PRIVACY INTERNATIONAL

State of Privacy Lebanon

January 2018

Table of contents

Introduction

Acknowledgment

The State of Privacy in Lebanon is the result of an ongoing collaboration between Privacy International and SMEX.

Key privacy facts

1. Constitutional privacy protection: The Lebanon constitution does not explicity mention the right to privacy.

2. Data protection law: Lebanon does not have an explicit data protection law.

3. Data protection authority: Lebanon does not have a data protection authority.

4. Recent scandals: EFF recently reported that malware-infected messaging apps have been operating since 2012, possibly involving a nation-state actor.

5. ID regime: Biometric passports and residence permits are being issued without a clear legal framework being in place.

Right to Privacy

The constitution

The Constitution of Lebanon does not explicitly protect the right to privacy. Article 14 only protects the inviolability of the home, stating: «The citizen›s place of residence is inviolable. No one may enter it except in the circumstances and manners prescribed by Law.»

Articles 8 and 13 of the Constitution indirectly guarantee individual liberty and freedom of expression, respectively. Some legal experts have interpreted that these laws could protect the secrecy of all means of communications, both mail and telephone calls, but this protection is not explicit.

Regional and international conventions

Lebanon is a signatory of a number of treaties with privacy implications, including:

- the Universal Declaration of Human Rights;
- the International Covenant on Civil and Political Rights;
- the International Convention on the Elimination of All Forms of Racial Discrimination (with the exception of Article 22);
- the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment;
- the Convention on the Rights of the Child;
- the International Covenant on Economic, Social and Cultural Rights;

- the International Convention for the Protection of All Persons from Enforced Disappearance;
- the Convention on the Rights of Persons with Disabilities;
- the United Nations Convention against Transnational Organized Crime;
- the Cairo Declaration on Human Rights in Islam; and
- the Arab Charter on Human Rights.

Communication Surveillance

Introduction

As of 2016, approximately 76 percent of Lebanese residents and citizens use the internet and there are 53.43 broadband subscriptions per 100 inhabitants. Following a decree from the Ministry of Telecommunication in July 2014, touch and Alfa, the two telecommunications companies in Lebanon, lowered broadband prices between 44 and 68 percent. Moreover, these companies also increased the capacity of broadband packages by almost 300 percent. After a one-day boycott of the two companies in 2017, Jamal Jarrah, the telecommunications minister, promised to lower the rates. In January 2018, users are able to purchase 500 MB for $10.

Surveillance laws

Telecommunication Interception Act

Several articles in a Lebanese law limit surveillance, but there is a gap between the law and its enforcement. In 1999 Lebanon was the first Arab country to introduce a legal framework for the interception of communications, with the Telecommunication Interception Act of 27 December 1999 (thereafter referenced as Law 140/1999), although the Cabinet did not adopt the law until 2009.

Law 140/1999 relates to the protection of secrecy of communications, stipulates that the right to secrecy of communications, both internal and external, wired or wireless (landlines and mobile of all types including mobile telephone, fax, electronic mails) is guaranteed and protected by law and cannot be subjected to any forms of tapping, surveillance, interception or violation except in cases of extreme urgency and upon obtaining a judicial or administrative order.

The judicial authorisation process, as outlined in Article 2 and Article 3 of the Law, states that interception may be authorised by court order in cases of emergency, provided the targeted individual is the suspect of a crime. The court order should specify the means of communication, subject matter of the procedure, the crime subject matter of the prosecution or the investigation, and the duration of interception, which may not exceed 2 months.

In accordance with Article 9, communications interception can also occur on the basis of the administrative authorisation of either the minister of interior or the minister of defence, after obtaining the approval of the Prime Minister in order to gather information aimed at combating terrorism, crimes against state security, and organized crime. To be lawful, such decisions must be approved in writing, duly justified and approved by the Prime Minister and should specify the means of communication, subject matter of the procedure, the subject matter of the prosecution or the investigation, and the duration of interception, which may not exceed two months.

Lebanese Code of Civil Procedures

Article 98 of the Lebanese Code of Civil Procedures regulates the regime regarding searches and seizures.

