accessnow.org

EXPOSED AND EXPLOITED: DATA PROTECTION IN THE MIDDLE EAST AND NORTH AFRICA

accessnow

Access Now defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions, and convenings such as RightsCon, we fight for human rights in the digital age.

Exposed and Exploited: Data Protection in the Middle East and North Africa

January 2021

TABLE OF CONTENTS

This report is a publication of Access Now and was written by Marwa Fatafta and Dima Samaro with the collaboration of Rima Sghaier who conducted research into the case studies. The authors would like to especially thank Arab Advancement for Social Media (7amleh), Social Media Exchange (SMEX), Jordan Open Source Association (JOSA), Reem Al-Masri, Rima Sghaier, Sage Cheng, Donna Wentworth, and the Access Now policy team for their contributions.

CONTACT

For more information about this report, please contact:

Marwa Fatafta (marwa@accessnow.org)
Dima Samaro (dima@accessnow.org)

Access Now (https://www.accessnow.org) defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions, and convenings such as RightsCon, we fight for human rights in the digital age.

I. EXECUTIVE SUMMARY

The year 2020 has witnessed governments respond to the global COVID-19 crisis by rushing to deploy technological solutions, from contact tracing applications to digital health certificates and passports. The pandemic has brought to center stage the significant threats new technologies can pose for human rights, underscoring the critical need for governments to prioritize the adoption of robust privacy safeguards and data protection legal frameworks for citizens' personal data.

Across the Middle East and North Africa (MENA), data protection legislation is still in its infancy, and it remains a low priority in countries where data protection laws are either very weak or non-existent. Nevertheless, governments have been quick to introduce proposals for use of technology that are data-heavy, such as national digital identity programs, biometric passports, and e-health services, disregarding how technology can be used to infringe citizens' privacy or exploit their personal data. Where data protection laws do exist, enforcement is problematic. National security agencies often enjoy unrestricted access to citizens' personal data, and private companies exploit and sell this information for profit without users' knowledge or consent.

Access Now is committed to protecting human rights and to advancing the global, regional, and local agendas on privacy and data protection. In this report, we highlight how privacy and data protection violations by state and non-state actors are compounded by the lack of legal data protection safeguards which would obligate public entities, private companies, and international organizations to respect and adhere to data protection principles, empower users to take agency and control over their personal information, and create mechanisms for grievance and redress when such violations occur.

We explore these issues and propose safeguards and policy recommendations for those involved in the collection and processing of personal data: governments, private companies, and international aid organizations. We include case studies for **Jordan**, **Lebanon**, **Palestine,** and **Tunisia**. Our goal is not to include an exhaustive list of all cases related to data protection, but to present a few key illustrative cases for each country. We have only scratched the surface here, and we welcome further input, examples, and investigations by citizens, activists, journalists, and civil society organizations.

II. INTRODUCTION

A woman in Beirut was driving while trying to ignore a man who was pestering her from his car. A few minutes later, she received a phone call from him. Before she hung up, the man informed her that he knows her home address. Where did he get this information from? Her license plate number. In 2014 in Lebanon, anyone could get access to your name, home address, phone number, and other personal data, such as your blood type, just by punching your car's license plate number into a mobile app.[1]

Similarly scary stories of intrusion into our private lives and personal information are unfortunately common in many parts of the Middle East and North Africa region. From the telecom company Orange dumping a pile of 1,500 service contracts, including IDs and copies of Tunisian citizens' passports, on the side of the street,[2] to people using same-sex dating apps to out and expose the sexual orientation of LGBTQ+ people in Morocco during the pandemic lockdown, circulating their photos on social media platforms without their consent,[3] there are countless examples of internet users in the region being exposed to violation of their privacy online — and in some cases, subsequently to physical harm and other rights violations offline without protection or access to remedy.

The right to privacy, connected to the right to data protection, is a fundamental human right. However, as we note above, as governments in the region rush to adopt new technologies that collect and process the personal data of millions of their citizens — such as digital IDs, biometric e-passports and driving licenses, or e-government services — they are failing to make protection of citizens' data a priority. Instead, national legislators and policy makers are heading in the opposite direction, adopting repressive legislation and policies, including cybercrime bills and anti-terrorism laws, that attempt to criminalize freedom of expression online and turn the internet into a heavily monitored and surveilled space.

In 2012, the United Nations Economic and Social Commission for Western Asia (ESCWA) issued a number of cyber legislation directives, including a directive on personal data protection, in an attempt to harmonize cyber legislation in the Arab World.[4] The directive on data protection was heavily based on the European Union's 1995 Data Protection Directive, the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the

[1] Najem, M. (2014, May 15). *In Lebanon, Apps Let You Get Someone Else's Personal Info With Ease*. Retrieved January 08, 2021, from https://slate.com/technology/2014/05/in-lebanon-apps-let-you-get-someone-else-s-personal-info-with-ease.html
[2] Dima Samaro, & Emna Sayadi. (2018, November 06). *Tunisia: Orange Telecom violates customers' right to privacy* (in Arabic). Retrieved January 08, 2021, from https://www.accessnow.org/%D8%AA%D9%88%D9%86%D8%B3-%D9%81%D8%B6%D9%8A%D8%AD%D8%A9-%D8%B4%D8%B1%D9%83%D8%A9-%D8%A3%D9%88%D8%B1%D9%88%D9%86%D8%AC-%D9%84%D9%84%D8%A5%D8%AA%D8%B5%D8%A7%D9%84%D8%A7%D8%AA%D8%8C-%D8%A7%D9%84%D8%A5/
[3] Human Rights Watch. (2020, October 28). *Morocco: Online Attacks Over Same-Sex Relations.* Retrieved January 08, 2021, from https://www.hrw.org/news/2020/04/27/morocco-online-attacks-over-same-sex-relations
[4] ESCWA. (2017, March 08). *Regional Harmonization of Cyber Legislation to Promote the Knowledge Society in the Arab World.* Retrieved January 08, 2021, from https://www.unescwa.org/publications/brochure-cyberlegislation-arab-world

processing of personal data and on the free movement of such data ("Directive 95/46/EC"). It also adopted the Organization for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980).

The ESCWA data protection directive was ambitious in putting forward key principles that would grant individuals and data subjects the right to consent to collecting, processing, and sharing their personal data, instituting obligations for data collectors and processors, and setting up independent oversight data protection authorities, among other aspects.

Unfortunately, the existing legislative and regulatory frameworks in the region remain lacking. Less than half of the 22 Arab countries have adopted national data protection laws, and the countries that do have such law in place — such as Tunisia, Lebanon, and Morocco — have weak, outdated frameworks and face serious challenges in enforcing and implementing the law. As a result, the personal data of millions of citizens is left subject to continuous exploitation by private companies for profit, and by governments for surveillance and suppression of free speech and political dissent in the name of fighting terrorism and crime or preserving national security.

Even worse, it appears that in some cases the driving motivation behind proposals for national data protection legislation is not to protect citizens' fundamental rights but to open the door for financial investment in the big data industry.

In this report, we aim to provide an overview of the current status of data protection in the MENA region by shedding light on the situation in four countries: Jordan, Lebanon, Palestine, and Tunisia. For each country, we analyze the existing regulatory and legal framework on privacy and data protection.

We also investigate recent cases of data breaches and privacy violations by governments and private companies in those countries. It is tremendously difficult to get the information necessary to determine how people's data are being collected and processed across the region. Given the lack of transparency and access to information in many MENA countries, journalists, activists, and civil society organizations like us struggle to do our jobs. Even when a country has access to information laws, our requests for information are often ignored. Such was the case when we asked the Tunisian Ministry of Health for information about the contact tracing mobile app the government deployed in June 2020.[5]

Adding to the complexity of the issue, many internet users in the region have become apathetic about online privacy and data protection legislation. As research by the Social Media Exchange (SMEX) shows, many people are convinced they are being constantly monitored by their governments and are

[5] Access Now. (2020, September 17). *To safeguard privacy, Tunisia must be transparent on tech used to fight COVID-19.* Retrieved January 22, 2021, from https://www.accessnow.org/to-safeguard-privacy-tunisia-must-be-transparent-on-tech-used-to-fight-covid-19/

resigned to that reality or conviction, while others believe there are far more egregious human rights violations that should be addressed, as well as larger social and political problems to tackle, such as corruption, poverty, and unemployment.[6]

It is important to emphasize that the MENA region is not monolithic, and the threats and risks individuals and groups face are shaped by the specific political, legal, social, and cultural contexts in which they live. The alarming examples of already vulnerable communities exposed to further risks and harm span from the mass collection of biometric data, such as iris scans and fingerprints, of 2.5 million refugees, to the invasion of online privacy for women and LGBTQ+ people, to the gay men in Morocco who were "outed" on social media and made the target of vicious online attacks, ostracized by their families, and kicked out of their homes in the middle of a pandemic. In these cases and many others, privacy and data protection are vital for safety.

At Access Now, we urge governments to adopt robust and effective laws and policies to protect people's personal data and information online, and urge private companies to uphold their responsibility to respect human rights instead of profiting off human rights violations.

III. DATA PROTECTION IN THE MENA REGION

JORDAN

1. Legal framework for privacy and data protection

Like many other local jurisdictions in the MENA region, Jordan does not have a strict data protection law in place to properly protect and promote the right to privacy. However, in 2014, the Ministry of the Digital Economy and Entrepreneurship (formerly known as the Ministry of Communications and Information Technology) introduced a draft law on the protection of personal data. Following a year and a half of public consultations with private and public stakeholders, the fifth and final draft is still in progress to date.

This initial proposal was followed by the formation of a committee to discuss the legislation, which involved the Ministry of Interior, the Ministry of Labor, the Ministry of Communications, the Telecommunications Regulatory Commission (TRC), the Central Bank, and the Information and Communications Association of Jordan. Civil society and human rights groups have been less involved in these parallel discussions, and their participation has been limited to providing comments on the draft legislation through the ICT Ministry's public consultations.

[6] SMEX. (2020, January 16). *A Snapshot of Digital Rights Coverage in the MENA Region.* Retrieved January 08, 2021, from https://smex.org/a-snapshot-of-digital-rights-coverage-in-the-mena-region/

In 2018, the ICT Ministry proposed the fourth revised version of the text to be compatible with the European Union's General Data Protection Regulation (GDPR).[7] Indeed, at first glance, the draft personal data protection bill seems to embrace key principles of the GDPR, such as transparency, accuracy, storage limitation, and data minimization. The draft also extends the application of the law to all private and public institutions in Jordan, including locally registered international agencies and organizations.

Yet in its current form, the bill raises significant concerns, particularly with regard to the proposed structure and setup of the future data protection authority. For example, Article 4 of the draft law proposes that the Data Protection Commission be chaired by the ICT Minister, which would undermine its independence and autonomy as an oversight body. As 7iber notes, this would constitute a structural conflict of interest, since the ICT Ministry "has a great interest in developing the tech sector, representing companies whose interests are to collect the largest amount of personal data and not necessarily protect the rights of the data owners."[8] The Commission would also include two members of the security forces to formulate and approve policies and strategies related to the protection of personal data, among other duties. It is doubtful that the data protection authority in its currently proposed structure would be able to investigate complaints on privacy violations if committed by the executive branch.

Furthermore, the draft law also contains broad and vague language that would permit the processing of personal data without obtaining prior approval if necessary for "security purposes" or the "public interest" (Article 15).[9] This is alarming given the fact that government agencies deal with large amounts of data, and should not be exempt from the requirement to get explicit consent before collecting or sharing people's personal data among its various offices. At minimum, core data protection rights, including the right to information and to redress, should apply. Without the appropriate safeguards, the current proposal violates the core principle and purpose of privacy legislation, which seeks to safeguard citizens' personal data from any potential infringements.

It is still unclear when the Jordanian parliament intends to pass this legislation. In the meantime, other laws and provisions that are linked to the right to privacy in Jordan include:

- **The Constitution:** While the right to privacy is guaranteed in the Constitution under Article 18, the 2011 constitutional amendments allow surveillance of private communications where judicial approval was granted, as a precondition for censorship, confiscation, or viewing of private communications.[10]

[7] Jordanzad. (2020, January 15). *Data Protection Draft law in Jordan* (in Arabic). Retrieved January 08, 2021, from http://www.jordanzad.com/index.php?page=article&id=360987
[8] 7iber. (2017, September 13). *Data Protection Law: A Call to Defend the Protection of Our Right to Privacy.* Retrieved January 08, 2021, from https://www.7iber.com/technology/data-protection-law-invitation-to-protect-our-privacy/
[9] *Ibid*.
[10] Constitute project. *Jordan's Constitution of 1952 with Amendments through 2016.* Retrieved January 08, 2021, from https://www.constituteproject.org/constitution/Jordan_2016.pdf?lang=en

- **Cybercrime draft law:** In December 2018, the government proposed amendments to the Cybercrime Law, which has since been withdrawn. The proposed amendments added the term "applications" to the definition of an "information system," which means that smart phone apps would be subject to mass surveillance. In addition, Articles 11 and 13 of the withdrawn law penalize defamation online and give the government the power to confiscate, suspend, and search personal computers and information systems, thereby violating individuals' right to privacy.[11]
- **Telecommunications Law No. 13/1995:** Article 56 states that "telephone calls and private communications are confidential matters that may not be violated, under legal liability." Although the legislation applies to the conventional means of communication, there is no clear reference to digital and online communications. The Telecommunication Law also allows communication to be monitored in accordance with a judicial or an administrative request. Article 29 of the law stipulates that "the licensee should commit to provide the necessary facilities to the competent authorities for the implementation of court and administrative orders that have to do with tracking communications specified in these orders."[12]
- **Penal Code:** While the Penal Code penalizes the dissemination of private messages by up to three months in prison, the Telecommunication Law's penalty for unauthorized surveillance ranges between a month and a year in prison, or a 100 to 300 dinar fine. Article 356 of Penal Code stipulates: "Anybody who spreads the content of a private call within the capacities of his position in the telephony service will be penalized for six months or charged with 20 JOD." In addition, Article 384 states: "Responding to the complaint of the victim, one is penalized for not more than three months in jail for breaching the private lives of others by eavesdropping, or surveillance through any other medium including recording audio. The penalty is multiplied in case of repetition." It should be noted that these penalties are only enforced on individuals whose duty is to transfer calls, while security institutions are exempted from such charges.[13]
- **Anti-Terrorism Law No.55/ 2006:** Article 4 states that "an individual may be subject to surveillance if the public prosecutor receives reliable information indicating that a person or a group of persons has ties to any terrorist activity." It's worth noting that vague concepts such as "reliable information" and "terrorist activity" are not defined in the law.[14]

