets compatible with 'BeAware' app." April 4, 2020. https://www.iga.gov.bh/en/article/the-iga-begins-distribution-of-electronic-bracelets-compatible-with-beaware-app

73 Ibid.

74 Ibid.

75 Information and eGovernment Authority. "Privacy Policy. https://bahrain.bh/wps/portal/!ut/p/a1/pZDLCoJQEIafxYVbZ_SUSLtjkmlakUl6NqFxUsMbatHjZy6CoBs0i4H5-T6YGWAQACujS5ZEXVaVUX6fmbqfr1CVFU2xzRkxkC5dYqx1nyy8UQ-EPYCKO5WtkWKj6yJSTd8429kUUSP_-eav_pui-M33eAk7YAP26YqPgPkA3u9hA0vyKh5-GtIyJloCrOFH3vBGOjd9nHZd3U5EFDGq61bqW86lQ1WI-EpJq7aD4JmEuvD94GqdxvnFoVQQbu3F7dQ!/dl5/d5/L2dBISEvZ0FBIS9nQSEh/

76 Ibid.

77 Ali Al Qaed, Mohammed, Al Arabiya. "Bahrain's 'BeAware' coronavirus app has saved lives: Here's how." August 13, 2020. https://english.alarabiya.net/en/views/news/middle-east/2020/08/13/Bahrain-s-BeAware-coronavirus-app-has-saved-lives-Here-s-how

78 Information and eGovernment Authority. "iGA Chief Executive Highlights Bahrain's COVID-19 Response at Global Ministerial Conference." July 3, 2020. https://www.iga.gov.bh/en/article/iGA-Chief-Executive-Highlights-Bahrain-COVID-19-Response-at-Global-Ministerial-Conference

79 Amnesty International. "Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy." June 16, 2020. https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/

80 Ibid.

investigation pointed to the apps reliance on real-time location data tracking, use of national ID numbers, and the use of a central server as serious privacy concerns. Amnesty Tech's reporting did not cause the Bahraini government to change the technical infrastructure of the app.[81]

There are no coercive mechanisms or regulations that enforce the app's limited purpose. Because there were no regulations released alongside the app, there are no guidelines, nor independent oversight determining an appropriate end date and cessation of use. There are also serious transparency concerns. The source code for the app is not open source and cannot be scrutinized by security researchers. There is also a lack of information on how the data is being used and with whom it is shared.

There are some limited privacy preserving mechanisms of the app, including that the use of the app is voluntary. Government statements have also claimed that individuals have the right to request their data to be deleted; however, it is unclear whether any Bahraini has successfully requested and deleted their data.

81 Ibid.

Country Studies: The United Arab Emirates

As of December 7th, 2020, there have been a total of 176,429 confirmed cases of COVID-19 and 592 deaths in the United Arab Emirates.[82] In response to the pandemic, the UAE government launched a total of three contact tracing and quarantine monitoring applications: StayHome, TraceCovid, and Alhosn. The StayHome app, launched in May 2020 by Abu Dhabi's Department of Health, is designed to monitor individuals who have been directed to quarantine.[83] Abu Dhabi's Department of Health also launched a second application called TraceCovid. This app was designed to assist and augment contact tracing by tracking infected individuals. Finally, the Alhosn app was launched on May 14, 2020 by both the Department of Health Abu Dhabi and the Dubai Health Authority. The Alhosn app combines the functionality of both the StayHome and TraceCovid apps and acts as the "the official integrated digital platform for COVID-19 tests in the UAE."[84] In addition to providing coronavirus test results, the app also tracks and traces infected individuals.[85]

The UAE has been accused of financing a sprawling domestic mass surveillance system, with one of the highest concentrations of surveillance cameras in the world.[86] Freedom House rated the country 1 out of 4 in response to the question: "Are individuals free to express their personal views on political or other sensitive topics without fear of surveillance or retribution?"[87] The country has been repeatedly accused of enhancing their domestic electronic surveillance in order to stifle freedom of expression and suppress peaceful critics.[88] While the UAE has a number of sector specific data protection and privacy laws, this troubling history of domestic surveillance raises serious doubts about the extent to which these laws are respected by state security authorities.

Legal Framework Of Data Protection And Privacy In The United Arab Emirates

There is not yet a unified, national data protection law in the UAE. Instead, there are a number of sector specific data protection laws, such as the Health Data Law, and data protection laws specific to financial free trade zones, such as the Abu Dhabi Global Market and the Dubai International Financial Center.

There are also a number of articles and provisions in other federal laws pertaining to data protection and privacy. The Emirati Constitution guarantees freedom and secrecy of communications. Article 31 reads: "Freedom of communication by means of the posts, telegraph or other means of communication and their secrecy shall be guaranteed in accordance with the law."[89]

In addition to the constitution, the Penal Code, the Civil Code, the Cybercrime Law, the Labour Law, the Emcredit Law, the Electronic Transactions and Commerce Law, the Medical Liability Law, the Telecommunications Law, the Regulatory Policy on Unsolicited Electronic Communications, and the Regulatory Framework for Electronic Payments all contain some provisions related to data protection and privacy.

There are two data protection laws and regulations governing the control and processing of data in their respective financial free trade zones: the 2015 Data Protection Regulations for the Abu Dhabi Global Market and the 2020 Data Protection Law for the Dubai International Financial Centre. The former protects personal data within Abu Dhabi's Global Market (ADGM) and governs how data can be used by businesses – data controllers and processors -- within the ADGM zone. The law came into effect on October 21, 2015 and amendment regulations came into effect on February 1, 2018.