Electronic Transactions and Personal Data Law

In 2010, the Parliament proposed the draft Electronic Transactions and Personal Data Law, which was last amended in 2017, but remains a draft as of January 2018. It addresses issues including the regulation of electronic signatures, which is a legal issue; e-commerce transactions, which is a commercial issue; and respect for individual privacy and the protection of personal data.

At the time, civil society organisations raised concerns about Article 82 of the Bill which would allow for warrantless search and seizure of financial, managerial, and electronic files, including hard drives, computers, etc.

Data retention

An order by the Public Prosecutor›s office in 2013 required all internet service providers (ISPs), and some internet cafes that offer internet access, to retain the data of their users› activity for a period of one

year. The order instructed «all landline and wireless internet service providers for homes and companies and from all cafés and stores providing their clients with devices through which they can access the Internet» to «do whatever it takes to activate and save all Internet log files going through their servers and routers, and prepare a periodical backup copy to save these files from being lost, for at least one year.» The order also outlines the type of user data that must retained including the username, user›s IP address, the websites to which they connected, and the protocols used in the process, in addition to specifying the user›s location.

Surveillance actors

The Security Agencies

There are several state institutions with power to conduct surveillance and access user data, including the General Directorate of General Security; the Directorate of the Internal Security Forces (ISF); and the Army Intelligence Directorate. The General Directorate of General Secrutiy is overseen by the Ministry of Interior.

The General Directorate of General Security was founded in 1921, and became a branch of the Ministry of Interior in 1959. The Directorate not only gathers intelligence and attempts to uphold national security, but also «[participates] in judicial investigations within the limits of threats against internal and/or external state security.» Additionally, is also responsible for issuing passports and residence permits.

The General Directorate of Internal Security Forces (ISF) are the national police and security force of Lebanon. The Intelligence unit was founded in 1991 and under Law No. 17. It directly reports to the Ministry of Interior.

The Cybercrime and Intellectual Property Rights Bureau, established in 2006, officially operates under the umbrella of the ISF but its legality is contested, given that it was established under a memorandum of service rather than by Law or Decree. The Bureau has been accused of acting as a censorship authority, mainly targeting journalists, bloggers and online activists. Its powers raise concerns as to the lack of safeguards protecting privacy and regulating the powers of the Bureau. On 2 October 2016 the leadership of the bureau changed after, Major Suzanne Hajj Hobeiche, the former bureau chief who had regularly targeted bloggers and activists, was asked to step down. Major Albert Khoury, a former lieutenant colonel in the ISF, replaced her.

Surveillance capabilities

Spyware Software

In January 2018, EFF and Lookout reported that Dark Caracal, «a prolific actor with nation-state level advanced Advanced Persistent Threat (APT) capabilities» was being «administered» out of a General Directorate of General Security building in Beirut, and has been active since 2012. While it remains unknown if General Security is running Dark Caracal, EFF was able to conclude that it has extracted «hundreds of gigabytes of data» and targeted thousands of victims in 21 countries. EFF found that Dark Caracal has obtained data from both mobile and desktop devices, with a particularly advanced focus on Android mobile devices. Dark Caracal obtained access to these devices through more traditional hacking means (eg phishing, social media pages, physical access), and it developed a surveillanceware - which EFF dubbed Pallas - that has the capability to extract information including SMS messages, texts from private messaging apps, images, screenshots, audio recording, contacts, and WiFi access points and SSIDs. The operation also used malware, including kinds never before seen by EFF, that has targeted Windows, OS X and Linux systems. Dark Caracal also used the previously-known FinFisher: malware usually installed via email or a fake software update. In the past, researchers had only observed Finfisher attacks on Desktop devices, but EFF noted that it targeted mobile devices as well.

According to EFF, Dark Caracal›s targets did not fit under one umbrella, but included «military targets, utilities, financial institutions, manufacturing companies, and defense contractors» as well as «military personnel, enterprises, medical professionals, activists, journalists, lawyers, and educational institutions.»

Prior to the EFF report, a 2015 report from Citizen Lab at the University of Toronto revealed that both General Security and the ISF had used FinFisher.