---

[11] Dima Samaro, & Emna Sayadi. (2019, February 20). *Cybercrime law in Jordan: Pushing back on new amendments that could harm free expression and violate privacy.* Retrieved January 08, 2021, from https://www.accessnow.org/cybercrime-law-in-jordan-pushing-back-on-new-amendments-that-could-harm-free-expression-and-violate-privacy/

[12] *Communications Law and its amendments No. 13 of 1995.* Retrieved January 08, 2021, from https://www.wipo.int/edocs/lexdocs/laws/ar/jo/jo056ar.pdf

[13] *Penal Code of Jordan (No. 16 of 1960).* Retrieved January 08, 2021, from https://www.ilo.org/dyn/natlex/natlex4.detail?p_lang=en&p_isn=79914&p_country=JOR&p_count=179&p_classification=01.04&p_classcount=6

[14] CYRILLA. *Anti-Terrorism Law (No.55 of 2006)*. Retrieved January 08, 2021, from https://cyrilla.org/en/entity/xc3gtsd647yr0iepk3o50cnmi?searchTerm=anti+jordan++

- **Credit Information Law No.15/2010:** Article 8 of the law states that the written consent of the consumer must be explicitly obtained prior to the disclosure of information about the consumer's credit status. However, the same article stipulates that "a company may reveal information about the customer if the entity requesting information is a bank or an insurance company or any other party approved by the governor." Article 18 allows the exchange of information between licensed companies with the approval of the governor.[15]
- **Access to Information Law:** Article 13 of the law states that "information on correspondence between government entities and other parties shall not be disclosed regardless of the means of communication." Apart from correspondence between government agencies, it is not clear if correspondence between citizens can be disclosed or not.[16]

In the absence of adequate data protection and proper safeguards for personal information, Jordanians will continue to confront threats to their right to privacy. This was acknowledged in November 2018 during the 31st session of the United Nations Human Rights Council's Universal Periodic Review (UPR), where Jordan received for the first time in its history two recommendations from Estonia and Brazil on respecting the right to privacy.[17] The Jordan Open Source Association (JOSA) previously recommended at the UPR that "online surveillance by the Jordanian government should be conducted in respect of human rights and the right to privacy to comply with the constitution and international human rights standards."[18]

Reforming Jordan's legal framework on privacy and data protection is of paramount importance, especially in light of the government's digitization of services and documents. In 2016, the Ministry of Interior and the Ministry of ICT introduced a mandatory smart national ID card to replace the old national identification documents and integrate more information about the holder.[19] The new card includes a chip (144 KB) to store biometric data including the iris scan and fingerprints of the ID holder as well as name, gender, place of birth, area of residence, and blood type. In later stages, the national ID card would include more information on health insurance, social security number,

[15] 7iber. *Credit Information Law (No.15 of 2010)*. Retrieved January 08, 2021, from https://www.7iber.com/wp-content/uploads/2016/06/%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA-%D8%A7%D9%84%D8%A7%D9%8A%D9%94%D8%AA%D9%85%D8%A7%D9%86%D9%8A%D8%A9.pdf

[16] CYRILLA. *Law on Securing the Right to Information Access (No 47 of 2007)*. Retrieved January 08, 2021, from https://cyrilla.org/en/entity/si4p74r2ylf2jfiequcqy3nmi?searchTerm=access+to+info

[17] OHCHR. *Universal Periodic Review - Jordan.* Retrieved January 08, 2021, from https://www.ohchr.org/EN/HRBodies/UPR/Pages/JOindex.aspx

[18] JOSA. (2020, July 13). *Co-submission to the Universal Periodic Review 31st Session — Jordan on the Right to Privacy.* Retrieved January 08, 2021, from https://jordanopensource.org/publications/1/cosubmission-to-the-universal-periodic-review-31st-session--jordan-on-the-right-to-privacy

[19] e-Government. *The Hashemite Kingdom of Jordan, Smart Card* (in Arabic). Retrieved January 08, 2021, from https://portal.jordan.gov.jo/wps/portal/Home/SmartCard?lang=ar&isFromLangChange=yes

citizens' electronic signature, voting activities, and more.[20]

Two years later, the Telecommunication Regulatory Commission announced that it will develop new rules that require new owners of SIM cards to submit their fingerprints to authenticate their numbers.[21] As noted previously, the lack of sufficient and adequate data protection legislation in place raises concerns regarding security and lack of transparency in processing such sensitive personal data.

2. Case studies

1) Abuse of personal data by Jordanian ISPs and telcos

In 2019, Access Now published a report with ImpACT International for Human Rights Policies highlighting how the five existing Internet Service Providers (ISPs) in Jordan — Zain, Orange, Umniah, TE Data, and Damamax — routinely collect the personal data of their subscribers without notifying them or disclosing how their data are being used and shared by these companies.[22] Only Orange responded to the report's findings, solely to reiterate "its full compliance with all legal and contractual requirements for customers' information privacy,"[23] without adequately addressing any of the questions and concerns we raised in our report.

The Telecommunications Regulatory Commission, on the other hand, affirmed in a public statement that it will investigate and take all necessary measures against privacy violations of telecommunications consumers in Jordan.[24] Despite these assurances, there has been no evidence of enforcing the Telecommunications Law (No. 13 of 1995) against the privacy abuses of ISPs.

According to Reem Al Masri, a researcher and tech journalist at the independent Jordanian media organization 7iber, the poor privacy policies of Jordanian telecom companies force "users [to]

[20] Thales group. *Jordan launches its new national ID card program.* Retrieved January 08, 2021, from https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/national-id-card-jordan

[21] Privacy International. (2019, June 11). *Timeline of SIM Card Registration Laws.* Retrieved January 08, 2021, from https://privacyinternational.org/long-read/3018/timeline-sim-card-registration-laws

[22] Dima Samaro. (2019, December 03). *New study: Jordanian ISPs violate customers' privacy.* Retrieved January 08, 2021, from https://www.accessnow.org/new-study-jordanian-isps-violate-customers-privacy/

[23] Business & Human Rights Resource Centre. (2019, December 9). *Orange responds to ImpACT International for Human Rights Policies and Access Now report.* Retrieved January 08, 2021, from https://www.business-humanrights.org/en/latest-news/orange-responds-to-impact-international-for-human-rights-policies-and-access-now-report/

[24] Telecommunications Regulatory Authority. (2019, November 13). *Confirmation of actions against any breach of customers' privacy* (in Arabic). Retrieved January 08, 2021, from https://www.almamlakatv.com/news/%D8%AA%D8%A3%D9%83%D9%8A%D8%AF-%D8%B9%D9%84%D9%89-%D8%A5%D8%AC%D8%B1%D8%A7%D8%A1%D8%A7%D8%AA-%D8%B6%D8%AF-%D8%A3%D9%8A-%D8%A7%D9%86%D8%AA%D9%87%D8%A7%D9%83-%D9%84%D8%AE%D8%B5%D9%88%D8%B5%D9%8A%D8%A9-%D8%A7%D9%84%D9%85%D8%B4%D8%AA%D8%B1%D9%83%D9%8A%D9%86-29064

basically agree to have their data shared with third-parties and not to be notified every time their data is shared." For example, one source in Jordan informed us that they were able to buy in 2019 a service from the telecom company Umniah which allows them to send promotional short message service (SMS) messages to clients in a selected city in Jordan. Unfortunately, some users believe that this practice is legitimate as it has become so customary, according to our source: "the company owns our phone numbers and by default we accept to receive advertisement. If we want to opt out, we can call the company."

The usual and obvious clientele of telecom subscribers' data are advertising agencies and private businesses, who want to promote certain products or services, or want to announce special offers or the seasonal sales. In some cases, however, these data are exploited for political purposes. During the trade union protests in 2018, citizens in Jordan received an SMS message the night before a planned protest. The message, sent from an unknown number, implicitly discouraged them from protesting. It is still not clear who sent the text, but the indications suggest users' phone numbers were shared with a third party, most probably one aligned with the Jordanian government.

Figure 1. *Screenshot of SMS received by citizens in Jordan in June 2018.*[25]

Translation: "Tonight is a test for the love of our homeland and appreciation for those who left their families to protect the homeland. #Think right"

2) Collection of refugees' biometric data by international organizations

Jordan was the first country in the world to use iris scan technology for humanitarian aid.[26] In 2016, the World Food Program (WFP), in partnership with the UN High Commissioner for Refugees (UNHCR), introduced an iris scan payment technology in Zaatari and Azraq refugee camps in Jordan, then

[25] Courtesy of Reem Al Masri.
[26] Privacy International. (2019, January 26). *State of Privacy Jordan.* Retrieved January 08, 2021, from https://privacyinternational.org/state-privacy/1004/state-privacy-jordan

expanded scanning to other camps and mobile centers, as part of program to allow refugees to buy groceries from stores.[27]

The WFP system relies on UNHCR's biometric refugee registration database, named EyeBank,[28] where iris scans are used first by UNHCR to register refugees over the age of three, and later for verifying their identity.[29] When a refugee shops for a bag of rice, for example, rather than handing over cash, they can have their iris scanned at the cashier, which authenticates their identity and deducts payment from their linked bank account. The WFP has piloted the iris scan payment technology in 206 merchant locations in Jordan.[30]

The same process is used for cash payments. Refugees can withdraw cash from iris-enabled ATM machines in urban areas in Jordan.[31] The iris scan technology is provided by a private company called IrisGuard, and it's used for authentication and payment in a number of cash assistance frameworks. In one framework, the Common Cash Facility (CCF), which is based on a public-private partnership between Cairo Amman Bank (CAB), UNHCR, and IrisGuard, different humanitarian organizations and government agencies can send their funds to refugees via subwallets linked to the UNHCR ID database.[32] As of 2018, CCF had 22 members, including UNHCR, UNICEF, Action Contre la Faim, ACTED, Medair, PU-AMI, World Relief Germany, Save the Children, and Danish Refugee Council.[33]

IrisGuard is registered in the UK.[34] It was co-founded by Imad Malhas who used the iris-scan technology "EyeHood" in 2001 for the first time in the United Arab Emirates to identify illegal immigrants so they could be deported,[35] and by Karim Kawar, one of Jordan's wealthy businessmen and former ambassador to the US and Mexico.[36] IrisGuard's advisory board used to include two former foreign intelligence officials: Frances Townsend, a US National Security advisor to former US President George W. Bush during the invasion of Iraq,[37] and Richard Dearlove, who was the head of UK spy

---

[27] World Food Program (WFP). (2016, October 6). *WFP Introduces Iris Scan Technology To Provide Food Assistance To Syrian Refugees In Zaatari.* Retrieved January 08, 2021, from https://www.wfp.org/news/wfp-introduces-innovative-iris-scan-technology-provide-food-assistance-syrian-refu

[28] IrisGuard. *Refugee Cash Assistance.* Retrieved January 08, 2021, from https://www.irisguard.com/where-we-work/humanitarian-assistance/refugee-cash-assistance/

[29] Die Zeit.(2017,December 17). *Iris Scan Technology Tested on millions of Non-volunteers.* (English translation published on UNHCR blog). Retrieved January 08, 2021, from https://www.unhcr.org/blogs/wp-content/uploads/sites/48/2018/01/article_1.pdf

[30] CGAP and World Bank Group. (2020, April). *Humanitarian Cash Transfers and Financial Inclusion: Lessons from Jordan and Lebanon.* Retrieved January 08, 2021, from http://documents1.worldbank.org/curated/en/974621587749884009/pdf/Humanitarian-Cash-Transfers-and-Financial-Inclusion-Lessons-from-Jordan-and-Lebanon.pdf

[31] *See Supra* note 18.

[32] *See Supra* note 19.

[33] *Ibid*.

[34] IrisGuard. Retrieved January 08, 2021, from https://www.irisguard.com/

[35] *See Supra* note 18.

[36] *See Supra* note 19.