The 2020 Data Protection Law for the Dubai International Financial Centre governs the control and processing of data within this financial free trade zone. Businesses and organizations were originally required to comply with these regulations by July 1st, 2020. Given the COVID-19 pandemic,

82 World Health Organization. "United Arab Emirates: WHO Coronavirus Disease Dashboard." Accessed on December 7, 2020 https://covid19.who.int/region/emro/country/ae

83 The United Arab Emirates' Government portal. "The StayHome app." May 5, 2020. https://u.ae/en/information-and-services/justice-safety-and-the-law/handling-the-covid-19-outbreak/smart-solutions-to-fight-covid-19/the-stayhome-app

84 The United Arab Emirates' Government portal. "The ALHOSN UAE app." May 14, 2020. https://u.ae/en/information-and-services/justice-safety-and-the-law/handling-the-covid-19-outbreak/smart-solutions-to-fight-covid-19/the-alhosn-uae-app

85 Ibid.

86 Gambrell, Jon. Associated Press. "Virus projects renew questions about UAE's mass surveillance." July 9, 2020. https://www.washingtonpost.com/world/the_americas/virus-projects-renew-questions-about-uaes-mass-surveillance/2020/07/09/4c9a0f42-c1ab-11ea-8908-68a2b9eae9e0_story.html

87 Freedom House. "The United Arab Emirates, 2019." https://freedomhouse.org/country/united-arab-emirates/freedom-world/2020

88 Human Rights Watch. "UAE: Authorities Enhance Surveillance of Critics." January 12, 2017. https://www.hrw.org/news/2017/01/12/uae-authorities-enhance-surveillance-critics

89 Constitution of the United Arab Emirates, art. 31 https://uaecabinet.ae/en/the-constitution

the government allowed a three-month extension on this deadline, ultimately requiring compliance by October 1, 2020.[90]

2015 Data Protection Regulations for the Abu Dhabi Global Market (ADGM)

Data Protection Principles

The law applies to data controllers and processors that handle data within the ADGM free trade zone.[91]

Data controllers must provide notice to individuals when collecting their personal data as soon as possible, as per article 6. This notice must include the purposes for which the data is being processed, as well as any other information that is necessary to ensure fair processing.[92] Data subjects have the right to withdraw this consent and prevent any further processing of data.[93]

Personal data is defined as "any information relating to an identifiable natural person".[94] Sensitive personal data is further defined as data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, criminal record, trade union membership, and health or sex life. Data controllers are defined as any person in the ADGM who determines the purposes and means of processing data. Data subjects are defined as the natural persons connected with personal data.[95]

The Rights of Data Subjects in the ADGM

The rights of data subjects are outlined in section two of the regulations. Data subjects have the right to consent to the use and processing of their data; consent or another legal basis is required for controllers to process data.[96] For sensitive personal data, separate and written consent is first required in order to process this data.[97] Data subjects have the right to access, correct, erase, or block data that is inaccurate. Data subjects also have the right to object to the processing of their data at any time on reasonable grounds. [98]

Data subjects have the right to obtain from data controllers' confirmation of the processing of their data, the purpose of the processing, the kinds of personal data being processed, and the entities to whom the data is being disclosed.[99]

Data subjects have the right to lodge complaints with the registrar, as per section 18.[100] Data subjects who suffer damage as result of a violation of certain provisions are entitled to compensation for the damage, as per section 17.[101]

Legal Obligations for Data Controllers and Processors in the ADGM

Data controllers must ensure that the data they process is done so fairly, lawfully, and securely.[102] Data must not be processed in a way that is incompatible with the rights of individual data subjects. The data must only be processed according to specified, explicit, and legitimate purposes, and not exceed nor transgress these.[103] Data processing must also be adequate, relevant, and not exceeding the purposes for which data is collected. Data must not be maintained for longer than is necessary, according to its purpose of collection.[104]

Data controllers also must obtain consent, or another legal basis before processing personal data and sharing this data with government authorities or other third parties.[105] Consent must also be obtained before the processing begins.[106]

90 Dubai International Financial Centre. "Mohammed bin Rashid enacts new DIFC Data Protection Law." June 1, 2020. https://www.difc.ae/newsroom/news/mohammed-bin-rashid-enacts-new-difc-data-protection-law/
91 Data Protection Regulations 2015; Data Protection Regulations 2018 https://en.adgm.thomsonreuters.com/rulebook/data-protection-regulations
92 Ibid. art. 6
93 Abu Dhabi Global Market, Office of Data Protection. Data Protection Guidance Note. Section 14.7 https://www.adgm.com/documents/office-of-data-protection/guidance/data-protection-guidance-notes.pdf
94 Data Protection Regulations 2015; Data Protection Regulations 2018. art. 20
95 Ibid. art. 20
96 Ibid. art. 2
97 Ibid. art. 3
98 Ibid. art. 11
99 Ibid. art. 10
100 Ibid. art. 18
101 Ibid. art. 17
102 Ibid. art. 1
103 Ibid. art. 1
104 Ibid. art. 1
105 Ibid. art. 2, 10
106 Ibid. art. 2

Data controllers are obligated to provide adequate technical and organizational measures to protect against unauthorized loss, destruction or damage to personal data.[107] Data processors are further obligated to inform data controllers in the event of a data breach or data loss, as soon as possible. Section nine also requires data controllers and processors to notify the registrar of a breach as soon as is reasonably practical.[108]

Data controllers must inform the registrar upon the decision to become a data controller.[109] Any entities wishing to process personal data or sensitive data must receive approval from the registrar. Controllers must establish and maintain records of their data processing activities.[110]

Transferring data outside of the ADGM can only occur if the jurisdiction has been designated as having an adequate level of personal data protection.[111] Other exemptions and conditions also apply. Controllers are liable for a fine of up to 15,000 USD if they do not comply with the data protection regulations or directions issued by the registrar.[112]

Health Data Law

Federal Law No. 2 concerning the use of information and communication technology in the health sector governs all electronic data in the UAE related to healthcare and is designed to protect sensitive healthcare data. The law defines the responsibilities for the collection, control and processing of healthcare data by healthcare providers, medical insurance providers, healthcare IT providers and other entities interacting with this data in the UAE.[113] The regulations stemming from the law were issued on April 22, 2020 via Cabinet Resolution 32 of 2020; these regulations come into effect on November 1, 2020. The Ministry of Health and Prevention is the effective regulator of the law.[114]

The law grants control to UAE's Ministry of Health to protect healthcare data originating within its borders. It also outlines certain provisions which allow for the collection and analysis of this data for the purpose of improving public health policies. There are three supervisory authorities for the law: The Ministry of Health and Prevention, the Dubai Healthcare city Authority, and the Customer Protection Unit at the Centre of Healthcare Planning and Quality in Dubai.