The Bulk Collection of Telecommunications Data

Since March 2014, the Cabinet has given the ISF and other agencies unhindered access to telecommunications data for periods of between six months and one year. When the Cabinet first awarded the ISF access to this data, Judge Awny Ramadan, head of the Lebanese accountability agency, said that the blanket and arbitrary government requests for the communication data of the approximately 5 million Lebanese citizens violated Law 140/99 given that every single citizen cannot be a suspect of a crime. Also, the decision permitted full access for a period of six months, which is far beyond the two months permitted by the Law 140/99 under Article 9. In October 2017, the Cabinet again gave security agencies full, unrestricted access to the electronic communications data of all Lebanese citizens for four months, a shorter period than any other previously granted.

This form of authorization started in December 2012, when the Information Branch of the ISF sought the interception and retention of all SMS text messages sent in Lebanon from 13 September to 10 November 2012 as part of its investigation into the car bombing that had occurred on 19 October 2012 in Beirut, which killed Wissam Al Hassan, the head of ISF. 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, phone numbers, addresses, names, and passwords. Lebanon›s Telecommunications Minister, Nicolas Sehnaoui, refused the request but it was reported that the government nevertheless obtained access to this data.

The United Nations International Independent Investigation Commission (UNIIIC), and the Special Tribunal for Lebanon (STL), set up to investigate the assassinations that have taken place in Lebanon, and in particular that of the late Prime Minister Rafiq Hariri in 2005, have also taken advantage of communications interception powers to permit the ISF unregulated access to private data of Lebanese citizens from an array of sources including university archives, medical records, and mobile phone records. As of January 2018, there is at least one case pending before the Special Tribunal for Lebanon where the expansive access to user data is being challenged.

General Directorate of General Security›s Relationship with Hacking Team

In 2015, Wikileaks revealed that General Security had been exchanging emails with Hacking Team, a surveillance company, since 2012. In February 2015, General Security emailed Gamma Group, another offensive surveillance company, and Hacking Team, inquiring specifically about Hacking Team›s Galileo Remote Control System, which infects mobile devices and intercepts their communications. The firm produced a demo for the software and General Security later signed a 450,000 euro contract for hacking team to hack 50 individuals.

Internet Filtering System

In January 2013, Citizen Lab published a research brief in which it reported that researchers had discovered three Blue Coat PacketShaper installations in various countries including Lebanon. PacketShaper is a technology that allows for the surveillance and monitoring of users› interactions on various applications such as Facebook, Twitter, Google Mail, and Skype. While such tools can be used for legitimate aims, such as controlling bandwidth costs, they can be used for filtering, censorship, and surveillance. Citizen Lab noted they had identified two installations of PacketShaper. One was found on «a netblock associated with IncoNet Data Management.» An additional PacketShaper installation was identified by a Google search on a netblock associated with «Virtual ISP Lebanon» (VISP).» The discovery of the installations came as the government was drafting a regulation pertaining to the public morals of online content. Although this draft regulation was later abandoned, the researchers noted that this was a curious coincidence given that Lebanon did not have a history of internet filtering prior to the publication of the draft regulation.

Cameras in Beirut

In June 2016, 2,000 cameras were installed across 350 surveillance points as part of the Beirut Surveillance Project. The municipality approved the $33 million project in 2014 and the Beirut-based company Guardia Systems, a subsidiary of MG Holding, installed the cameras. Two control rooms with fifty operators monitor these cameras and two data centers are able to store up to 10,000 terabytes of video footage.

Surveillance oversight, checks and balances

The judiciary is tasked with overseeing surveillance practices under Article 16 of Law 140/99, but this rarely happens. Based on information Al-Akhbar, a Beirut-based media outlet, obtained from the retired President of the Court of Audits, it appears that the actual role of the judiciary in authorising or overseeing the administrative authorisation of interceptions is merely symbolic. In practice, the Prime Minister routinely circumvents the requirement for judicial authorisation by directly authorising intercepts himself.

As a safeguard against abuse, Article 16 stipulates that such administrative decisions must be verified by an independent judicial commission, which consists of the first president of the Court of Cassation, the president of the State Shura Council, and the president of the Court of Audits, or three judges from separate and independent judicial bodies.