[37] Frances Fragos Townsend short biography. (2018, February 12). Retrieved January 08, 2021, from https://network2020.org/past-benefits/frances-fragos-townsend/

agency MI6.[38]

The technology provided by IrisGuard — dubbed "EyePay" — is closed source, so we don't know how it works, how secure it is, and to what extent it guarantees privacy and protection for the refugees' biometric and sensitive personal data. According to IrisGuard's website, "EyePay" uses blockchain technology in what the WFP calls the "Building Blocks" project, through the integration of Ethereum cryptocurrency.[39]

IrisGuard's business model appears to be based on a percentage of the transaction charge. According to a World Bank report, in the framework of the CCF, IrisGuard takes 15% of each transaction charge as an authentication fee, paid by Cairo Amman Bank. Transaction charges in Jordan range from 1.15 to 1.32 % of the transfer amount.[40]

The company states on its website that the UNHCR has "successfully and effortlessly" enrolled over 2.5 million Syrian refugees displaced in Jordan, Lebanon, Iraq, Egypt, Syria, and Turkey using its technology.[41] It is unclear if all the UNHCR-registered refugees in Jordan (751,901 as of October 31, 2020) have been enrolled using the technology.[42]

This is alarming. The use of biometric technology has serious human rights implications, and poses grave dangers to an already severely vulnerable community. As we explain in our paper on digital identity,[43] biometric identifiers such as fingerprints, DNA, or iris and retina patterns, are sensitive personal data, and if the information is compromised or breached, the damage is irreparable. In the words of IrisGuard's co-founder, Malhas: "A person's iris does not change from age three until death… anyone who has been scanned can be perfectly identified at the age of 100 on the basis of their biometric characteristics." This makes iris-based authentication a highly invasive form of authentication, and governments and organizations must therefore engage in serious data protection and cybersecurity considerations, before rolling out these systems. Given the significant risks they pose, these systems require a much higher threshold of justification than other alternatives. Proponents of such invasive biometric ID systems typically argue that they advance more efficient and accurate delivery of services or aid, reduce corruption, prevent fraud, and promote more

[38] Richard Dearlove biography. Retrieved January 08, 2021, from http://investors.kosmosenergy.com/board-member/sir-richard-dearlove
[39] World Food Program (WFP). *Building Blocks Blockchain for Zero Hunger.* Project webpage. Retrieved January 08, 2021, from https://innovation.wfp.org/project/building-blocks
[40] *See Supra* note 19.
[41] *Ibid*.
[42] UNHCR. *Operational Portal: Sum based on data from the official public UNHCR database.* Retrieved January 08, 2021, from https://data2.unhcr.org/en/situations
[43] Access Now. (2019, November). *National Digital Identity Programmes: What's Next?* Retrieved January 08, 2021, from https://www.accessnow.org/accessnow-digital-id-paper

accountability. However, implementing iris authentication to "[reshape] the shopping experience"[44] for Syrian refugees invades privacy for an aim that is neither necessary nor proportionate.[45]

Furthermore, the use of this technology for humanitarian assistance constitutes a form of implicit coercion and negates one of the foundational principles of data protection: an individual's agency and consent. As E. Tendayi Achiume, the UN Special Rapporteur on racism, racial discrimination, xenophobia and related intolerance, notes in her thematic report on emerging digital technologies in border and immigration enforcement, "conditioning food access on data collection removes any semblance of choice or autonomy on the part of refugees — consent cannot freely be given where the alternative is starvation."[46] It's worth noting here that half of the refugees arriving in Jordan are under the age of 18, and the UNHCR is reported to scan children over the age of three.[47]

Another major concern is the lack of transparency by both UNHCR and WFP. There is no publicly available information on the selection and procurement of IrisGuard, if and how they obtain consent from refugees, if they share these data with third parties or local government agencies, how the data are stored, and what technical and legal safeguards are in place to protect this massive amount of sensitive data. Access Now sent a letter to UNHCR and WFP Jordan offices to request more information regarding these concerns.[48]

3) Government requests for access to users' data collected via ride-sharing apps

The local digital rights NGO Jordan Open Society Association (JOSA) has raised the alarm regarding a recent amendment to the regulation published by the Ministry of Transportation in May 2018 for licensing ride-calling apps, including Uber and Careem.[49] The regulation obligates these companies to share their users' personal data, their trip details, and geolocation, and the new amendment further permits judicial and security agencies to have direct access to the companies' servers and databases, which may facilitate mass surveillance of Jordanian citizens.[50] As noted by JOSA, "processing this data may constitute a violation of the citizens' right to privacy in light of the absence of any conditions in

[44] *See Supra* note 16.
[45] ARTICLE 19 and Electronic Frontier Foundation (EFF). (2014, May). *Necessary & Proportionate International Principles on the Application of Human Rights Law to Communications Surveillance.* Retrieved January 25, 2021, from https://www.ohchr.org/documents/issues/privacy/electronicfrontierfoundation.pdf
[46] OHCHR. *Report of Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, A/75/590, 2020.* Retrieved January 08, 2021, from https://www.ohchr.org/EN/newyork/Documents/A-75-590-AUV.docx
[47] *See the aforementioned Die Zeit report, supra* note 18.
[48] Access Now. (21 October, 2020). *Letter to UNHCR and WFP Re: Collection of biometric data in refugee camps in Jordan.* Retrieved January 08, 2021, from https://www.accessnow.org/cms/assets/uploads/2020/11/Access-Now-Letter-to-UNHCR-and-WFP-on-Jordan.pdf
[49] Jordan Open Source. *Regulation on Passenger through the use of smart apps (2018)* (in Arabic). Retrieved January 08, 2021, from https://opinions.jordanopensource.org/wp-content/uploads/2018/05/d0001075.pdf
[50] Anbat news. (2020). *JOSA: "Amending the regulations for transport apps allows for collective surveillance of passengers"* (in Arabic). Retrieved January 08, 2021, from https://alanbatnews.net/article/197268

the law in relation to the processing of that data by the (Land Transport) authority, and there are no restrictions on the transfer of data from the authority to other bodies."[51]

LEBANON

1. Legal framework for privacy and data protection

The Lebanese Constitution does not explicitly guarantee the right to privacy. Article 14 stipulates that "the dwelling is inviolable" and provides protection only to the citizen's place of residence.[52] However, one legal interpretation argues that Article 8, which guarantees individual liberty, and Article 13, which guarantees freedom of expression, indirectly guarantee individuals the right to privacy and the secrecy of all communications, including phone and mail.[53]

Lebanon adopted a data protection law, Law No. 81 Relating to Electronic Transactions and Personal Data (E-Transactions Law), in 2018. Even though the draft of the law went through many rounds since it was first introduced in 2004, the updated and adopted draft failed to reflect the evolution of the internet or address the privacy and data protection associated with the emergence of new technologies.

Many of the provisions are vague and ambiguous. For example, the law does not define what consent is for data subjects, and it prohibits individuals from withdrawing their consent to collect and process their personal data once it was previously given, or if "the data-processing officer is obliged to collect the data under the law."[54]

The law does not place any time limits on data retention, nor does it acknowledge or regulate the processing of sensitive personal data such as biometric information. Instead, it provides only a list of exemptions when a license for collecting and processing data is not required. Additionally, the law fails to grant individuals the right to be notified in case there is a breach of privacy, and most worryingly, individuals do not have the right to know how their personal data are being processed for purposes related to national security.[55]

[51] Interview with Jordan Open Society Association (JOSA), 2020.
[52] The Constitute Project. *Lebanon's Constitution of 1926 with Amendments through 2004.* Retrieved January 08, 2021, from https://www.constituteproject.org/constitution/Lebanon_2004.pdf?lang=en
[53] Privacy International. SMEX, and the Association for Progressive Communication. (2015, March). *Universal Periodic Review Stakeholder Report: 23rd Session, Lebanon*. Retrieved January 10, 2021, from https://privacyinternational.org/sites/default/files/2018-02/Lebanon_UPR_23rd_session_Joint_Stakeholder_submission_0.pdf
[54] SMEX. (2018, October). *Law No. 81 Relating to Electronic Transactions and Personal Data*.
[55] SMEX. Check Article 103 of the law. Retrieved January 10, 2021, from https://smex.org/wp-content/uploads/2018/10/E-transaction-law-Lebanon-Official-Gazette-English.pdf

Furthermore, the law also does not mandate the creation of an independent data protection authority, which is crucial for ensuring proper oversight and enforcement of the law. Instead, it grants more power and authority to the executive branch of the government, namely to the Ministry of Economy and Trade, which has the authority to handle data collection and processing requests. Article 97 of the law grants the three ministries of defense, interior, and public health the authority to handle licensing of data related to external and internal state security, penal offenses, and judicial proceedings, as well as health, genetic identity, or sexual life respectively.

The power granted to the Ministry of Interior is particularly concerning. In December 2012, the Internal Security Forces (ISF), which directly reports to the Ministry of Interior, requested the interception and retention of all SMS messages sent in the period of two months following the killing of its intelligence chief in a car bombing in Beirut.[56] A leaked document from the Ministry of Information showed that the types of data requested included 2G and 3G data subscribers in Lebanon, including log files, IP addresses, usernames and passwords, phone numbers, names, and addresses, as well as the applications used on subscribers' phones.[57] In March 2014, the Lebanese cabinet gave the ISF and other security agencies full, unrestricted access to the electronic communications data of all Lebanese citizens for periods between six months and one year, and renewed it again for a period of four months in October 2017.[58]

In the face of such egregious privacy and data protection violations, the E-Transactions law is weak and fails to provide robust safeguards, and therefore, it was heavily criticized by civil society and legal experts. As Lebanese digital rights organization Social Media Exchange (SMEX) noted, the main purpose of the law seems to be to "facilitate the expansion of online commerce without regard to the effect this expansion might have on data protection."[59]

In addition to the E-Transactions Law of 2018, a number of privacy-related laws and sectoral laws and provisions provide limited protection for personal data, including:[60]

- **The Right of Access to Information Law (Law 28/2017):** The law provides limited protection for personal data through prohibiting public institutions from sharing citizens' personal information. Article 4 of the law grants citizens the right to access their personal data and files

[56] *See Supra* note 31.
[57] Electronic Frontier Foundation. (2013, February 07). *Data Request from Lebanese Security Agency Sparks Controversy.* Retrieved January 10, 2021, from https://www.eff.org/deeplinks/2012/12/lebanese-security-agency-user-data-request-sparks-controversy
[58] Privacy International. (2019, January 27). *State of Privacy Lebanon.* Retrieved January 10, 2021, from https://privacyinternational.org/state-privacy/1081/state-privacy-lebanon
[59] SMEX. (2020, March 31). *An "Ugly" New Data Protection Law in Lebanon.* Retrieved January 10, 2021, from https://smex.org/an-ugly-new-data-protection-law-in-lebanon/
[60] SMEX. (2020, October 12). [Report] *Building Trust: Toward a Legal Framework that Protects Personal Data in Lebanon*. Retrieved January 10, 2021, from https://smex.org/building-trust-toward-a-legal-framework-that-protects-personal-data-in-lebanon-report/

collected by public authorities, and in limited cases also private companies that are either controlled by the government or contracted to provide a public service or manage a public property. This information includes a citizen's "name, identification number, code, or other identifying features such as fingerprints, eye, voice, and image recognition." It also grants citizens the right to "request correction, completion, updating, or deletion of personal information related to them in the event that it is incorrect, incomplete, ambiguous, outdated, or is the kind of information prohibited from being collected, used, exchanged, or retained."[61]

- **The Consumer Protection Code (Law 659/2005):** The law obligates business suppliers not to disclose their consumers' data without their consent, and to "take all measures necessary to keep such information secret."[62]
- **The Code of Medical Ethics (Law 288/1994):** Article 7 obligates doctors with professional secrecy. Physicians must keep confidential all information shared by the patient, and any information which the physician has seen, learned, discovered, or inferred in the course of practicing his profession or as a result of the tests he conducted, with a few exceptions such as reporting sexually transmitted diseases or other diseases that must be reported to the authorities.[63]
- **The Lebanese Penal Code:** Articles 579, 580, and 581 punishes anyone who, by virtue of their position, profession, or art, is aware of a secret and discloses it without a legitimate reason, or anyone who discloses a phone call or who opens mail not intended for him or her.[64]
- **The Banking Secrecy Act (1956):** The law prohibits banks from sharing banking secrets and information to any public or private entity except in cases defined by the law.[65]
- **The Telecommunications Law (Law 431/2002):** It must be noted that this law, which regulates the telecommunications services sector, does not address personal data protection, with the exception of Article 38, which obligates controllers and inspectors to respect confidentiality of information they have access to while conducting their official duties.[66]
- **The Telecommunications Interception Act (Law 140/1999):** This law stipulates that the right to secrecy of communications is protected and cannot be subjected to any form of tapping, surveillance, interception, or violation, except in cases of extreme urgency and upon obtaining

[61] CYRILLA. (2017). *The Right of Access to Information Law of 2017.* Retrieved January 10, 2021, from https://cyrilla.org/en/entity/s1g1mlpyymh?page=3
[62] *See Supra* note, 36.
[63] CYRILLA. *The Physician's Law No. 288 of 1994 and its amendments in 2012.* Retrieved January 10, 2021, from https://cyrilla.org/en/entity/s4tb7viliry0tyjiuzsi6n7b9?page=1
[64] CYRILLA. *Penal Code No. 340 of 1943.* Retrieved January 10, 2021, from https://cyrilla.org/en/entity/o9438um4ko3gq0omr3sicc8fr?page=128
[65] CYRILLA. *The Banking Secrecy Law of 1956.* Retrieved January 10, 2021, *from* https://cyrilla.org/en/entity/vj24q5xwaxx1hhm4h48b5u3di
[66] World Bank. *Lebanon Telecommunications Law No. 431 of 2002.* Retrieved January 10, 2021, from https://ppp.worldbank.org/public-private-partnership/library/lebanon-telecommunications-law-law-431-2002

> a judicial or administrative order. This includes wired or wireless communications; landlines, mobile telephone, fax, and electronic mail.

In a country rampant with corruption and where the interests of the state and business often intertwine, the current data protection legal framework provides weak and insufficient protections from the government's abuse of power, such as by striking deals with private companies that are close to ministries or politicians, in order to get access to citizens' personal data and trade this information for profit. For instance, the two major telecommunications companies, Alpha and Touch, which are owned by the government, reportedly "admit selling their subscribers' data to businesses or individuals who want to send text messages to a target group as defined by gender, age, and profession."[67] Touch also can sell target groups, identified based on users' behavior.[68]

The rise in the use of biometric technology for identification further necessitates the need for a stronger data protection law in Lebanon. In August 2016, the General Directorate of General Security started issuing biometric passports with a chip which holds the passport holder's full name, birthdate, photo, and fingerprints.[69] In January 2017, the Ministry of Interior also started issuing biometric driving licenses,[70] and three months later, General Security announced it will introduce biometric residence permits for foreign and Arab residents. Furthermore, in December 2017, the Minister of Telecommunications proposed for security purposes the introduction of biometric SIM cards, whereby anyone who purchases a SIM must provide biometric information.[71]

The collection of citizens' sensitive personal information in the absence of a strong data protection framework is compounded by the lack of cybersecurity strategy and capabilities to ward off malicious attacks and threats in Lebanon.[72] It wasn't until August 2019 that the Lebanese cabinet introduced a National Lebanese Strategy for Cybersecurity with help from the European Union,[73] which was met with skepticism given the state's lack of needed resources and competences to implement such a

[67] *See Supra* note, 36.
[68] Touch's SMS advertising page. Retrieved January 10, 2021, from https://www.touch.com.lb/autoforms/portal/touch/business/sms-advertising/mobile-media
[69] The General Directorate of General Security's. *Biometric Lebanese passports issuance.* Retrieved January 10, 2021, from https://www.general-security.gov.lb/en/posts/182
[70] *See Supra* note 36.
[71] SMEX. (2020, July 29). A Brief History of Personal Data Collection in Lebanon. Retrieved January 10, 2021, from https://smex.org/a-brief-history-of-personal-data-collection-in-lebanon/
[72] *The assessment of the Lebansese Telecommunications Regulatory Authority of Lebanon's Cybersecurity.* Retrieved January 10, 2021, from http://www.tra.gov.lb/Cybersecurity-in-Lebanon
[73] Middle East Institute. (2020, December 01). *Lebanon's cybersecurity strategy emerges.* Retrieved January 10, 2021, from https://mei.edu/publications/lebanons-cybersecurity-strategy-emerges

strategy.[74] Consequently, the government might end up handing its cybersecurity responsibilities to private companies, raising further concerns and questions about data protection.