Data is defined as all electronic data originating in the UAE related to the healthcare sector. Unlike the two other free trade zone specific data laws, the healthcare data law is a federal law and applies to all entities in the UAE that provide healthcare services or handle electronic healthcare data, including entities within the free trade zones.[115]

The regulations issued in April 2020 pertain to the authorized access to the mandated centralized healthcare database, the conditions of use of this database, provisions regarding the exchange of healthcare data, and requirements for the storage of healthcare data.[116]

The Rights of Data Subjects

Under the healthcare data law, the confidentiality of healthcare data and patient information is guaranteed. Anyone coming into contact with healthcare data must maintain its confidentiality and only use it for health purposes, unless the patient's written consent is given.[117]

There are five circumstances under which the law allows healthcare data to be shared without obtaining the data subject's consent:

1. Responding to a request for information issued by insurance companies covering medical services;

2. For the purpose of scientific research

107 Ibid. art. 9
108 Ibid. art. 9
109 Ibid. art. 12
110 Ibid. art. 12
111 Ibid. art. 4
112 Ibid. art. 17
113 PwC. "Healthcare data protection in the UAE: A new federal law." https://www.pwc.com/m1/en/publications/documents/healthcare-data-protection-in-the-uae.pdf
114 Library of Congress Law. "Regulating Electronic Means to Fight the Spread of COVID-19: the UAE." https://www.loc.gov/law/help/coronavirus-apps/uae.php
115 United Arab Emirates, Federal law no. 2 concerning the use of information and communication technology in the health sector. Art. 2 https://elaws.moj.gov.ae/MainArabicLawFromLaw.aspx?val=UAE-LC-Ar_2019-02-06_00002_Kait.html,AL1,&np=undefined&lmp=undefined
116 Baker McKenzie. "United Arab Emirates: Updates on UAE health regulations." July 14, 2020. https://www.lexology.com/library/detail.aspx?g=e672fe0c-bb26-4629-bbee-629389fb1d1d
117 United Arab Emirates, Federal law no. 2. art. 16

3. For the purpose of adopting preventative public health and treatment measures;

4. To respond to a request for information issued by a judicial authority;

5. To respond to a request from health authorities for public health.[118]

The Regulations based on the law that were issued in 2020 outline further rights for data subjects. Most importantly, the regulations grant the right to data subjects to opt out of the centralized health database outlined in both the health data law and its regulations.[119]

Legal Obligations for Data Controllers and Processors

The law obliges controllers and processors of health care data to protect the data against unauthorized loss, alteration, deletion, addition or access. All necessary technical precautions must be taken to ensure the security of the data.[120] All entities processing health care data are obliged to keep this data confidential and only authorized individuals have access to it. Data controllers are not allowed to share this data without authorization from the data subject.[121]

> “ Article 20 mandates that all healthcare entities are required to retain data for a period not less than 25 years. ”

The law puts significant constraints on the transfer of data outside the borders of the UAE. It is not permissible to store, process, generate or transmit health data outside of the UAE, unless a special exemption has been granted by the Ministry.[122] The penalty for violating this rule is a fine between 500,000 and 700,00 Emirati Dirhams (136,130 to 190,582 USD).

The law also places strict conditions on the preservation of healthcare data. Article 20 mandates that all healthcare entities are required to retain data for a period not less than 25 years from the date of the last instance where the data was gathered.[123]

A centralized data management system is also outlined in the law. A centralized system for the management and processing of healthcare data will be created and controlled by the federal Ministry of Health.[124] All of the data collected and processed by healthcare entities will be housed within this database. Data stored in this database will be controlled by regulations set forth by the government that will ease access and exchange of data.[125] Only certain entities with permission from health authorities will have access to this database. The integrity and accuracy of the data must be ensured.[126]

The regulations provide more detail on the centralized database. A centralized committee will be established to take responsibility for the creation and maintenance of the database. The committee will include the Ministry of Health and other local health authorities. The Ministry of Health will be responsible for verifying that the data in the database meets quality and compliance standards. Entities uploading and making use of the database are required to adhere to certain privacy and security standards that ensure the accuracy and integrity of the data.[127]

Health care data controllers and processors can be subject to penalties if provision in the law are violated. Fines range from one thousand to one million Emirati Dirhams (272 to 272,260 USD) for violations of the law.[128]

COVID-19 Contact Tracing App In The UAE

The AlHosn UAE contact tracing application was jointly launched by the Ministry of Health and Prevention, the Abu Dhabi Health Authority, and the Dubai Health Authority. The AlHosn app is the official digital platform for COVID-19

118 Ibid. art. 16
119 Baker McKenzie. “United Arab Emirates: Updates on UAE health regulations.” July 14, 2020. https://www.lexology.com/library/detail.aspx?g=e672fe0c-bb26-4629-bbee-629389fb1d1d
120 United Arab Emirates, Federal law no. 2, art. 4
121 Ibid. art. 4
122 Ibid. art. 13
123 Ibid. art. 20
124 Ibid. art. 5
125 Ibid. art. 6
126 Ibid. art. 8
127 Baker McKenzie. “United Arab Emirates: Updates on UAE health regulations.” July 14, 2020. https://www.lexology.com/library/detail.aspx?g=e672fe0c-bb26-4629-bbee-629389fb1d1d
128 United Arab Emirates, Federal law no. 2, art. 25

in the UAE and can be downloaded for iOS and Android. Before the launch of AlHosn, the department launched two other applications; "StayHome" and "TraceCOVID". The AlHosn app was later launched and combined the functionalities and purposes of these two apps.[129] The AlHosn app is available in Arabic, English, and Hindi. As of writing, there were over 1 million installs of the app via the Google Play store.