Despite this safeguard, it seems this provision is not oftenrespected in practice. High-level judicial and parliamentary sources told al-Akhbar that «all security services, without exception, continue to illegally operate their own wiretapping divisions of unknown nature and scope…This means that there are no guarantees the security services are not eavesdropping on the Lebanese without any legal oversight.» In addition, the media outlet quotes a senior judicial source saying, «the security services themselves do not trust each other. If they all operated through the surveillance centre run by the Ministry of Interior in accordance with the law, everyone will be able to see what other security services are up to. Because they sometimes compete, away from national interests, each agency has its own ‹centre› away from the law.»

Surveillance case law

Examples of surveillance

Foreign agents

There have been reports of attempts by the Israeli government to recruit people to work with them through social media, particularly Facebook, and to infiltrate the Lebanese telecommunication system. On 12 December 2017, General Security posted a warning on its Facebook page advising users to beware of fake pages like LIOR ANONYMOUS TEAM, which it had claimed were associated with Israeli Mossad and actively trying to recruit Lebanese citizens. Furthermore, in December 2011, February and July 2012, and September 2014, the Lebanese authorities announced that they had discovered Israeli spying equipment, which the Israelis subsequently destroyed.

In 2012, Kaspersky Lab, a Russian multinational computer security company, published a report showing they had discovered Flame, a nation-state created malware, in Iran and various other countries in the Middle East and the majority of the infected machines were in Lebanon. The research was unable to determine whether the bank component of the malware was used to spy on financial/banking transaction or steal money.

Data Protection

Data protection laws

Lebanon does not have a law explicitly regulating the protection of personal data; thus, the legal framework for data protection is weak. Privacy is regulated by other various provisions including various articles in Law 140/99, Article 2 of the Banking Secrecy Law of 3 September 1956 (the Banking Secrecy Law), and the Penal Code under articles 579, 580, and 581 relating to the violation of secrets. The recent Right to Access Information Law «prevents public institutions from providing anyone with private and personal information about Lebanese citizens.» More specifically, Article 7 of the Code of Medical Ethics (Law no. 288 of 22 February 1994) protects the confidentiality of physician and patients relationships, and Articles 51 and 58 of the Consumer Protection Code (Law no. 659 of 4 February 2005) states that that suppliers must not disclose data without the consent of the consumer.

Law 431/2002, which regulates the telecommunications sector, does not address the protection of personal data at all.

The draft Electronic Transactions and Personal Data Law would be the most comprehensive law regarding personal data. The five chapters of Section V (General Provisions Concerning the Protection of Personal Data, Collection and Processing of Personal Information, Procedures Required for Processing, Right of Access and Correction and Penal Provisions) of the law address personal data issues. The law still has shortcomings; chiefly, it does not specify the cases where personal data processing is permitted and only mentions specific cases that would warrant an authorization. There is also no independent body to monitor implementation and compliance. Additionally, there is no specification about whether or not the Lebanese state can transfer data to foreign countries (i.e in a security agreement).»

Accountability mechanisms

On 19 January 2017, parliament ratified the Access to Information law, which, in theory, compels government agencies to «publish key documents such as an annual report, orders and decisions, and office expenditures» and allows both individuals and organizations to request and obtain access to government information. The law also proposed the creation of an Anti-Corruption Commission (ACC), but this still does not exist. This is a major issue because the law states that the ACC would rule on the requests that the government must fulfill and as long as the ACC does not exist, there is no independent body that is regulating these requests. When SMEX requested information about Inmobiles, the company contracted to register IMEI numbers, in August of 2017, the government did not respond.

Data breaches: case law

Our research has not yet identified any private related issues relating to examples of data breaches in Lebanon. Please send any tips or information to: research@privacyinternational.org

Examples of data breaches

Online voter registration

In May 2018, Lebanese citizens residing outside of Lebanon will be able to vote abroad for the first time.