2. Case studies

1) Mishandling voters' personal data ahead of elections

Voter data, such as official voter registers or voter lists used for political campaigning, are essential and significant assets for elections and democratic processes and therefore can be susceptible to data breaches, hacks, leaks, and mishandling for profit or political gain.[75]

In Lebanon, "voters lists are usually given away or can be sold for a nominal amount (i.e the cost of the disks that they're stored on)."[76] In one instance, a Lebanese citizen residing in France received a WhatsApp message from a political candidate intended for a woman and her husband, inviting them for a voters' meeting in Paris.[77] This is explained by the fact that the man, who helped in registering voters, had used his phone number in filing registration forms. He suspected that the voter database had been passed along or sold by the Ministry of Foreign Affairs to political candidates.

According to SMEX, "the legal framework for data protection in Lebanon is fragile and the ambiguous language in Article 115 of the 2017 Election Law requires the Ministry of Foreign Affairs and Expatriates to 'publish and circulate' the lists of names of voters residing abroad 'by all possible means' in order to ensure that the identity of the expatriates matches the information mentioned in the personal status records."[78] For example, ahead of the 2018 parliamentary elections, the Lebanese Embassy in the United Arab Emirates leaked via email the personal data of more than 5,000 Lebanese citizens residing in the country. The email, which was sent for registered voters to verify their personal information, enlisted an excel sheet attachment with their full name, mother's name, father's name, gender, date of birth, religion and denomination, marital status, and home address.[79]

---

[74] Khodor, H. (2019, August 31). *Cybersecurity as dangerous as border security: Protecting the state and citizens* (in Arabic). Retrieved January 10, 2021, from https://www.almodon.com/economy/2019/8/31/%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A-%D8%A8%D8%AE%D8%B7%D9%88%D8%B1%D8%A9-%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%AD%D8%AF%D9%88%D8%AF-%D8%AD%D9%85%D8%A7%D9%8A%D8%A9-%D8%A7%D9%84%D8%AF%D9%88%D9%84%D8%A9-%D9%88%D8%A7%D9%84%D9%85%D9%88%D8%A7%D8%B7%D9%86%D9%8A%D9%86

[75] Tactical Tech. (2019). *Breaches, Leaks and Hacks: The vulnerable life of voter data.* Retrieved January 10, 2021, from https://ourdataourselves.tacticaltech.org/posts/breaches-leaks-hacks/

[76] Interview with Grant Baker, Research Manager at SMEX, 2020.

[77] A tweet fromJP.A (@JPierreAn) posted on March 29, 2018. Retrieved January 10, 2021, from https://twitter.com/JPierreAn/status/979336312527491073

[78] Interview with SMEX, 2020.

[79] SMEX. (2019, June 16). *Lebanese Embassies Expose the Personal Data of Registered Voters Living Abroad.* Retrieved January 10, 2021, from https://smex.org/lebanese-embassies-expose-the-personal-data-of-registered-voters-living-abroad/

SMEX obtained a copy of a similar email sent to more than 200 Lebanese registered voters in the Hague. The email also included an Excel sheet attachment containing personal information. In a clear indication of Lebanon's indifference to protecting personal data, the embassy entered the voters' email addresses in the Cc field, instead of using the Bcc field.[80]

2) Telcos and ISPs' disregard of privacy and data protection

Lebanon has a particularly large number of ISPs. There are currently 114 licensed ISPs, according to research conducted by SMEX. Yet, only 39 have a website, only four of those have a privacy policy published on their website, and four published their terms of services.[81] OGREO, a state-owned fixed internet service that provides internet connection to all ISPs in Lebanon, neither provides a privacy policy on its website, nor shares information on the use or management of users' data.

Most of the Lebanese ISPs do not share information about how they are gathering, storing, and selling user data, before or after people sign up for their services. Unfortunately, even the few ISPs that do have a privacy policy are not exactly transparent. According to SMEX, "websites with privacy policies, which are only available in English, provide users with the policy only after they have signed a contract. The publicly displayed policies, on the other hand, apply exclusively to the website. Therefore, users cannot determine how the ISPs are gathering and selling user data neither before nor after signing up for their services."[82]

The threat to users' privacy is further exacerbated by the telecommunications companies' use of Deep Packet Inspection (DPI) technology, which enables examination of data packets transmitted in a given network, typically to look for malware or unwanted online traffic in the user-defined payload of the transmission. Use of DPI technology can also facilitate mass surveillance and censorship. It allows telcos to monitor users' unencrypted communication in real time, to identify and analyze users' online habits, and to implement targeted blocking and internet shutdowns.

In February 2020, the *Al-Akhbar* newspaper reported that Alfa purchased DPI software from Sandvine in 2015 and uses this technology to share the personal information of its subscribers with security agencies.[83] In 2018, the company renewed its DPI technology with a new $3 million contract with the US-based firm NEXIUS. However, the technology remains non-operational, and according to a security

[80] *Ibid*.
[81] SMEX. (2020, February 26). *Lebanese ISPs Lack Transparency.* Retrieved January 10, 2021, from https://smex.org/lebanese-isps-lack-transparency/
[82] *Ibid*.
[83] Farfour, H. (2020, February 14). *Spying on ISPs subscribers* (in Arabic). Retrieved January 10, 2021, from https://al-akhbar.com/Community/284136/%D8%A8%D8%B1%D9%86%D8%A7%D9%85%D8%AC-%D8%A7%D9%84%D8%AA%D8%AC%D8%B3%D8%B3-%D8%B9%D9%84%D9%89-%D9%85%D8%B4%D8%AA%D8%B1%D9%83%D9%8A-%D8%A7%D9%84%D8%AE%D9%84%D9%88%D9%8A-%D9%87%D8%AF%D8%B1-%D8%A3%D9%85-%D9%86%D8%AC%D8%A7%D8%AD-%D9%88%D8%B4%D9%8A%D9%83

official, it is not needed by security agencies.[84] Touch was also considering purchasing the same technology from NEXIUS.[85]

A recent report by *Masaar* on the activities of Sandvine found that Lebanon is home for one of the most important partners of Sandvine in the MENA region, Computer Information Systems (CIS). CIS's partnership with Sandvine involves DPI solutions and the confirmed list of clients in Lebanon include Al-Mada, Alfa, touch, OGERO, Sodetel, the Ministry of Telecommunications, and the Telecommunications Regulatory Authority.[86]

PALESTINE

1. Legal framework for privacy and data protection

Data protection in Palestine presents a very complex yet illustrative case to show how state actors can exploit personal data and information in contexts of armed conflict or war for oppression and control. In the case of the occupied Palestinian territory (oPt), Palestinian internet users face three distinct but interlinked challenges: their subjugation to an occupying power's military laws, Israel's sovereignty and control over the Palestinian ICT infrastructure, and their exposure to one of the largest surveillance operations in the world.[87]

The Palestinian territories — the West Bank, the Gaza Strip, and East Jerusalem — have been occupied by Israel since 1967. Palestinian communities in the oPt are subject to particulary complex and multiple legal systems.[88] Palestinians living in the West Bank, for instance, are governed by a dual legal system:[89] Palestinian law administrated by the Palestinian Authority in restricted pockets of land where it has full civil control (as well as Jordanian law of 1967),[90] and Israeli military orders issued

[84] *Ibid*.
[85] SMEX. *Security Heaven, Privacy Hell: Lebanese Telcos Introduce Deep Packet Inspection (DPI)*. Retrieved January 10, 2021, from https://smex.org/security-heaven-privacy-hell-lebanese-telcos-introduce-deep-packet-inspection-dpi/
[86] Masaar. (2020, November 15). *Sandvine...the surveillance octopus in the Arab region.* Retrieved January 10, 2021, from https://masaar.net/en/sandvine-the-surveillance-octopus-in-the-arab-region/
[87] Haaretz. (2019, July 15).) *This Israeli Face-recognition Startup Is Secretly Tracking Palestinians.* Retrieved January 10, 2021, from https://www.haaretz.com/israel-news/business/.premium-this-israeli-face-recognition-startup-is-secretly-tracking-palestinians-1.7500359
[88] These include Ottoman law, British Mandate emergency regulations, Israeli civil law for East Jerusalem and Jewish settlers, Jordanian civil law in the West Bank, Egyptian civil law in Gaza, Israeli military law in the West Bank, legislation and executive decrees issued by the Palestinian Authority, in addition to agreements and signed protocols between Israel and the Palestinians. Given this complexity and the specific scope and purpose of this report, we will address data protection issues in the West Bank only.
[89] Husseini, H. (2016). *Legal Duality in the Occupied West Bank.* Retrieved January 10, 2021, from https://pij.org/articles/1683/legal-duality-in-the-occupied-west-bank
[90] In accordance to the Interim Agreement on the West Bank and the Gaza Strip of the Oslo Accords signed between Israel and the Palestinians in 1995, the Palestinian Authority has full civil and security control over Area A (18% of the West Bank) and full civil control and joint Israeli-Palestinian security control over Area B (about 22% of the West Bank).

since 1967. These include a military proclamation which permitted the application of the Defense (Emergency) Regulation of 1945 (enacted by the British Mandate), the Military Order 101 issued in August 1967, and Military Order 1651 promulgated in 2010. Israel has systematically used its broadly worded military orders to unlawfully restrict and violate the rights of free assembly, association, expression, and press for Palestinians in the occupied West Bank.[91] By contrast, Israeli settlers who live in the West Bank remain under the jurisdiction of Israeli law and court system, which results in institutionalized and systematic discrimination.[92] Consequently, the Israeli authorities "have deprived the nearly 2.5 million Palestinians they rule over in the West Bank of their basic rights — rights enjoyed by the more than 400,000 Israeli settlers living in illegal settlements in the same territory."[93]

Therefore, Israel's privacy and data protection law, the Protection of Privacy Law (the PPL), passed in 1981, in addition to the guidelines of the Israeli Privacy Authority established in 2006, do not apply to Palestinians in the West Bank nor in the Gaza Strip. It is worth noting here that the European Commission determined on January 31, 2011, in accordance to Article 25(6) of directive 95/46/EC, that Israel provides adequate protection with regard to the automated processing of personal data.[94] The European Commission decision applies "without prejudice to the status of the Golan Heights, the Gaza Strip and the West Bank, including East Jerusalem, under the terms of international law,"[95] which effectively disregards Israel's failure and systematic violations of the right to privacy and data protection of Palestinians in the oPt.

As an occupying power, Israel has legal obligations towards Palestinians in the occupied territories, both under the law of occupation and international human rights law.[96] Israel signed the United Nations' International Covenant on Civil and Political Rights (ICCPR) in 1966, and ratified it in 1991. However, the Israeli authorities have long maintained that their human rights obligations under international law do not extend to Palestinians in occupied territories. Israel argues that the ICCPR does not apply extraterritorially, and therefore it excludes the oPt.[97] The UN Human Rights

[91] Human Rights Watch. (2019, December 18). *Born Without Civil Rights.* Retrieved January 10, 2021, from https://www.hrw.org/report/2019/12/17/born-without-civil-rights/israels-use-draconian-military-orders-repress
[92] The Association for Civil Rights in Israel. (2014 October). *One Rule, Two Legal Systems: Israel's Regime of Laws in the West Bank.* Retrieved January 10, 2021, from https://law.acri.org.il/en/wp-content/uploads/2015/02/Two-Systems-of-Law-English-FINAL.pdf
[93] *See Supra* note, 78.
[94] The Official Journal of the European Union. (2011, January 31). Retrieved January 10, 2021, from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ%3AL%3A2011%3A027%3A0039%3A0042%3AEN%3APDF
[95] *Ibid*, Article 2(2).
[96] The duties of the occupying power are constituted primarily in the 1907 Hague Regulations, the Fourth Geneva Convention (GC IV, art. 27-34 and 47-78), as well as in certain provisions of Additional Protocol I and customary international humanitarian law. See *the ICRC guide on occupation and international humanitarian law*. Retrieved January 10, 2021, from https://www.icrc.org/en/doc/resources/documents/misc/634kfc.htm#:~:text=The%20main%20rules%20o%20f%20the,acquire%20sovereignty%20over%20the%20territory.&text=Transfers%20of%20the%20civilian%20population,Collective%20punishment%20is%20prohibited.
[97] The official Israeli interpretation of Article 2(1) of ICCPR contends that the ICCPR's protections extend only to individuals that are both physically "within its territory" and legally "subject to its jurisdiction." (2019). See Georgetown Journal of International Law, *An International Right to Privacy: Israeli Intelligence Collection in the Occupied Palestinian Territories.*

Committee, which is the UN body responsible for monitoring the implementation of ICCPR by state parties, and the International Court of Justice, have both rejected this position.[98]

On the other hand, the Palestinian Basic Law, which serves as the constitutional framework for the Palestinian legal system, criminalizes "any violation of any personal freedom, of the sanctity of the private life of human beings, or of any of the rights or liberties."[99] It also guarantees Palestinian citizens access to fair remedy if their fundemental rights have been violated. In practice, however, there have been only limited efforts by the Palestinian Authority (PA) to protect the privacy of Palestinian individuals and safeguard their personal information.