The app is not mandatory. Dr. Farida Al Hosani, an official spokesperson for the UAE health sector, explained: "the UAE did not impose the use of AlHosn app on individuals and institutions due to the government's confidence in the high level of awareness within the population of this crucial matter and its trust that there is a joint sense of responsibility shared by the various segments of our community, regardless of their nationalities or backgrounds."[130]

The app has three main functions: it provides contact tracing services to health authorities, it provides access to COVID-19 tests results, and remotely monitors home quarantining individuals. Individuals are required to enter their national ID and phone number to the app in order to register and authenticate it. Bluetooth and push notifications must be turned on.[131]

Bluetooth is used to connect with nearby devices that also have the app installed. Bluetooth will exchange encrypted Security Tracing Identifiers (STIs) locally with devices that come into proximity with each other. The government has said these STIs consist only of anonymized data and include timestamps to record the time of the encounter. These STIs are only stored locally on the phone for a period of three weeks and are encrypted.[132]

If an individual tests positive for COVID-19, health authorities will request that they share the stored list of encrypted STIs on their phone to contact those on the list. When two phones with the app come into close contact, they exchange metadata stored within them. The government guarantees a high degree of privacy protection through the use of artificial intelligence and "other technological tools".[133] They claim that the data is encrypted, and it only remains locally on the user's phone. The government has also claimed that the model that is used in the app is decentralized.[134]

Authorities claim that no personally identifiable information is collected through the app. Individuals will be contacted by Health authorities in the event that they test positive for COVID19. After testing positive, authorities will first request their consent before uploading the list of anonymized IDs registered in the app. Only the IDs from the last 21 days will be uploaded by health authorities.[135]

While the app is not officially mandatory, access to some public spaces, including parks and beaches, are restricted without the app. Anyone who wishes to enter these spaces must present a negative COVID-19 test result via the AlHosn app before entering.[136]

The government launched a series of nation-wide campaigns to encourage individuals to download and install the app because it was recognized that contact tracing apps rely on a high number of users to be effective.[137]

The government has repeatedly emphasized that the AlHosn app is an important part of the UAE's overall strategy in balancing the virus and the need to return to normal activities. The government said that downloading and using the app was "part of the civil duty of every individual." Travellers arriving to the UAE are required to install AlHosn to assist authorities with quarantine monitoring.[138]

129 WAM Emirates News Agency. "Health Sector launches new app 'ALHOSN UAE' as part of efforts to contain COVID-19." April 25, 2020. https://wam.ae/en/details/1395302838940

130 WAM Emirates News Agency. "Senior UAE officials praise Alhosn's pivotal role during reopening of activities." June 16, 2020. https://wam.ae/en/details/1395302848952

131 WAM Emirates News Agency. "UAE public urged to join COVID-19 contact tracing app Alhosn to protect themselves, communities." May 20, 2020. https://wam.ae/en/details/1395302843942

132 United Arab Emirates: the Supreme Council for National Security. "Alhosn UAE App." https://www.ncema.gov.ae/alhosn/index.html

133 WAM Emirates News Agency. "Health Sector launches new app 'ALHOSN UAE' as part of efforts to contain COVID-19." April 25, 2020. https://wam.ae/en/details/1395302838940

134 United Arab Emirates: the Supreme Council for National Security. "Alhosn UAE App." https://www.ncema.gov.ae/alhosn/index.html

135 Ibid.

136 WAM Emirates News Agency. "Abu Dhabi re-opens some public beaches, parks from tomorrow." July 2, 2020. https://wam.ae/en/details/1395302852846

137 WAM Emirates News Agency. "UAE public urged to join COVID-19 contact tracing app Alhosn to protect themselves, communities." May 20, 2020. https://wam.ae/en/details/1395302843942

138 WAM Emirates News Agency. "COVID-19 recoveries rise to 11809; 941 new cases identified." May 20, 2020. https://wam.ae/en/details/1395302843976

> “There is no independent oversight mechanism for the app, nor specific set of guidelines governing its use.”

Assessment

The UAE’s AlHosn app, together with its legal framework for health care data, have more robust data protection and privacy conditions compared to other states surveyed. AlHosn has the most detailed technical information on the app’s functions than any other state surveyed for this study. Users have a greater knowledge of privacy oriented design choices of the app, including the use of Bluetooth, rather than GPS location tracking. The app also makes use of anonymized STIs, stored locally on people’s devices, which are recommended by security and privacy researchers. The app is not mandatory, which grants users greater discretion and power over their data.

Despite these benefits, the code for the app is not open source. As a result, the technical description of the app must be taken for granted from statements and information released by the government. There are also no concrete details about exactly how long the data will be stored and whether there are any sunset clauses or mandatory deletion deadlines. This is particularly troublesome because the law itself mandates that health care data law be retained for a period of at least 25 years. It is not clear whether individuals have the right to delete or access data collected via the app.

Additionally, some public spaces are restricted unless the app is downloaded. These restrictions can disadvantage individuals unwilling to download the app and those who do not have a smartphone capable of running the app. This can lead to unfair discrimination against vulnerable groups. Finally, there is no independent oversight mechanism for the app, nor specific set of guidelines governing its use. These mechanisms are necessary in order to independently review and assess the use of the technology.