On 20 November, voter registration closed with over 90,000 Lebanese registering to vote. Immediately after the closure of this registration period, Shada Wehbe, a social media trainer and blogger, noticed that the site for voter registration, Lebanese Diaspora Vote (LDV), was using cookies to track visitors without asking for their consent or providing any disclosure about what this data may be used for. Double-click, a company owned by Google, and Facebook›s Pixels owned the cookies attached to the LDV website. Both of these tools track users browsing habits.

American University of Beirut

In 2014, a hacker leaked information about the mismanagement of the American University of Beirut (AUB). The leaked information included data from American University Hospital (AUH), and the hacker confirmed to a reporter that they were able to access medical files from AUH, not just files about mismanagement. AUB itself had acknowledged that «the technical environment … is not secure.» Moreover, a third party, FTI consulting, also noted that the information systems adequately protect patients› private information.

Personal Cell Phone Numbers

Alfa and touch, the two state-owned mobile phone operators in Lebanon, sell users› data to businesses and advertising agencies. Whether users in Lebanon buy a prepaid or postpaid line, these two companies exploit their data. Neither company provides a service to opt-out from these messages, though users can block specific numbers. SMEX found that businesses pay $11,000 to send 500,000 SMS messages and $430 to send 360,000 emails on average. These messages are not always sent en masse, as touch identifies target groups based on usage behavior, enabling businesses to send targeted advertisements.

License Plates

Information linked to license plates numbers are leaked from the vehicle registration center on an annual basis. Some of this information includes names, addresses, phone number, dates of birth and license plates numbers. The data is leaked on CD-ROMs without any form of encryption.

In an investigative report produced by Al-Jadeed TV, «The Customs Rally: The Tax Evasions Race» exposed the ease in which these CD-ROMs can be purchased. Despite the privacy and security repercussions, the government has not taken any action to prevent these continuous leaks.

Identification Schemes

ID cards and databases

Biometric passports and residence permits

In 2013, the Directorate of General Security announced that it would start using biometrics passports as a result of a request by the United Nations agency International Civil Aviation Organization (ICAO). ICAO had notified the Directorate on 31 December 2012 and set a deadline of 24 November 2015 for all of its members to adopt biometric technologies. In August 2015, the government began issuing biometric passports. The Directorate stated that it waited until 2015 because various Lebanese embassies had received noticed that their host countries were only going to accept machine-readable passports going forward.

Inkript, a Lebanon-based subsidiary of Resource Group Holding (RGH), which submitted a joint offer with Gemalto, a digital security company with its headquarters in the Netherlands, won the tender to supply Lebanon with security-print biometric passports. Inkript manages the programming and software development in-house, and Gemalto is in charge of manufacturing the passports and matching the programme›s interface with the coding machines.

In 2017, the government began issuing biometric residence permits as well. These permits are similar to the passports, but they are for residents, not citizens.

SMEX asked the Directorate of General Security about the methods and systems it uses to protect the personal data from the biometric passports and residence permits, the parties that have access to this data, and the types of coordination between Lebanon and the countries of foreign nationals who live in Lebanon, and the data-sharing relationship between the Directorate and the UNHCR. In response to these questions, the Directorate replied the biometric passports and residence permits are a «technological and organizational development consistent with the Directorate›s policy of constantly developing its work.» The letter also stated that coordination with the UNHCR follows protocols outlined in a memorandum of understanding from 2003 and that «all eligible foreign nationals, including Syrians» are using the biometric passports.

In the absence of a clear legal framework regulating the adoption of biometrics as a form of identification, few safeguards exist to limit and control their use. Currently, the data can potentially be used as a tool for surveillance.

An additional concern is the use of private companies, Gemalto and InKript, which raises questions as to the ownership of this data, the responsibility, and accountability of the government to protect the data from abuse, theft, and loss. Given that Lebanon does not have a comprehensive data protection law, it is essential for the government to take necessary steps to ensure the protection of its citizens› personal data when engaging with third parties. Gemalto claimed that their office network had been the target of attacks in 2010 and 2011, «probably» by the NSA, the U.S. intelligence agency, and GCHQ, the British intelligence agency; although in this case it was claimed by Gemalto that they only got access to the encryption keys of 2G SIM cards. It is important to note how such companies have now become the target of intelligence agencies.