To date, there is no data protection law and it remains a non-priority for the PA. Instead, the PA has prioritized the adoption of a controversial cybercrime law (Law 16/2017), which was enacted in 2017 by presidential decree and in full secrecy.[100] Palestinian activists, journalists, and civil society strongly opposed the law because it has broadly worded and ambigious clauses that threaten freedom of expression and the right to privacy online, and Palestinian authorities can misuse it to clamp down on political dissent and independent media.[101] As a result of the strong opposition to the law, the PA issued by decree an amended law (No.10 of 2018). While the amendments respond to some of the concerns Palestinian legal experts and civil society have raised, a number of problematic articles remain.[102]

Article 4 of the cybercrime law (2018) penalizes unlawful access to information systems which could result in "deletion, addition, disclosure, destruction, alteration, transfer, capture, copy, dissemination, reproduction or attachment of data or electronic information."[103] Article 7 also penalizes anyone who intentionally and unlawfully receives, records, or intercepts any data by at least one year in prison and a fine between 1,000 and 3,000 Jordanian Dinar. Additionally, Article 22 prohibits "arbitrary or illegal interference with the privacy of any person or the affairs of his family, home or correspondence," and the dissemination of the information thereof.

Retrieved January 10, 2021, from https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2019/10/GT-GJIL190033.pdf

[98] *Ibid*.

[99] Article 32 of the Amended Basic Law of 2003. Retrieved January 10, 2021, from https://www.elections.ps/Portals/0/pdf/The_Amended_Basic_Law_2003_EN.pdf

[100] Global Voices Advox. (2017, August 5) *Will Palestine's New Cybercrime Law Pave the Way for More Rights Violations?* Retrieved January 10, 2021, from https://globalvoices.org/2017/08/03/will-palestines-new-cybercrime-law-pave-the-way-for-more-rights-violations/

[101] *Presidential Decree No. (16) for the year 2017 Regarding Cybercrime.* Retrieved January 10, 2021, from https://security-legislation.ps/sites/default/files/law/Law%20by%20Decree%20No.%2010%20of%202018%20on%20Cybercrime.pdf

[102] Association for Progressive Communications (APC). (2018, June 5). *Has the Palestinian Cybercrime Law really been amended?* Retrieved January 10, 2021, from https://www.apc.org/en/news/has-palestinian-cybercrime-law-really-been-amended

[103] *Ibid*.

However, the law includes a number of privacy-encroaching provisions. Most notably, it obligates ISPs to retain users' data for at least three years and to provide the public prosecutor access to all data and information when needed. It also grants the public prosecutor the authority to order the immediate collection of unrestricted data including monitoring private communications, traffic data, and metadata.[104]

To what extent could a Palestinian data protection law provide necessary privacy safeguards? Unfortunately, not much. Even if the PA adopted data protection legislation, it would grant limited protection given that the entire Palestinian ICT infrastructure is under the control of Israel, which it has maintained since its occupation of the Palestinian territories in 1967. Upon the signing of the Oslo peace agreement in 1995, Israel handed partial control of the ICT infrastructure in the West Bank and Gaza to the PA. Despite the right granted to Palestinians under the agreement to develop their own independent ICT,[105] the Israeli authorities remain in total control of the electromagnetic waves as well as of importing and installation of any equipment by Palestinian telcos and ISPs under undisclosed "security reasons."[106] As a result, Israel routinely denies Palestinians access to new technologies. For instance, it took over a decade for the Israeli authorities to grant the Palestinian mobile operators their request to introduce 3G networks,[107] and they have yet to allow 4G networks.

This legal and infrastructural architecture has allowed the mass surveillance of Palestinian communities and the exploitation of their personal data for decades without accountability. Providing testimony on the privacy violations committed by the Israeli intelligence, one Israeli officer stated: "Any information that might enable extortion of an individual is considered relevant information. Whether said individual is of a certain sexual orientation, cheating on his wife, or in need of treatment in Israel or the West Bank – he is a target for blackmail."[108] Indeed, members of the LGBTQ+ community in Palestine are extorted by the Israeli intelligence to turn informants or else they are outed and exposed.[109]

Personal data of Palestinian individuals are collected in all sorts of ways. In 2018, the Israeli army set up temporary checkpoints in the West Bank where they stopped and asked Palestinian men to fill out forms requesting their name, age, phone number, ID, and license number, in addition to a photocopy

[104] *Ibid*.
[105] Article 36 of Annex III of the Oslo Accords sets out the provisions regulating the telecommunications sphere in the oPt.
[106] 7amleh. (2018, December). *Connection Interrupted: Israel's Control of the Palestinian ICT Infrastructure and Its Impact on Digital Rights.* Retrieved January 10, 2021, from https://7amleh.org/wp-content/uploads/2019/01/Report_7amleh_English_final.pdf
[107] Sawafta, Reuters, A. (2018, January 24). *Palestinians get 3G mobile services in West Bank.* Retrieved January 10, 2021, from https://www.reuters.com/article/israel-palestinians-telecom-idUSL8N1PJ3FW
[108] The Guardian. (2014, September 12). *'Any Palestinian is exposed to monitoring by the Israeli Big Brother'.* Retrieved January 10, 2021, from https://www.theguardian.com/world/2014/sep/12/israeli-intelligence-unit-testimonies
[109] Mondoweiss. (2014, September 15). *Israel surveils and blackmails gay Palestinians to make them informants.* Retrieved January 10, 2021, from https://mondoweiss.net/2014/09/blackmails-palestinian-informants/

of their ID.[110] According to Israeli media, this arbitrary collection of personal data is used to set up a database for countering terrorism. Given that there is no legal protection for Palestinians living in the West Bank, as we explained previously, Palestinians do not have any access to remedy for the systematic violations of their privacy and misuse of their personal data.

As the Shin Bet, the Israeli internal security agency, stepped in at the outbreak of the COVID-19 pandemic in Israel, it was revealed that the agency has been maintaining a classified database for the past 18 years, which includes the data of every person who uses telecom services in Israel. The database, known as "the Tool," includes data about the location of the user's device, the cell and antenna zone to which it is connected, the metadata of every voice call and text message sent or received, and internet browsing history. The information collected by the Tool is saved for an unknown period, and the rules about how it is stored, protected, and deleted are top secret.[111]

2. Case studies

1) Al Munasiq app and abusive collection of Palestinians' information by Israeli defense forces

In February 2019, the Israeli Coordination of Government Activities in the Territories (COGAT) — the military's civil administration in the oPt — launched a mobile application called the Coordinator (المنسق, Al Munasiq) to offer Palestinians from the oPt digital access to a number of their services, mostly related to applications for stay and entry permits to Israel.

Whereas COGAT claims that "the app was developed for the benefit of the Palestinian public,"[112] its intrusive collection of data might suggest a different motive. According to the app's terms of service, Palestinian users are required to consent to the collection and use of their data "for any purpose, including for security purposes."[113] This includes access to geolocation data, messages, files stored on the phone, and access to the phone's camera. The terms of service also make it clear that the use and storage of users' data is up to the sole discretion of the Israeli authorities:

> "You agree and declare that you know that all the information you are asked to provide is not required by law or defense regulations, and it is provided of your own free will, so that we can

[110] Haaretz. (2018, March 08). *Israeli army setting up extensive database with personal details of Palestinians collected at checkpoints.* Retrieved January 10, 2021, from https://www.haaretz.com/israel-news/.premium-idf-info-we-collect-on-palestinians-meant-for-anti-terror-database-1.5886616

[111] Brookings Institution. (2020, July 06). *How Israel's COVID-19 mass surveillance operation works.* Retrieved January 10, 2021, from https://www.brookings.edu/techstream/how-israels-covid-19-mass-surveillance-operation-works/

[112] Haaretz. (2020, May 15). *Israel tells court would stop forcing Palestinian laborers to give access to phone data.* Retrieved January 10, 2021, from https://www.haaretz.com/middle-east-news/palestinians/.premium-over-50-000-palestinians-forced-to-give-phone-data-to-israel-1.8844580

[113] *Ibid*.

> make use of it as we see fit. In addition, you consent that we may store the information you have provided to us in our databases based on our considerations."[114]

The app came under scrutiny in the wake of the COVID-19 pandemic. While COGAT claims that use of app is voluntary, Palestinian residents and workers in Israel were forced to download and use the app during the pandemic.[115] In April 2020, the Israeli Ministry of Agriculture also instructed Israeli employers to require their Palestinian empolyees to fill out a health declaration on the COGAT's app prior to their entry to Israel. By November 2020, the number of app users had doubled from June 2020, with more than 100,000 downloads compared to 50,000 in June.

To clarify, Palestinians from the occupied territories who reside or work in Israel must obtain permits from COGAT in order to lawfully do so. Due to the pandemic, however, the coordination offices in the West Bank were closed and consequently Palestinians were instructed to check the status of their permits only through the Al Munasiq app. As highlighted by the Center for the Defense of the Individual (HaMoked) and Physicians for Human Rights- Israel, "people have no real free choice in the matter and must install the intrusive application." Palestinian applicants have " to make sure they are lawfully present in their homes – otherwise they face the threat of deportation and separation from their families."[116]

As a result, HaMoked petitioned the High Court of Justice objecting to the app's violation of users' right to privacy and dignity under Israeli and international law. The court dismissed the petition because actual harm had not been proven. However, COGAT amended the terms of service to clarify that the app has no access to files, contacts, and photos, and that the user's consent is strictly related to the provision of the specific data required for the service in use.[117]

Nevertheless, the Palestinian Digital Rights Coalition warned Palestinians not to download and use the application, describing it as "dangerous." Indeed, taking into consideration that COGAT provides services which require processing the personal information of Palestinians, such as full name, ID number, place and date of birth, family members, place of residence, and age, among other data points, the further collection of private data through Al Munasiq app constitutes a severe infringement

---

[114]Middle East Monitor. (2020, April 09). *Israel tells Palestinians to use tracking app to verify their residency status.* Retrieved January 10, 2021, from https://www.middleeastmonitor.com/20200409-israel-tells-palestinians-to-use-tracking-app-to-verify-their-residency-status/

[115]Middle East Eye. (2020, April 8). *'The Coordinator': Israel instructs Palestinians to download app that tracks their phones.* Retrieved January 10, 2021, from https://www.middleeasteye.net/news/coordinator-israel-instructs-palestinians-download-app-tracks-their-phones

[116]HaMoked. (2020). *HaMoked and PHR-Israel demand: Israel must stop compelling Palestinians holding Israeli stay permits to download an intrusive mobile application in order to ascertain their permits' renewal.* Retrieved January 10, 2021, from http://www.hamoked.org/Document.aspx?dID=Updates2157

[117] HaMoked. (2020). *Following HaMoked's demand: the military amended the invasive terms of use of the mobile app enabling Palestinians to check the status of permit requests, 2020.* Retrieved January 10, 2021, from http://www.hamoked.org/Document.aspx?dID=Updates2175

of Palestinians' right to privacy and may lead to further human rights violations, especially given its use by an occupying power.[118]

2) Facial Recognition: Israel's thriving business, Palestinians' privacy nightmare

In early October 2019, Palestinians found a surveillance camera camouflaged as a stone planted at a village cemetery near the West Bank city of Ramallah. The camouflaged camera was reported to be manufactured by AnyVision, an Israeli company which sells facial recognition technology.[119] While the company denied these reports, its involvement was implicated in another secret military surveillance project throughout the West Bank. According to an investigation published by NBC, AnyVision's technology was used in an Israeli secret surveillance scheme to monitor the movement of Palestinians, a scheme named "Google Ayosh" in a reference to the technology's ability to search and find people.[120] The project's success won the company a top defense award in 2018 for "preventing hundreds of terror attacks" with the use of "large amounts of data." In addition to uncovering the classified project, NBC says it has received evidence that AnyVision's technology has also been used by the Israeli police to track Palestinians' movement throughout East Jerusalem.[121]

The technology in question is one of AnyVision's core products, "Better Tomorrow." Through installed facial recognition cameras, an automated watchlist alerting system can identify the faces of "suspects" in crowds, and track and categorize vehicles. This technology, coupled with Israel's profiling database, is a powerful surveillance tool. AnyVision also provides facial recognition technology at 27 Israeli military checkpoints in the West Bank to authenticate the identity of Palestinians crossing into Israel.[122] It is important to note that this technology is not used at checkpoints used by Israelis.

Following NBC's report and public outcry from activists and civil society,[123] who pointed to evidence that AnyVision's software helped entrench Israel's military occupation, Microsoft decided to

[118] APC. (2020, June 15). *7amleh: Palestinian Digital Rights Coalition warns against phone application "The Coordinator".* Retrieved January 10, 2021, from https://www.apc.org/en/news/7amleh-palestinian-digital-rights-coalition-warns-against-phone-application-coordinator
[119] Middle East Monitor. (2019, October 07). *Palestinians discover camouflaged surveillance device in Ramallah cemetery.* Retrieved January 10, 2021, from https://www.middleeastmonitor.com/20191007-palestinians-discover-camouflaged-surveillance-device-in-ramallah-cemetery/
[120] NBC. (2019, November 19). *Why did Microsoft fund an Israeli firm that surveils West Bank Palestinians?* Retrieved January 10, 2021, from https://www.nbcnews.com/news/all/why-did-microsoft-fund-israeli-firm-surveils-west-bank-palestinians-n1072116
[121] *Ibid*.
[122] Haaretz. (2019, July 15). *This Israeli face-recognition startup is secretly tracking Palestinians.* Retrieved January 10, 2021, from https://www.haaretz.com/israel-news/business/.premium-this-israeli-face-recognition-startup-is-secretly-tracking-palestinians-1.7500359
[123] Jewish Voice for Peace. *Tell Microsoft: #DropAnyVision.* Retrieved January 10, 2021, from https://dropanyvision.org/

investigate[124] whether the use of facial recognition technology developed by AnyVision complied with its ethics and principles.[125] Microsoft hired former U.S. Attorney General Eric Holder and his team at Covington & Burling to perform an audit of AnyVision which found that "AnyVision's technology has not previously and does not currently power a mass surveillance program in the West Bank that has been alleged in media reports."[126] Despite the audit results, Microsoft and AnyVision announced in a joint statement in March 2020 to "have agreed that it is in the best interest of both enterprises for Microsoft to divest its shareholding in AnyVision."[127]

In June 2020, as major tech companies continued to divest from facial recognition technology,[128] AnyVision doubled down on its investment instead, stating it has no plans to leave the business.[129] Why should it? Israel's surveillance industry has been thriving for decades, by exporting surveillance technology to repressive regimes worldwide, which is then used to target activists and dissidents.[130] Its "success" is reinforced by the marriage between the Israeli tech industry and the military, as well as the use of Palestinian communities as guinea pigs for those technologies.