Country Studies: Kuwait

As of December 7, 2020, there have been 144,369 confirmed cases of COVID-19 in Kuwait and 891 deaths.[139] Kuwait's Ministry of Health launched an app, "Shlonik", to monitor individuals in quarantine and to track COVID-19 cases throughout the country. In a report released in June, Amnesty Tech identified Kuwait's "Shlonik" app as one of the most invasive COVID-19 tracing apps in the world.[140] The Kuwaiti government has also been accused of widespread domestic surveillance. Freedom House has claimed that "freedom of expression [in Kuwait] is curtailed by state surveillance".[141]

Legal Framework Of Data Protection And Privacy In Kuwait

There is no national privacy law in Kuwait, nor is there a data protection regulating authority. However, there are other laws that contain provisions related to privacy. The Constitution of Kuwait guarantees the right to privacy. Article 39 writes: "Freedom of postal, telegraphic and telephone correspondence is safeguarded and confidentiality is guaranteed. Messages may not be monitored except in instances specified by law and in accordance with those procedures."[142]

> "There is no national privacy law in Kuwait, nor is there a data protection regulating authority."

Law no. 20 of 2014 contains privacy provisions related to electronic transactions. The law regulates civil, commercial and administrative transactions in general, and there are some provisions governing electronic records, signatures, transactions, messages and documents related to these transactions.[143]

Provisions related to data protection and privacy are outlined in chapter seven of the electronic transactions law. The unlawful access, disclosure, or publishing of personal data related to personal, financial, or health status is prohibited without the consent of the concerned individuals. Entities are required to detail the reason why personal data is being collected, as well as ensure its accuracy. Entities are also required to protect data from loss, damage, or unauthorized access. Data subjects have the right to request access to this data and to delete or change their own data. The law outlines penalties for violating the law, which include fines between 5,000 and 20,000 Kuwaiti Dinars (16,368 USD to 65,474 USD) and up to three years imprisonment.[144]

Unfortunately in Kuwait, public and private entities alike are left to their own discretion to decide the rights of data subjects. There is no larger authority to guide these issues. There are also no clear guidelines to determine the rights of data subjects, the responsibility of data controllers and processors, and general principles for data protection and privacy.

COVID-19 Contact Tracing App In Kuwait

On April 18th, Kuwait's Ministry of Health, in collaboration with the Central Agency for Information Technology, launched a COVID-19 contact tracing app called "Shlonik".[145] The app is available for devices that support iOS 10.0 or later or Android and is available in five different languages: Arabic, English, Urdu, Tagalog and Bengali. A phone number and national ID number are required to sign up for the app.[146] There were over 100,000 downloads on the Google Play store by the time of writing.[147]

139 World Health Organization. "Kuwait: WHO Coronavirus Disease Dashboard." Accessed on December 7, 2020 https://covid19.who.int/region/emro/country/kw

140 Amnesty International. "Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy." https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/

141 Freedom House. "Kuwait, 2019." https://freedomhouse.org/country/kuwait/freedom-world/2020

142 Kuwait, Constitution. art. 39 http://www.kna.kw/clt-html5/run.asp?id=2024

143 Kuwait, Law No. 20 of 2014 Concerning Electronic Transactions https://www.e.gov.kw/sites/kgoArabic/Forms/MagazineA.pdf

144 Ibid. art 32 - 36

145 Kuwait News Agency. "MoH taps technology to monitor home-quarantined returnees." April 18, 2020. https://www.kuna.net.kw/ArticleDetails.aspx?id=2886643&language=en

146 Library of Congress. "Saudi Arabia; Oman; Kuwait: Ministries of Health Begin Using Mobile Apps to Combat COVID-19." June 18, 2020. https://www.loc.gov/law/foreign-news/article/saudi-arabia-oman-kuwait-ministries-of-health-begin-using-mobile-apps-to-combat-covid-19/

147 Google Play. "Shlonik." https://play.google.com/store/apps/details?id=com.healthcarekw.app&hl=en_GB&gl=US

The app is designed to monitor individuals in mandatory quarantine and was first launched in concert with Kuwait's effort to repatriate stranded Kuwaiti citizens.[148] Citizens and other individuals returning to Kuwait are required to download and install the app on their mobiles. Bluetooth is required to be turned on in order to track people who may have come into contact with positive cases.[149]

Returnees are also provided with a mandatory bracelet at the airport upon arrival. The location of returnees is tracked through both the application and the bracelet. Individuals are required to complete their first check-in upon arrival at the airport by recording a voice note through the app and taking a photo of themselves that clearly shows their face. They are also required to register their quarantine location. All of this data will be used to verify future check-ins via the app. The Ministry of Health has stated that they use AI technology to verify these check-ins.[150]

The app is paired with the bracelet to ensure that returnees are abiding by the mandatory 14-day quarantine. Amnesty Tech found that the application frequently checks the distance between the bracelet and the device and that location data was uploaded to a central server every ten minutes.[151] Individuals in mandatory quarantine are also required to send live selfies to the application to confirm that they are abiding by the quarantine rules. The Ministry of Health has the ability to contact quarantine people through the app and request live selfies at random intervals to confirm they are abiding by the rules. These photos are matched with previous photos to ensure compliance. They will also request vital signs, like temperature, to monitor the health of the individual.[152]

People who break the 14-day quarantine rule could be subject to a fine of up to 5,000 Kuwaiti dinars (16,368 USD), three months imprisonment, or both. If individuals are caught violating quarantine, they will be taken directly to a governmental quarantine facility and possibly face legal action.[153]

Dr. Mona Al-Khabaz, a representative from the Ministry of Health, stated that the application is supported by a 24-hour monitoring center. The center is said to have more than 100 doctors who are tasked with monitoring quarantining people and providing health advice to those in need.[154]

The app provides official information about the coronavirus and allows users to message or speak directly with doctors affiliated with the Ministry of Health. The privacy policy for the application directs to the Kuwait government online privacy statement; there is no specific privacy policy for the application itself.[155]

Assessment

Both the technical components of Kuwait's COVID-19 contact tracing application and the country's broader data legal framework raise serious privacy concerns. The app was not launched with a limited purpose that detailed a bookended duration or the epidemiological conditions under which the program will be suspended.