Voter registration

In September 2017, the Cabinet also approved biometric election cards for the May 2018 election, but due to time and resource constraints, these will not be introduced in time for those upcoming elections. Nonetheless, they remain on the agenda for subsequent elections.

SIM card registration

In December 2017, it was reported that the Cabinet planned to introduce biometric SIM card registration, which would force Lebanese citizens and residents to provide a thumbprint to purchase a SIM card. Al-Jadeed TV reported that the government is introducing this measure because 20% of the phones in the country do not actually belong to their listed owners. Al-Jadeed also reported that the government cited security reasons

Similarly, the Lebanese government reintroduced a proposal for IMEI registration, mandating that everyone who purchased a phone to have their identity attached to the IMEI number of the device. In April 2017, Jamal Jarrah, the current telecommunications minister, reintroduced the proposal and awarded the contract to Inmobiles, a subsidiary of Resource Holding Group. IMEI registration was briefly implemented in Lebanon, when Nicolas Sehnaoui, a former telecommunications minister introduced it in 2013 in an effort to prevent theft and fraud. However, Boutros Harb, the subsequent telecommunications minister, ended this policy, stating that it was ineffective and costly.

Policies and Sectoral Initiatives

Cybersecurity policy

Our research has not yet shown any specific examples of privacy issues related to cybersecurity policy in Lebanon. Please send any tips or information to: research@privacyinternational.org

Cybercrime

Our research has not yet shown any specific examples of privacy issues related to cybercrime in Lebanon. Please send any tips or information to: research@privacyinternational.org

Encryption

Our research has not yet shown any specific examples of privacy issues related to encryption in Lebanon. Please send any tips or information to: research@privacyinternational.org

Licensing of industry

Our research has not yet shown any specific examples of privacy issues related to the licensing of industry in Lebanon. Please send any tips or information to: research@privacyinternational.org

E-governance/digital agenda

Our research has not yet shown any specific examples of privacy issues related to e-governance and the digital agenda in Lebanon. Please send any tips or information to: research@privacyinternational.org

Health sector and e-health

Our research has not yet shown any specific examples of privacy issues related to the health sector in Lebanon. Please send any tips or information to: research@privacyinternational.org

Smart policing

Our research has not yet shown any specific examples of privacy issues related to smart policing in Lebanon. Please send any tips or information to: research@privacyinternational.org

Transport

Our research has not yet shown any specific examples of privacy issues related to transport in Lebanon. Please send any tips or information to: research@privacyinternational.org

Smart cities

In September 2017 OGERO, the telecommunications service provider, and Data Consult, a privately owned technology company announced that Beit Misk was the first «smart city» in Lebanon. Beit Misk itself is a small, manufactured city, intended to replicate a traditional Lebanese village, but as a smart city it now has the capability to measure «water levels, energy consumption and environmental conditions.» The decision making process did not involve civil society actors, though Marc Nader, COO of Data Consult, stated that Data Consult was not using this data for any other purpose at a launch event for the Lebanon IGF.

Migration

Our research has not yet shown any specific examples of privacy issues related to migration in Lebanon. Please send any tips or information to: research@privacyinternational.org

Emergency response

In August 2014, the government cut off access to mobile internet services in Arsal, a town in the north-east of Lebanon, after fighters from ISIS and al-Nusra entered the town. The shutdown lasted three years and mobile internet service was not made available until September 2017.

Humanitarian and development programmes

Our research has not yet shown any specific examples of privacy issues related to humanitarian and development programmes in Lebanon. Please send any tips or information to: research@privacyinternational.org

Social media

In 2015, SMEX reported that the state blocked eight gambling websites, 23 websites for offering escort services, five pornographic websites, 11 Israeli websites, two websites for breaching copyright and one LGBT website.

They have also been unconfirmed reports of extralegal methods used to identify anonymous online users, but most victims do not report these incidents and often choose to keep these incidents secret, according to a report from Open Society. Due to the nature of these incidents, the Open Society report does not go into further detail.

Location / Region / Locale: Lebanon Global South

Programme: Building the Global Privacy Movement

Resource Type: State of Privacy

Partner: SMEX