AnyVision has used the oPt as "testing ground" before it marketed and exported its spyware to foreign countries. While 95% of the company's revenues come from customers outside of Israel, "Israel was the first territory" where they "validate their technology" before it's exported, according to the company's co-founder and former CEO Eylon Etshtein.[131] It is worth noting that Etshtein himself served in the Israeli Defense Forces. The company's president, Amir Kain, is also the former head of

[124] Middle East Eye. (2019, November 16). *Microsoft to investigate work of Israeli facial recognition technology it funded.* Retrieved January 10, 2021, from https://www.middleeasteye.net/news/microsoft-investigate-work-israeli-facial-recognition-technology-it-funded
[125] Microsoft. (2018). *Six Principles for Developing and Deploying Facial Recognition.* Retrieved January 10, 2021, from https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2018/12/MSFT-Principles-on-Facial-Recognition.pdf
[126] M12. (2020, April 08). *Joint Statement by Microsoft & AnyVision – AnyVision Audit.* Retrieved January 10, 2021, from https://m12.vc/news/joint-statement-by-microsoft-anyvision-anyvision-audit/
[127] *Ibid*.
[128] The Verge. (2020, June 09). *IBM will no longer offer, develop, or research facial recognition technology.* Retrieved January 10, 2021, from https://www.theverge.com/2020/6/8/21284683/ibm-no-longer-general-purpose-facial-recognition-analysis-software
[129] Haaretz. (2020). *Tech Giants Stage Facial Recognition Retreat, but Israeli Startups Stay in the Game.* Retrieved January 10, 2021, from https://www.haaretz.com/israel-news/business/.premium-tech-giants-stage-facial-recognition-retreat-but-israeli-other-startups-stay-in-1.8920814
[130] According to an extensive investigation based on 100 separate sources in 15 countries published in 2018 by Haaretz, Israeli companies sold surveillance used in targeting activists in Bahrain, Indonesia, Angola, Mozambique, the Dominican Republic, Azerbaijan, Swaziland, Botswana, Bangladesh, El Salvador, Panama, Nicaragua, Mexico, Uzbekistan, Kazakhstan, South Sudan, Honduras, Peru, Colombia, Uganda, Nigeria, Ecuador and the United Arab Emirates, among others. See Haaretz, *Revealed: Israel's Cyber-spy Industry Helps World Dictators Hunt Dissidents and Gays*. Retrieved January 10, 2021, from https://www.haaretz.com/israel-news/.premium.MAGAZINE-israel-s-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays-1.6573027201
[131] NBC. (2019, November 19). *Why did Microsoft fund an Israeli firm that surveils West Bank Palestinians?* Retrieved January 10, 2021, from https://www.nbcnews.com/news/all/why-did-microsoft-fund-israeli-firm-surveils-west-bank-palestinians-n1072116

the defense ministry's security department, and one member of its advisory board is the former Mossad chief Tamir Pardo.[132]

TUNISIA

1. Legal framework for privacy and data protection

In Tunisia, the culture of online privacy and the protection of personal data is still modest, despite the fact that the right to privacy is codified in the Tunisian Constitution of 2014 as well as the Data Protection Law (No 63).[133] In fact, since 2002, Tunisia has been a pioneer in the MENA region in its adoption of laws and policy on privacy that aim to safeguard people's personal data from unlawful processing, but the regime is still not adequate.

The Data Protection Law (No 63) was adopted in 2004 under the regime of the former president of Tunisia, Zine el Abidine Ben Ali, who infamously censored and controlled online content. To date, this flawed Tunisian data protection framework remains in place even though it has repeatedly been deemed incompatible with the newly established principles of the 2014 Tunisian Constitution and Tunisia's international obligations. This situation generates legitimate concerns regarding the real-world effects of the consecration of the right to data protection in Tunisia.

The 2004 law details the scope of data protection, and establishes a national commission in charge of its enforcement. The law is based on the principles of lawfulness, processing, and accountability; it gives rights to those individuals whose data are processed, and sets out obligations for the organizations and individuals in charge of the processing. However, the law has a number of shortcomings, primarily due to the fact that it is outdated and thus fails to address rising risks associated with the advancement and use of new technologies. For example, Article 4 of the law defines personal data as "any information whatever its origin or its means relating to an individual who can be identified, directly or indirectly, with the exception of any information related to public life or considered public life by law."[134] There is no indication as to whether the law applies to the processing of personal data of users online. Moreover, public entities such as police stations are exempted under the law from any obligation that would apply to personal data processors. Furthermore, public entities are not obliged to declare data processing, and as a result, individuals'

[132] Forbes. (2019, August 01). *Microsoft Slammed For Investment In Israeli Facial Recognition 'Spying On Palestinians'.* Retrieved January 10, 2021, from https://www.forbes.com/sites/thomasbrewster/2019/08/01/microsoft-slammed-for-investing-in-israeli-facial-recognition-spying-on-palestinians/

[133] *Instance nationale de protection des données personnelles (INPDP), Activity Report 2009-2017.* (in Arabic) .Retrieved January 10, 2021, from http://www.inpdp.nat.tn/Rapport_2009-2017.pdf

[134] Access Now.(2018, November 09). *In Tunisia, an open debate on data protection and the right to access information.* Retrieved January 10, 2021, from https://www.accessnow.org/in-tunisia-an-open-debate-on-data-protection-and-the-right-to-access-information/

right to informed consent is severely limited.

The law provides for the establishment of the National Authority for the Protection of Personal Data (INPDP), which came into being in 2009, five years after the law was passed. The INPDP has no authority to issue regulations or make decisions concerning data violations, and according to Article 76 its mandate is limited to receiving complaints from citizens about privacy violations, and to make official recommendations on issues related to data protection without having the power to enforce them. This functionality of the INPDP contravenes the nature of regulatory and oversight bodies, which should be proactive and independent in enforcing their rules to prevent violations of personal data.

The current legislation fails to address the right to proper redress and remedy when violations of privacy occur. More worrying yet, as far as we know, there has been no judicial ruling or court decision that punishes violations of these data protection standards, 16 years after the law came into enforcement. Along the same lines, there is no clear mechanism for tracking the status of cases referred to the judiciary, including those cases referred by the INPDP.

In November 2017, Tunisia became the 51st member state to sign onto the Council of Europe's Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data. The country has also ratified the protocol amending the Convention.[135] In adopting Convention 108, Tunisia has an obligation to ensure the Convention is fully and effectively enforced by reforming its domestic data protection law to adhere to best practice guidelines set out in Convention 108.

Accordingly, in March 2018, Tunisia introduced a new draft law on the protection of personal data to replace the outdated 2004 law. The bill is modeled on and reflects key principles of the EU's General Data Protection Regulation (GDPR) and mandates that any party who processes personal data adheres to the principles of transparency, fairness, and respect for human dignity. The bill also extends protection requirements to non-Tunisian processors of personal data in the country. The 2018 draft law has a number of other improvements to the law in force. For example, the text extends the concept of personal data to online activities and information such as computer and device Internet Protocol (IP) address, GPS coordinates, email address, biometric data, and more.

The draft bill also seeks to appoint data protection officers within the various institutions charged with handling and protecting personal data. However, the definition of personal data does not distinguish between personal information and public data, which inadvertently could harm the right to access information. It is essential to reach a balance between the two rights in order to ensure the

[135] Legislation Tunisia, P. (2017). *Ratifying the accession of the Republic of Tunisia to convention n°108 of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal data and its additional protocol n°181 regarding supervisory authorities and trans-border data flow.* Retrieved January 10, 2021, from http://www.legislation.tn/en/content/ratifying-accession-republic-tunisia-convention-n%C2%B0108-he-council-europe-convention-protectio

principles of transparency and accountability, a point highlighted by Imed Hazgui, the former Head of the Access to Information Authority.[136]

While Tunisia continues to strive for political and legal reforms as a new democracy, it's more urgent than ever to prioritize issues related to privacy and data protection. Due to the lack of political stability, serious data protection violations could serve to threaten the ongoing democratic transition in Tunisia in the wake of the 2011 revolution. This issue manifested during the presidential and legislative elections of 2019, when political candidates exploited the personal data of Tunisian citizens, such as their ID card numbers, names, and signatures, to obtain "endorsements" without the explicit consent of the individuals concerned.[137]

The violations of the right to privacy and lack of transparency are not limited to the government and public institutions only, but also involve the private sector, Information and Communications Technology (ICT) companies, and Internet Service Providers (ISPs). According to the INPDP annual activity report, data processors such as private companies rarely engage with the INPDP to claim their own processing in compliance with the law.[138]

The lack of proper enforcement in Tunisia has led to major scandals involving personal data. In 2016, the Ministry of Interior submitted a bill requiring citizens to replace existing identity cards with a chip-enabled biometric one (biometric ID).[139] This proposal was massively criticized by civil society organizations as the new ID would allow for substantial privacy violations and abuses of personal data as well as increased surveillance, tracking, and storage of citizens' health and banking data.[140] The draft law didn't include or even reference any procedural or sufficient safeguards or limitations on what kind of data will be collected and how this large database of citizens' personal information will be used. The biometric ID card would also have granted officials unrestricted access to rich data profiles that could be misused and turned against citizens. While this draft law was withdrawn in 2018 in response to the concerns raised by INPDP and Tunisian human rights groups, we fear it is likely to resurface.

---

[136] Access Now. (2018, November 13). *Tunisia: Recap of Open Debate on Data Protection & Access to Information* (in Arabic). Retrieved January 10, 2021, from https://www.accessnow.org/%D8%AA%D9%88%D9%86%D8%B3-%D8%AD%D9%88%D8%B5%D9%84%D8%A9-%D8%AD%D9%88%D9%84-%D8%A7%D9%84%D9%84%D9%82%D8%A7%D8%A1-%D8%A7%D9%84%D8%AA%D9%81%D8%A7%D8%B9%D9%84%D9%8A-%D8%AD%D9%88%D9%84-%D9%85%D8%B4%D8%B1/

[137] Access Now. (2019, October 13). *Tunisia: Falsified endorsements in the presidential elections. What happens next?* Retrieved January 10, 2021, from https://www.accessnow.org/tunisia-falsified-endorsements-in-the-presidential-elections-what-happens-next/

[138] *Ibid*.

[139] Access Now. (2020, June 16). *National Digital Identity Programmes: What's Next?* Retrieved January 10, 2021, from https://www.accessnow.org/national-digital-identity-programmes-whats-next/

[140] Access Now. (2016, December 02). *Tunisia: Statement on Proposed National ID Card.* Retrieved January 10, 2021, from https://www.accessnow.org/tunisia-statement-proposed-national-id-card/

The current extraordinary circumstances of the global health crisis could serve as cover for the Tunisian government to prioritize and pass legislation that lacks transparency and openness, as in the case of the National Unique Identifier Decree. The decree was issued in May 2020 by the former Prime Minister Elias Al-Fakhakh, in collaboration with the Minister of Local Affairs and the Minister of Communication Technologies and Digital Transformation. The government classified it as one of the top priorities for dealing with the COVID-19 crisis, even though the text contains ambiguities that could lead to significant security risks.[141] The decree seeks to integrate information on Tunisian people that exists in various administrative services, but does not include specific details to show whether the government will use a centralized database to collect and store personal data on citizens.

2. Case studies

1) Cell site location tracking and conflicting statements

On June 14, 2020, former Prime Minister Elyes Fakhfakh announced in a live interview that a special government operations unit called "Operations Hall" used cell site location tracking or what he called "location and movement tracking through SIM cards" during the COVID-19 lockdown.[142] After backlash from citizens on Twitter,[143] Fakhfakh claimed that his government didn't engage in any illegal surveillance activities and that all tracking operations were performed in collaboration with the National Data Protection Commission (INPDP).

Chawki Gaddes, president of the INPDP, reacted by denying that the commission had any knowledge of the use of such surveillance technology.[144] The next day, Gaddes changed his earlier statement, stating that the government actually requested the use of software called "Al-Manara," which is based on cell site location tracking, and that it was granted permission to do so as long as citizens' personal data are anonymized.[145] Aside from the conflicting statements, it is unclear if the INPDP has the

[141] Access Now. (2020, July 14). *What is Tunisia's unique identifier, and why is it being pushed now?* Retrieved January 10, 2021, from https://www.accessnow.org/what-is-tunisias-unique-identifier-and-why-is-it-being-pushed-now/
[142] Attasia. (2020, June 15). *Interview with the former Prime Minister, Elyes Al-Fakhfakh* (in Arabic). Retrieved January 10, 2021, from https://www.youtube.com/watch?v=GnXTBtWDBRg
[143] A tweet from the former Prime Minister, Elyes Al-Fakhfakh (in Arabic). Retrieved January 10, 2021, from https://twitter.com/ElyesFakhfakh/status/1272279318467674115?s=20
[144] Mosaique FM. (2020, June 14). *The Independent Personal Data Protection Authority: We're not aware of monitoring citizens' phones* (in Arabic). Retrieved January 10, 2021, from https://www.mosaiquefm.net/ar/%D8%AA%D9%88%D9%86%D8%B3-%D8%A3%D8%AE%D8%A8%D8%A7%D8%B1-%D9%88%D8%B7%D9%86%D9%8A%D8%A9/755697/%D9%87%D9%8A%D8%A6%D8%A9-%D8%AD%D9%85%D8%A7%D9%8A%D8%A9-%D8%A7%D9%84%D9%85%D8%B9%D8%B7%D9%8A%D8%A7%D8%AA-%D8%A7%D9%84%D8%B4%D8%AE%D8%B5%D9%8A%D8%A9-%D9%84%D8%A7-%D8%B9%D9%84%D9%85-%D9%84%D9%87%D8%A7-%D8%A8%D9%85%D8%B1%D8%A7%D9%82%D8%A8%D8%A9-%D9%87%D9%88%D8%A7%D8%AA%D9%81-%D8%A7%D9%84%D8%AA%D9%88%D9%86%D8%B3%D9%8A%D9%8A%D9%86
[145] Acharaa. (2020, June 15). *Internal conflict: Independent Personal Data Protection Authority* (in Arabic). Retrieved January 10, 2021, from https://acharaa.com/uncategorized/%D8%AA%D8%B6%D8%A7%D8%B1%D8%A8-%D8%A8%D9%8A%D9%86-%D9%87%D

necessary technical capacity to review the tracking technologies and to guarantee the anonymization of citizens' personal information.