There is also a notable lack of transparency in regard to the app. The source code is not open source and is therefore not available for scrutiny. There is not enough available information relating to how personal data collected through the app is processed, including mandatory sunset clauses requiring the timely deletion of data.

According to government statements, data is uploaded to a centralized server and the app requires personally identifiable information, such as a national ID number and phone number. These design components do not adhere to the principle of privacy protection by design and data minimization.

These concerns about the technical components of the app and lack of transparency surrounding its use are further compounded when considered that Kuwait lacks a data protection framework. There are no guidelines governing the proper collection and processing of sensitive health data, nor any independent oversight mechanisms that could establish independent reviews and assessments of the technology.

148 Kuwait Times. "Bader Al-Kharafi: Zain changes network name to 'Shlonik'." April 21, 2020. https://news.kuwaittimes.net/pdf/2020/apr/21/p05.pdf
149 Kuwait News Agency. "MoH taps technology to monitor home-quarantined returnees." April 18, 2020. https://www.kuna.net.kw/ArticleDetails.aspx?id=2886643&language=en
150 Kuwait Times. "Bader Al-Kharafi: Zain changes network name to 'Shlonik'." April 21, 2020. https://news.kuwaittimes.net/pdf/2020/apr/21/p05.pdf
151 Amnesty International. "Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy." June 16, 2020. https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/
152 Kuwait News Agency. "MoH taps technology to monitor home-quarantined returnees." April 18, 2020. https://www.kuna.net.kw/ArticleDetails.aspx?id=2886643&language=en
153 Ibid.
154 Xinhua News Agency. "Kuwait uses app to monitor quarantined returnees." May 12, 2020. https://www.macaubusiness.com/kuwait-uses-app-to-monitor-home-quarantined-returnees/
155 Kuwait, eGovernment privacy policy https://www.e.gov.kw/sites/kgoenglish/Pages/InfoPages/PrivacyStatement.aspx

Conclusion

Regional Trends

In the mid-2010s, many Gulf states began to recognize the financial and economic need for adequate data protection and privacy legislation. While early adopters elsewhere in the region passed data protection guidelines in the late 20th century – Israel, mainly – most other states in the region began discussing similar legislation in the 2010s. Currently, Qatar, Bahrain, and the UAE have at least some form of data protection and privacy legislation. The one notable exception is Kuwait, which does not yet have a national level data protection law.

Broadly, the data protection and privacy laws surveyed within the three states that currently have data protection laws resemble international standards like the EU's GDPR and Directive. The laws resemble these international standards in both structure and substance. Regarding structure, most of the laws surveyed assign a data regulatory authority at the national level, although the activeness of this authority varies greatly among jurisdictions. These jurisdictions also broadly resemble international data protection standards regarding fundamental data protection principles, the rights of data subjects, and the legal obligations of data controllers. At the same time, some articles within these laws distinguish these jurisdictions in important ways from international standards, particularly exemptions related to national security and security authorities. Moreover, in the Gulf states surveyed, a lack of evidence of demonstrating enforcement of these laws suggests they may exist on paper only.

Lack of Evidence of Enforcement

There is a notable lack of information which indicates broad enforcement of data protection and privacy laws within these jurisdictions. The four jurisdictions surveyed have either enforcement authorities that are significantly inactive or no enforcement authority at all. Additionally, it was difficult to find evidence of cases where existing data protection laws were enforced; this was particularly pronounced in Qatar, Bahrain and the UAE. The lack of evidence of people or entities taken to court under these laws brings forward important questions about the level of implementation of data protection laws in these jurisdictions. The absence of evidence of enforcement suggests the extent to which these laws are actually applied is limited.

The following is a timeline of the most relevant data protection laws within the surveyed jurisdictions:

2005 Qatar Financial Centre Data Protection Regulations (financial centre law)

2015 United Arab Emirates, Abu Dhabi Global Market Data Protection Regulations (financial centre law)

2016 Qatar Protection of Personal Data (national law)

2018 Bahrain the Issues of the Personal Data Protection Law (national law)

2019 United Arab Emirates, Health Care Data Law (national law)

2020 United Arab Emirates, Dubai International Financial Centre Data Protection Law (financial centre law)

In terms of structure, both the UAE and Qatar established subnational data protection laws covering special financial zones before passing national level data protection laws. The UAE still does not have a non-sector specific national level data protection law, but it is rumored this law is under discussion.

The responsible regulatory authority varies among these jurisdictions. While Bahrain's data protection law outlines the creation of a data protection authority, this authority has not yet been established nor allocated a budget. Instead, the Ministry of Justice has been acting in this role until a separate authority is established. The Ministry of Transport and Communications is the responsible data regulatory authority at the national level in Qatar while Qatar's Financial Centre Regulatory Authority is responsible for data matters in that jurisdiction. In the UAE, a Data Protection Administrator is established within the Dubai International Financial Centre; the Registration Authority Registrar is the responsible authority within the Abu Dhabi Global Market.

Data Principles Across Jurisdictions

Fundamental Principles

Fundamental principles for the collection and use of data across these five jurisdictions broadly aligns with standards set forth by the European Union in both the EU's Directive

and the GDPR. The important exception is Kuwait, which does not yet have a data protection or privacy law. The UAE does not yet have a non-sector specific federal data law; instead, there are two emirate level data laws covering the two different free trade jurisdictions and a federal level health care data law. The UAE's health care data law is the only one of its kind in the Gulf.