2) Robots and drones used to patrol the streets of Tunisia to enforce COVID-19 lockdown

Since March 2020, at the onset of the COVID-19 outbreak, the Tunisian Ministry of Interior has used robots and thermal imaging cameras to monitor citizens' compliance with social distancing measures.[146] Tunisian company Enova Robotics signed an agreement with the Ministry of Interior to start operating surveillance robots called "PGuard" and nicknamed "robo-cops" by local media.[147] These robots are equipped with a set of infrared cameras.

The number of the Tunisian-built surveillance robots deployed on the streets is unknown. The manufacturer, Enova Robotics, told the BBC it was a confidential matter. One robot, however, was spotted patrolling and interrogating citizens in the streets in Tunisia's capital city, Tunis.[148] In addition, the Ministry of Health received on April 23, 2020 four drones equipped with thermal cameras and speakers as a donation from a Tunisian private company called Telnet Holding.[149]

The Ministry of Health tested the use of drones in the Tunisian town of Sidi Thabet, Ariana. On June 2, 2020, the Ministry of Health signed a cooperation agreement with the Ministry of Agriculture to use the drones together "in support of the efforts of the Ministry of Health to confront the COVID-19 pandemic, by conducting large-scale scans to measure the temperatures of citizens to the extent of a 7-kilometer diameter and to broadcast awareness messages on speakers."[150] The text of the agreement is not public.

9%8A%D8%A6%D8%A9-%D8%AD%D9%85%D8%A7%D9%8A%D8%A9-%D8%A7%D9%84%D9%85%D8%B9%D8%B7%D9%8A%D8%A7%D8%AA-%D8%A7%D9%84%D8%B4%D8%AE%D8%B5%D9%8A%D8%A9/

[146] BBC. (2020, April 03). *Coronavirus: Tunisia deploys police robot on lockdown patrol.* Retrieved January 10, 2021, from https://www.bbc.com/news/world-africa-52148639

[147] Official Facebook page of Tunisian Ministry of Interior. (2020). *The Tunisian Ministry of Interior uses modern technologies to implement public health ban measures* (video in Arabic). Retrieved January 10, 2021, from https://www.facebook.com/ministere.interieur.tunisie/videos/1106579619691659/?v=1106579619691659

[148] *Ibid*.

[149] Jawhara FM. (2020). *In response to COVID-19: "Telnet" donates four drones to the Ministry of Health* (in Arabic). Retrieved January 10, 2021, from https://www.jawharafm.net/ar/article/%D8%AA%D8%A7%D9%84%D9%86%D8%A7%D8%AA-%D8%AA%D8%AA%D8%A8%D8%B1%D9%91%D8%B9-%D8%A8%D8%B7%D8%A7%D8%A6%D8%B1%D8%AA%D9%8A-%D8%AF%D8%B1%D9%88%D9%86-%D9%84%D9%88%D8%B2%D8%A7%D8%B1%D8%A9-%D8%A7%D9%84%D8%B5%D8%AD%D8%A9-%D9%84%D9%84%D8%AA%D8%B5%D8%AF%D9%8A-%D9%84%D9%81%D9%8A%D8%B1%D9%88%D8%B3-%D9%83%D9%88%D8%B1%D9%88%D9%86%D8%A7/105/165554

[150] Official Facebook page of Tunisian Ministry of Health. (2020). *Cooperation agreement between the Ministry of Health and Ministry of Agriculture to use drones in investigating the Coronavirus* (in Arabic). Retrieved January 10, 2021, from https://www.facebook.com/santetunisie.rns.tn/photos/a.186499378055841/3146685808703835/?type=3&theater

Allegedly, Telnet Holding acquired the drones from China. The company claimed on Facebook they are the same drones used in Wuhan.[151] Similar to the robots, there is no public information available about the drones' technology and capabilities. There were no comments by the INPDP, and it is unclear if the INPDP was consulted before the deployment of these drones.

IV. DATA PROTECTION AND COVID-19

Since late 2019, the world has been fighting the COVID-19 pandemic, and in response, governments in the MENA region and across the world have rushed to use technology, such as contact-tracing applications and geo-location tracking, in their efforts to contain and stop the spread of the virus. Not only is there a lack of scientific evidence to show the use of such applications are effective as a public health measure, they pose grave risks for privacy and data protection.

Chart: How well do MENA contact tracing apps protect data and privacy?

In an effort to mitigate the privacy dangers associated with use of these technologies, Access Now published key privacy and data protection recommendations for governments, including a list of dos and don'ts for privacy-respecting COVID-19 contact tracing apps.[152] In the table below, we provide an overview of the contact-tracing apps deployed in Jordan, Lebanon, Palestine, and Tunisia based on these dos and don'ts. In the section below, we provide more detailed information for each country.

Requirement	Ma3an (Lebanon)	Aman (Jordan)	Amankom (Palestine)	Men Ajlekom (Palestine)[153]	E7mi (Tunisia)
Voluntary/ Mandatory	Voluntary	Mandatory	Voluntary	Mandatory	Voluntary
Open source/ Closed source	Open source	Closed source	Closed source	Closed source	Closed source
Decentralized/ Centralized	Centralized	Decentralized	Unknown	Unknown	Centralized

[151] Telnet Holding official page on Facebook. (2020). Retrieved January 10, 2021, from https://www.facebook.com/telnet.holding.tn/posts/207318817354557

[152] Access Now. (2020, March). *Privacy and public health: the dos and don'ts for COVID-19 contact tracing apps.* Retrieved January 10, 2021, from https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf

[153] This application is a GPS tracking app of COVID-19 patients, and not a contact tracing app. We enlisted it here to demonstrate how problematic it is.

Privacy policy and user consent integrated in the app	Yes	Yes	Yes	Unknown	Yes
Use of anonymized data	Yes	Yes	No	Unknown	Yes
Bluetooth and/or location data	Bluetooth Might require location data on Android devices.	Location data	Bluetooth and location data	GPS	Bluetooth
Storage secured through encryption	Yes	Yes	Unknown	Unknown	Yes
Proportionate data retention mandates	Yes "Contact data stored on the device is automatically deleted after 21 days. We will delete all data in the data store after the COVID-19 pandemic has concluded."	Partially Data automatically deleted after 14 days for non infected users, data retention for exposed or infected users unknown.	Unknown	Unknown	Partially Data automatically deleted after 14 days for non infected users, data retention for exposed or infected users unknown.

JORDAN

On May 20, 2020, Jordan launched a new app called "Aman" (meaning "safety" in English) as part of the strategy to slow and eventually control the spread of COVID-19. The partnership to develop the app included the Ministry of Health, the Prime Minister's Office, private company Delivery Associates

Digital, and "a group of tech-savvy volunteers who aim to leverage Jordan's tech talent in fighting the coronavirus pandemic," named Jotech Community.[154]

The app relies on Bluetooth geolocation (GPS) coordinates and requests permission to access physical movement data — which determines whether a person is walking, running, biking, or driving a car — and for how long the person has stayed in the vicinity of a certain geographical location. Aman stores such data locally on the user's device and delivers a file containing the infected person's data covering 14 days prior to the date of confirmed infection to an employee from the Ministry of Health, and uploads the data afterwards to the Ministry of Health server.

The app does not rely on open-source protocols which hinders the ability to understand how it functions and the extent to which its design reflects commitment to respect the right to privacy and information security.[155]

While the app was voluntary to download at the early stages of the COVID-19 outbreak, it later became compulsory for the public and private sectors, as well as passengers traveling to and from Jordan. Those who visit government departments or institutions are also obliged to download the app. On August 11, 2020, the government stressed in a circular from Prime Minister Omar Al-Razzaz to all ministries, institutions, and government departments, that all necessary measures will be taken to prevent visitors from entering government departments without activating the contact-tracing app. An employee from each institution was also assigned to download the app for all staff employed in government departments. Al-Razzaz additionally requested all ministries, institutions, and government departments to provide him with a weekly report on the extent to which employees and visitors comply with the new requirements and obligations.[156]

LEBANON

The Lebanese authorities have also turned to technology in response to the pandemic. The Ministry of Public Health, in partnership with the Faculty of Health and Sciences at the American University of Beirut (AUB), launched in September 2020 the app "Ma3an" (meaning "together" in English), which

[154] Official website of the contact-tracing app "Aman." Retrieved January 10, 2021, from https://amanapp.jo/en/page/8/AboutAman

[155] JOSA. (2020, August 30). *Contact Tracing Apps Must Respect Privacy and Digital Security Principles.* Retrieved January 10, 2021, from https://jordanopensource.org/blog/24/contact-tracing-apps-must-respect-privacy-and-digital-security-principles

[156] Addustour. (2020, August 11). *Circular from Prime Minister Omar Al-Razzaz regarding "Aman" the contact tracing app* (in Arabic). Retrieved January 10, 2021, from https://www.addustour.com/articles/1165890-%D8%AA%D8%B9%D9%85%D9%8A%D9%85-%D9%85%D9%86-%D8%A7%D9%84%D8%B1%D8%B2%D8%A7%D8%B2-%D9%84%D9%84%D9%85%D9%88%D8%B8%D9%81%D9%8A%D9%86-%D9%88%D8%A7%D9%84%D9%85%D8%B1%D8%A7%D8%AC%D8%B9%D9%8A%D9%86-%D8%AD%D9%88%D9%84-%D8%AA%D8%B7%D8%A8%D9%8A%D9%82-%D8%A3%D9%85%D8%A7%D9%86%D8%8C

uses Bluetooth technology to alert users when they have come in close contact with other users who have tested positive for COVID-19. The app collects "contact data," which includes an encrypted user ID, random and temporary server-generated codes, the Bluetooth signal strength of other users of the app with whom a user comes into contact, and the date and time of contact.[157]

According to an initial static analysis performed by the digital security team of SMEX, the app collects minimal personal data, but has security flaws. For example, the app lacks encryption and leaves users of older Android phones potentially susceptible to a zero-day vulnerability. Many files in the application are hard-coded, meaning that sensitive and confidential information, including the administrator's usernames and passwords, may be accessible to malicious third-party actors.[158]

TUNISIA

With the outbreak of COVID-19, the Tunisian government rushed to technology-based solutions as a measure to control the transmission of the virus. Within the framework of a public-private partnership (PPP), the Ministry of Health's National Center of New and Emerging Diseases has signed a contract with a start-up company named Wizzlabs to deploy a contact tracing app named "E7mi" (meaning "protect" in English).

On July 24, 2020, the INPDP confirmed in a press release that it authorized the app's data collection and processing without indicating whether they performed any technical assessments of the application.[159] Access Now filed an access to information request about the E7mi app, first to then Minister of Health Abdellatif Mekki in July 2020, and then as a reminder to interim Minister Mr. Mohamed Habib Kchaou in August 2020.[160] We requested to have a copy of the consultation conducted between the Ministry of Health and INPDP regarding the compliance of the E7mi app with the requirements of the Law on the Protection of Personal Data of 2004, as well as a copy of the contract concluded between the startup company, Wizzlabs, and the Ministry of Health concerning the terms and conditions for using the E7mi app.[161]

After 20 days had passed — the maximum period that the government has to respond to a formal request for access to information under Article 14 of Organic Law No. 2016-22 — we received no

[157] Lebanese Ministry of Public Health. (2020). *"Ma3an" Together Against Corona* (in Arabic). Retrieved January 10, 2021, from https://moph.gov.lb/en/ma3an
[158] SMEX. (2020, September 17). *Security Concerns with Lebanon's New Contact Tracing App.* Retrieved January 10, 2021, from https://smex.org/security-concerns-with-lebanons-new-contact-tracing-app/
[159] Independent Personal Data Protection Authority. (2020). *Press statement* (in Arabic). Retrieved January 10, 2021, from https://www.facebook.com/INPDP.TN/photos/a.880606318675657/3142913009111632/?type=3&theater
[160] Access Now. (2020, September 18). *To safeguard privacy, Tunisia must be transparent on tech used to fight COVID-19.* Retrieved January 10, 2021, from https://www.accessnow.org/to-safeguard-privacy-tunisia-must-be-transparent-on-tech-used-to-fight-covid-19/
[161] *Ibid*.

answer to our request, nor did we get a notice to show sufficient legal grounds to prevent sending us a reply.

PALESTINE

Amid COVID-19, the Palestinian Authority (PA) launched a number of closed-source contact-tracing and location tracking apps with little to no transparency. In June-July 2020, according to testimonies shared with us through 7amleh, Palestinian students going back home from abroad had an application downloaded forcefully on their mobile phones by Palestinian security forces at the borders. The name of the application is not confirmed as students were not informed on the app; rather, security forces took their phones and downloaded it themselves. Some of the students reported that it was downloaded from a Chrome browser and not from an app store, and that it may have been called "Men Ajlekom" (meaning "for you" in English).