Qatar, Bahrain, and the UAE share similar data protection principles in regard to the collection and use of data. Across these jurisdictions, data must be processed fairly, honestly, legitimately for a clear and specific purpose. Data must be processed only in support of the purposes for which it was originally collected. These principles are articulated within the national data laws of Qatar, Bahrain, and within the Emirate level data laws of Dubai and Abu Dhabi. There are no notable differences in the definitions of personal data, sensitive data, data controller and data processor across these jurisdictions.

In Qatar, and Bahrain, data laws apply to all natural and legal persons. In the UAE, the law is applicable to these persons established within the free zone under the jurisdiction of the law (either Abu Dhabi free zone or Dubai free zone). Bahrain and Qatar share special exemptions for data processed in the context of personal or family affairs; in both of these jurisdictions, the law does not apply to data processed under such circumstances.

The appointment of a data protection officer varies across jurisdictions. In Qatar, Bahrain, and the Abu Dhabi Global Market, there is no obligation to appoint a data protection officer. In Qatar, the role of data protection officers is not outlined in the law; whereas in Bahrain, while there is no mandate requiring the appointment of a protection officer, it is possible for the data authority in that country to issue requirements for certain kinds of data controllers to appoint a protection officer. In the Dubai International Financial Centre, the appointment of a data protection officer is voluntary, unless a controller or processor is conducting high-risk processing.

Bahrain, the Dubai International Financial Center, and the Abu Dhabi Global Market share similar restrictions on cross border data transfers; these restrictions broadly reflect international standards. These jurisdictions do not allow data to be transferred outside of their borders, except under certain conditions. These conditions will vary by jurisdiction, but all include the foundational principle that transfers cannot occur unless the receiving country at minimum ensures a level of protection that is comparable with that provided under the sending state's law. Qatar is an outlier in its approach to cross border data transfers insofar as data controllers are instructed to not take any action that would reduce the flow of data across borders, unless this processing violates the terms of the law or violates the privacy of the individual.

Sanctions for violating the provisions of each respective jurisdiction vary. These sanctions range from only fines in some jurisdictions to the possibility of imprisonment in others.

Rights Of Data Subjects

Jurisdictions with designated data protection and privacy laws establish rights for data subjects broadly in line with international standards like the GDPR. Across these jurisdictions, data subjects have the right to be notified as to the processing of their data and the purpose of the processing. Qatar and the two free zones in the UAE outline a general right to object to the processing of one's personal data. In Bahrain, the right to object to processing is limited to the right to object to processing for the purposes of direct marketing or the making of one's data public; there does not appear to be a general right to object to processing.

Across all three jurisdictions with data protection laws, data subjects are granted the right to consent to the processing of their data and the right to withdraw this consent. These jurisdictions all detail the right of data subjects to access, correct and delete their own personal data.

It must be reminded that the data subject rights in the UAE outlined above apply only to the two economic free trade zones – Dubai International Financial Centre and Abu Dhabi Global Market – as the UAE does not have a federal level data protection law, except for the law specific to healthcare data.

Legal Obligations Of Data Controllers

In addition to establishing rights for data subjects, data protection laws in these jurisdictions also detail legal obligations and responsibilities for data controllers and processors. Such obligations are in addition to the duties and obligations data controllers and processors have to data subjects.

Broadly, the duties and obligations of data controllers and processors in Qatar, Bahrain, the Abu Dhabi Global Market, and the Dubai International Financial Centre are in line with international standards like the GDPR. Controllers are

obligated to process data lawfully and fairly. Processing must be in line with principles such as transparency, integrity and respect for the rights of data subjects. They are obliged to comply with the conditions of processing outlined in the law. Data controllers must process data according to the purpose for which it was collected and should not exceed this purpose. Processors are also required to respond to requests from data subjects.

Controllers and processors are also obligated to protect against unauthorized or illegitimate access to data under their responsibility. Adequate technical and administrative security measures must be undertaken to protect against loss, damage, deletion, or unauthorized access to data. Controllers must ensure their processors are taking adequate measures. Processors are also obligated to inform controllers in the event of a data breach. Controllers are also obligated to inform data subjects in the event of a data breach, if the breach causes harm to the privacy of the data subject.

There are no major differences in the detailed obligations and responsibilities of data controllers and processors across these jurisdictions. One outlying article of note, however, is found in the UAE's Healthcare Data Law. Controllers of healthcare data are obligated to retain data for at least 25 years from the date of the last instance where the data was gathered. This remarkably long mandatory retention period differs greatly from every other jurisdiction surveyed and international data retention standards.

Exemptions Related To National Security

The legal authority upon which governments and entities can collect, process, and access data broadly resembles international standards. However, some states have granted themselves supplemental powers and special exemptions related to national security. The existence of broad exemptions on the basis of national security have important implications for the health of data protection and privacy in the region. The existence of these exceptions are fundamental when we consider whether or not these frameworks have adequately protected the right to privacy, or instead, have sanctioned and facilitated privacy violations.

Of the jurisdictions surveyed, Bahrain has the largest, far-reaching exemptions related to national security. The law does not apply to any measures related to national security. Security related bodies like the Ministry of Defense, the Ministry of Interior, the National Guard, the National Security Service and "any other security service in Bahrain" are fully exempted from the law.

Qatar's privacy law also details exceptions related to national security concerns, although these exceptions are less comprehensive than Bahrain's. Under Qatar's law, the consent of data subjects must be obtained by a data controller before their data can be collected and processed. Article 19 grants broad exceptions to the requirement of consent to government bodies. The competent authority is not required to first obtain consent to processing from data subjects for any purposes related to protecting national and public security, protecting the international relations of the date, protecting the financial interests of the state, or to prevent criminal offenses.