According to our research, we believe it may be the same application reported in August 2020 by a Palestinian citizen, who upon being tested positive for COVID-19 received a WhatsApp message from the Ministry of Health in Palestine with as an Android Package (APK) file to download.[162]

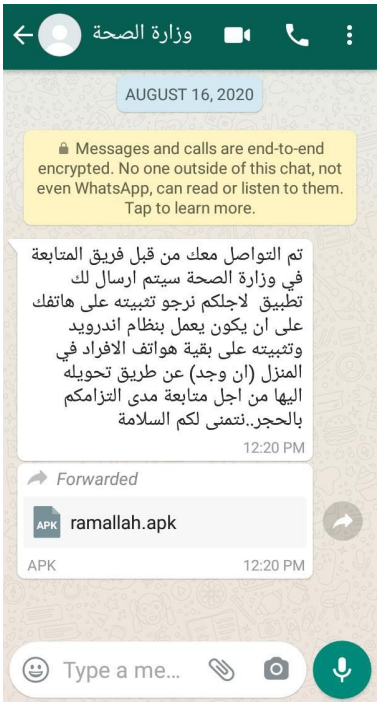

Figure 2. *Screenshot of the WhatsApp message sent from the Ministry of Health in Palestine with the APK file.*

Translation: "You have been contacted by the follow-up team at the Ministry of Health. An application will be sent to you. Please install it on your phone, provided that it works on an Android system, and install it on the phone of all persons' phones at home (if applicable) by forwarding the file in order for us to monitor your compliance to the quarantine...We wish you safety."

[162] APK is the package file format used by the Android operating system, and a number of other Android-based operating systems for distribution and installation of mobile apps.

We obtained a copy of the APK file from 7amleh. We investigated it via Apktool,[163] and found that the above-mentioned app is indeed called "Men Ajlekom," and it requires permissions to collect data from the phone via device location. The app was developed by the Palestinian security forces and it aims to monitor COVID-19 patients' movements and their compliance with home quarantine rules.[164] Even though the head of the cyber unit in the Palestinian Preventive Security stated that the app was developed according to "international standards,"[165] there has been no transparency about the technology used or the app's privacy policy.

When conducting our research in September 2020, we found a page on the website of the Ministry of Health about a COVID-19 tracing application called "Manee'" (or "immune" in English). According to a terms of service (ToS) and privacy document, the app uses Bluetooth and GPS.[166] However, we were not able to locate a link to download the app, nor did we find it on the Apple or Google app stores. Privacy is mentioned in one paragraph in the ToS as "one of the Ministry's top priorities," but with no further details or information. By October 2020, the page couldn't be reached which led us to think the project was eventually abandoned.[167]

On October 26, 2020, however, the Ministry of Health announced the launch of a new contact-tracing application called "Amankom" (or "your safety" in English).[168] The app relies on Bluetooth technology and according to the Ministry of Health, the data collected are stored on the phone.[169] The link to download the app directs to downloading an APK file. The application was also available on the Play Store and Apple App Store, with more than 5,000 downloads by November 2020.

As we analyzed the app's APK file on Apktool, we found Amankom is a new name or a new version of the "Manee3" app which requires permissions to collect data via Bluetooth and GPS.

---

[163] An open source tool that enables decoding android app resources.
[164] Alghad. (2020, July 15). *Palestine develops a contact tracing app to control the spread of COVID-19*. Retrieved January 10, 2021, from https://www.alghad.tv/%D9%81%D9%84%D8%B3%D8%B7%D9%8A%D9%86-%D8%AA%D8%B7%D8%A8%D9%8A%D9%82-%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A-%D9%84%D9%85%D8%B1%D8%A7%D9%82%D8%A8%D8%A9-%D8%A7%D9%84%D9%85%D8%B5%D8%A7%D8%A8/
[165] *Ibid*.
[166] Ministry of Health in Palestine. (2020). *Terms of service of using contact tracing app* (in Arabic). Retrieved January 10, 2021, from http://site.moh.ps/Content/File/kwGvJ8oDcPxnQBaKgvwTL5af_EzMT7VqDTzoCvRwN66FEthB7.pdf
[167] Official website of the Palestinina Ministry of Health. Retrieved January 10, 2021, from http://site.moh.ps/index/ArticleView/ArticleId/4976/Language/ar#
[168] Akhbar Elyom. (2020). *"Amankom" a contact tracing app to monitor the spread of COVID-19 in Palestine* (in Arabic). Retrieved January 10, 2021, from https://akhbarelyom.com/news/newdetails/3144846/1/-%D8%A3%D9%85%D8%A7%D9%86%D9%83%D9%85-..-%D8%AA%D8%B7%D8%A8%D9%8A%D9%82-%D8%B0%D9%83%D9%8A-%D9%81%D9%8A-%D9%81%D9%84%D8%B3%D8%B7%D9%8A%D9%86-%D9%84%D8%B1%D8%B5%D8%AF-%D9%81%D9%8A%D8%B1%D9%88%D8%B3-%D9%83%D9%88%D8%B1%D9%88%D9%86%D8%A7
[169] Ministry of Health in Palestine. (2020). *"Amankom" contact tracing app* (in Arabic). Retrieved January 10, 2021, from moh.ps/mohsite/index/Amankom/Language/ar

Even if the Ministry of Health alleges through the scarce available public information that the contact tracing is based on Bluetooth technology, our sources in Palestine tested the application and confirmed that it wouldn't open if it was not also granted permission to the device's location. The Ministry of Health does not explain why the app requires access to the device's location.

The Ministry of Health publishes a privacy policy for the app on its website.[170] However, the privacy policy fails to provide specific essential information such as what information is collected, who can access it, and how it will be used, nor does it include a sunset clause for its use. The Ministry instead mentions that "all user data will be deleted after the end of the coronavirus pandemic, with the Palestinian Ministry of Health announcing that it has ended in Palestine."[171]

Furthermore, under a section titled "How the app and privacy policy works," there is a mention of "secure and encrypted servers" with no reference to security and privacy safeguards which would ensure that the connection between the users and the servers is also secure and encrypted. The network security configuration of the app permits clear text traffic, which is not surprising as the app links to a few resources on the official website of the Ministry of Health, which is also not secured.

V. POLICY RECOMMENDATIONS

Access Now has been working on data protection policy and legislation from our founding in 2009, and it continues to be one of our highest global and regional priorities. Our policy recommendations below stem from our experiences working on privacy and data protection legislation across the globe, digital identity programs, and, most recently, our work on privacy during the COVID-19 global pandemic.

For states	
1. Adopt comprehensive data protection law centered around people's rights	Lawmakers in the region must prioritize the adoption of robust data protection legal frameworks that center the fundamental rights of users over the economic interest of the government and private companies. To that end, we developed a guide for lawmakers, ***Creating a Data Protection Framework: A Do's and Don'ts Guide for Lawmakers***, building on our experience and lessons from the EU's General Data Protection Regulation (GDPR).[172]

[170] *Ibid*.
[171] *Ibid*.
[172] Access Now. (2018, November). *Creating a Data Protection Framework: A Do's and Don'ts Guide for Lawmakers — Lessons from the EU General Data Protection Regulation.* Retrieved January 10, 2021, from https://www.accessnow.org/cms/assets/uploads/2019/11/Data-Protection-Guide-for-Lawmakers-Access-Now.pdf

	A framework aiming to protect personal data and guarantee users' agency and control over their personal information must include binding rights for users, including their right to explicit consent, object, erase, rectify, and access their data. Most importantly, governments must ensure there are open, transparent, and inclusive consultations at the initiation of any reform or adoption of such frameworks to avoid creating weak laws counterproductive to their purpose. In all stages, meaningful participation from civil society groups must be ensured.
2. Establish an independent data protection authority and robust mechanisms for enforcement	No data protection framework, no matter how great, can be complete without a robust enforcement mechanism which includes the creation of an independent data protection authority (DPA) or commission. The authority must have the powers, resources, and expertise to monitor implementation, launch investigations, and sanction entities in case of data protection violations and negligence. The management and functions of the DPA must be disconnected from the executive authority and security agencies.
3. Avoid broad data protection exemptions and privacy limitations for national security	National security agencies in the MENA region often restrict and violate citizens' right to privacy under the pretext of safeguarding national security and fighting terrorism. Those agencies usually operate in secrecy and without oversight. Therefore, data protection and privacy laws and regulations should not provide exemptions for national security agencies. Any access granted to users' personal data must follow the principle of necessity and proportionality.
4. Institute "privacy by design" principles in any data processing programs or proposals	National digital ID, biometric passports, government e-services, and similar programs are data heavy, both during enrollment and when transactions are regularly authenticated. Any data that are shared, especially sensitive and personally identifiable information (PII), raise significant risks for privacy and data protection. Therefore, it is of utmost importance that governments adhere to the concept of data protection by design and by default. Engineers must ensure that privacy and data protection are considered both in the initial design phase of product and services and throughout their

	deployment and use, and that they are set to the highest standards of privacy safeguards.
5. When rolling out biometric and digital identity programs, governments must ensure that:[173]	• The scope of use for digital ID programs are explicitly and clearly defined and restricted, provided for in the law, and explain the use to the public. • The enrollment and use of the digital ID is voluntary. It should not be a requirement for citizens to access government services such as healthcare and education. • Data collection and storage are not centralized. Centralized data collection and storage for a national digital ID creates a single point of failure and poses grave risks and therefore should be avoided. • A secure and strong technology infrastructure as well as a cybersecurity framework is in place.

For private companies
• Publish a formal and clear commitment to protect and respect the right to privacy and personal data.
• Release regular transparency reports that disclose law enforcement requests for user information, threats to privacy, and surveillance. These reports should also provide information on the company's process for responding to those requests and notifying affected consumers, and help identify risks to privacy.
• Comply with data protection and privacy regulations where applicable, as they also provide basic instructions on the collection and processing of personal data.
• Provide effective, rights-compatible grievance mechanisms for users to raise concerns early and openly about violations to their privacy.

[173] For a comprehensive framework for national digital identity programs, check our key policy recommendations in our working paper: Access Now. (2018). *National Digital Identity Programmes: What's Next?* Retrieved January 10, 2021, from https://www.accessnow.org/national-digital-identity-programmes-whats-next/

For international organizations	
Key international organizations have been using biometric technology which collects biometric data for the identification and authentication of refugees, with the justification that it makes the delivery of humanitarian aid and cash payments more efficient and accurate, preventing fraud and promoting accountability. However, as we highlighted previously in the report, the collection and use of biometric data poses significant risks for individuals. Given the high risk for exploitation of these data, and the irreparability of breaches, Access Now calls for a moratorium on the collection and use of biometrics (including facial recognition) for authentication purposes.[174] Requiring individuals to provide their unchangeable and personal biometric data at great risk to privacy should be a measure of last resort.	
1. Ensure that providing biometric identifiers is voluntary and opt-in, not a mandatory measure	Individuals, particularly from vulnerable and marginalized communities, must not be coerced to provide their biometric identifiers as a precondition for receiving aid or services. The use of biometric and digital ID programs must be based on the users' agency and informed consent. Creating mandatory registration or enrollment based on a single identity program can exacerbate the risk of exclusion, profiling, and surveillance. Instead, multiple voluntary identification and authentication frameworks must be promoted and implemented.
2. Conduct human rights impact assessments, ex ante and ex post	Humanitarian organizations must ensure that their technology in use is built on a foundation which protects the fundamental rights of users, particularly their right to privacy. Human rights impact assessments should be conducted before deployment, during implementation, and throughout the life cycle of these programs.
3. Do not create centralized databases of individuals' biometric data	Given the sensitivity of biometric information, we recommend such data are stored in a decentralized manner. A centralized database creates a single point of failure, and therefore can be more vulnerable to threats and attacks.

[174] See our #WhyID open letter to the leaders of international development banks, the United Nations, international aid organizations, funding agencies, and national governments on the use of digital ID programs: https://www.accessnow.org/whyid/

4. Provide transparency in terms of disclosure of cybersecurity policies	Steps must be taken to ensure that the cybersecurity policies and principles developed to safeguard the digital identity infrastructure are disclosed to the public. Given the public importance and scale of such projects, these disclosures must be made as a matter of a right to citizens. Additionally, such practices would encourage review of the policies by experts and other stakeholders. This would inform the government, open up issues for consultations, and lead to the development of more robust cybersecurity policies and a more secure ecosystem as a whole.
5. Conduct mandatory human rights impact assessments and due diligence processes for every public-private partnership	Private companies entrusted with the sensitive personal data of millions of people must be vetted for their respect and protection for human rights through a comprehensive due diligence process. Public-private partnerships must also be transparent and follow open and transparent public procurement procedures, open contracting, and transparency reporting, and be made available to the public.
6. Minimize data collection and transfers	Those creating digital ID initiatives must minimize the collection and transfer of data associated with biometric identifiers. This can reduce risks and harm if the data are compromised. We recommend in general that developers employ on-device authentication when biometric identifiers are used as “passwords,” rather than using centralized cloud storage/authentication.

V. CONCLUSION

Our analysis of legal frameworks and the examples we present in this report make a clear and urgent case for national governments in the MENA region to prioritize the adoption of robust and strong data protection legislation that centers users' rights, grants them autonomy and choice over their personal information, and protects their privacy against surveillance and exploitation for profit, as well as unlawful or accidental threats, hacks, and breaches. Governments must ensure they conduct public, transparent, and inclusive consultations with all relevant stakeholders when developing data protection laws, and particularly with NGOs and civil society. To this end, Access Now welcomes the opportunity to collaborate and work alongside policy makers in the region to advance and protect the right to privacy and data protection in the region.

This is only the first step, however. Enforcement of the legislation is key to success. Governments, the private sector, and international organizations that collect and process citizens' personal data share the responsibility to protect personal data and provide transparency on how personal data are collected, used, stored, and shared — and with whom. We encourage and welcome our readers, and especially investigative journalists and civil society organizations, to further investigate and unearth data protection violations and exploitation across the region, as a necessary step to bring these cases to light and defend digital rights in the MENA region.