Furthermore, data subjects are also granted the right to request access to their data in Qatar. Controllers are allowed to reject such a request and are not required to provide the individual with an explanation of this rejection on the basis of protecting national and public security, protecting the international relations of the date, protecting the financial interests of the state, or to prevent criminal offenses.

The UAE's Health Data Law, the Dubai International Financial Centre Data Protection Law, and the Abu Dhabi Global Market Data Protection Law are mostly free of any far-reaching exceptions relating to national security. However, there is one small article of note located within the data protection law established within the Dubai International Financial Centre. The law grants data subjects the right to access their personal data. Article 33 allows controllers to restrict this access in order to protect public security, national security or the rights of others. This exception, however, must only be enacted if necessary and proportionate and with respect to the fundamental rights and legitimate interests of the individual.

It is important to remember that Kuwait does not currently have any national level data protection framework and therefore the legal basis upon which state and non-state entities can access and process data are not yet delineated. There are no limits on access, rights of data subjects or legal obligations for data controllers and processors.

Data Laws And Contact Tracing

As the outbreak of COVID-19 grew throughout the spring of 2020, the private sector and governments alike promoted various new technologies to fight the pandemic. While

technology optimists argued that a 21st century pandemic required 21st century solutions, skeptics warned about the potential for abuse these technologies posed, particularly during a period of extreme uncertainty. Critics warned that, without adequate safeguards, the widespread deployment of new technologies to fight the pandemic could have far reaching repercussions for our post-pandemic world, leading to increased state surveillance.

To assess whether newly deployed contact tracing applications are striking an appropriate balance between surveillance in the service of public health and protection of user privacy, the legal and policy frameworks of these apps have been examined. Their deployment and use has also been documented. While the technical specifications and policy guidelines for the apps are not uniform across these jurisdictions, certain privacy concerns are consistent throughout.

Shared Concerns

The apps surveyed in these jurisdictions lack a limited purpose and clear timelines on their deployment and use. There is also a notable lack of transparency in both their technical design and regulatory mechanisms.

> “ There is a notable lack of transparency around the policies and regulations of the use of these apps. ”

International standards on the use of COVID 19 contact tracing applications universally hold that apps must be deployed with guidelines designating a clear and limited purpose. Apps should not be deployed without clear guidelines determining how long they will be in use, what epidemiological conditions must be present to warrant their deployment, and a clear exit strategy detailing how this technology will be phased out and when their affiliated data will be deleted. None of the jurisdictions surveyed issued clear guidelines on the limited purpose and use of the applications. Qatar, Bahrain, the UAE and Kuwait did not issue defined timelines about how long citizens will be expected to use their respective apps or under what conditions the apps and their tracking programs will end. This is particularly troublesome in Qatar, where the app is mandatory.

There was also a notable lack of transparency in both the technical design of the apps and their policies for use across these jurisdictions. The source code for the apps was not available openly for any of the jurisdictions surveyed, making it difficult for security researchers and other developers to assess the app’s functionalities. Because the code is not published and open source, observers are forced to rely on statements released by government ministries about how the app functions and whether it adheres to privacy by design principles. Rather than relying on trust, citizens have the right to verify these claims.

Similarly, there is also a notable lack of transparency around the policies and regulations of the use of these apps. The rights of data subjects and rules concerning the collection, processing, retention and deletion of data are completely opaque in every jurisdiction surveyed. While some states voluntarily provided information about how the app operates, citizens are relying solely on trust that this information is accurate. Instead, states should guarantee mandatory data deletion times and other important policy components via the passage of primary legislation governing the deployment and use of the apps.

Bahrain and Kuwait did not issue specific privacy policies governing the apps, but instead relied on generic privacy policies pre-issued for any data related to their respective ministries of ICT.

Do Robust Data Laws Indicate Privacy Preserving Apps?

In assessing both the data protection legal framework across these jurisdiction and the deployment of their own contact tracing apps, one important question was whether or not the existence of a strong privacy legal framework indicates a privacy preserving app: Is there a relationship between a robust legal framework and privacy preserving COVID19 contact tracing application? Ultimately, the strength of a state’s data protection legal framework in most cases is a reliable indicator of how privacy conscious their contact tracing app. The more robust a state’s privacy legal framework is, the more privacy preserving their app has proven to be.

For example, the UAE’s data protection legal framework is relatively robust, compared to the other states studied for this report. While they do not currently have a national level data protection law, their subnational laws strongly resemble the EU’s GDPR. The UAE’s national contact tracing app, AlHosn, is also one of the most privacy preserving applications surveyed in this study. While the code is not open source, it has by far the most technical information available on how the app itself actually works.

Despite the robustness of the UAE's subnational data protection laws, the UAE has a documented history of state-backed privacy violations. Other jurisdictions surveyed have also been implicated in state-sponsored digital attacks violating privacy. This, combined with the notable lack of evidence failing to demonstrate broad enforcement of data protection laws, further brings into question whether these laws exist on paper only. If there is evidence demonstrating that states themselves do not respect their own data protection and privacy legal framework, it is difficult to use the letter of these laws to evaluate a genuine commitment to data protection and privacy principles.

States with laws that have large exemptions for security bodies, like Bahrain, also have less privacy conscious apps. Similarly, Kuwait is the one state surveyed that does not have a data protection law and its app is arguably the most privacy invasive of the five jurisdictions included in this report. Therefore, it seems the existence of a robust and thorough data protection and privacy legal regime is a likely indicator of the respective states adherence to international norms surrounding the development of COVID-19 contact tracing apps. The greater degree of similarity of a state's data protection frameworks with international standards like the GDPR, the greater the likelihood of a state's COVID-19 contact tracing apps compliance with international standards.