Mapping the Landscape of Digital Surveillance in Lebanon

December 2016

SMEX
Social Media Exchange
تبادل الإعلام الإجتماعي

www.smex.org
www.facebook.com/smex
www.twitter.com/smex

This report was researched and written by Mohamad Najem and edited by Lara Bitar.

Acknowledgments: The author is grateful to Dr. Charbel Kareh and Ms. Ghida Frangieh, whose feedback and input enriched this report. All errors and omissions are the author's.

Graphic Design: Salam Shokor Art

Published in 2016 by
Social Media Exchange Association,
Kmeir Building, 4th Floor, Badaro, Beirut, Lebanon

Contents

Introduction

1. This report, produced by Social Media Exchange (SMEX) in December 2016, provides an overview of the state of online privacy and mass digital surveillance in Lebanon. It builds on the previous joint stakeholder report "The Right to Privacy in Lebanon,"[1] submitted as an element of the 23rd Universal Periodic Review. SMEX is a registered Lebanese non-profit organization working to advance self-regulating information societies in the Middle East and North Africa.

2. This report examines the legal framework (or lack thereof) within which state-led mass digital surveillance is taking place. Additionally, it lists the country's main state actors in the field of surveillance and documents use cases of mass surveillance technologies, and names the companies that have sold those systems and services over the last five years.

3. This research aims to further the understanding of the impact of mass digital surveillance on human rights, and particularly the right to privacy, in Lebanon. By providing foundational knowledge about the types and scope of surveillance taking place in Lebanon, we aim to open the necessary space for public discussion, reporting, and advocacy to protect and promote digital rights.

"This research aims to further the understanding of the impact of mass digital surveillance on human rights, and particularly the right to privacy, in Lebanon."

4. From this basis, the SMEX Fellowship for Reporting on Digital Freedoms, a public-interest journalism fellowship, will be launched. Local journalists will be invited to apply for two stipend-supported fellowships during which they will lead in-depth investigations into matters tackling privacy and surveillance. The fellowship aims to further expand the baseline of knowledge of mass surveillance in Lebanon, raise awareness of these issues, and inform evidence-based public debate.

5. While this report focuses on digital surveillance, SMEX also acknowledges that online surveillance in Lebanon is often tied to physical surveillance. Under the Beirut City Surveillance project, for instance, images of citizens and visitors will be captured by closed circuit television or street cameras and transmitted over digital networks to monitoring stations. In the absence of a legal mandate or framework, this project threatens to violate every resident and visitor's right to privacy.

6. This report relies on Privacy International's working definition of "communication surveillance:"

> *"The interception, collection, preservation and retention of information that has been communicated, relayed or generated over communications networks to a group of recipients by a third party. This third party could be a law enforcement agency, intelligence agency, a private company, or a malicious actor. Communications surveillance does not require a human to read the intercepted communication, as any automated action of communications surveillance represents an interference with the right to privacy."*[2]

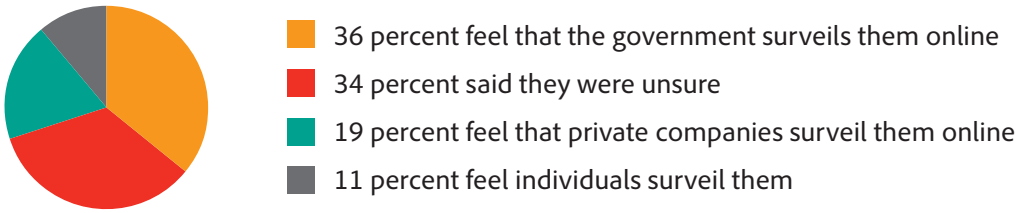
Internet Usage in Lebanon

	Number of Users	Percentage of Population	Reporting Period
Internet Penetration[3]	4,545,007	75.9 %	As of June 30, 2016
Facebook Penetration[4]	3,100,000	51.8 %	As of June 30, 2016
Mobile Broadband Subscriptions[5]	3,147,170	53.5 %	2014

[1] *Privacy International, "The Right to Privacy in Lebanon," March 1, 2015. Accessed December 12, 2016. Available at: https://www.privacyinternational.org/node/580*
[2] *Privacy International, "Communications surveillance." Accessed December 5, 2016. Available at: https://www.privacyinternational.org/node/10*
[3] *Internet World Stats, Lebanon, June 2016. Available at: http://www.internetworldstats.com/middle.htm#lb*
[4] *Internet World Stats, Lebanon, June 2016.*
[5] *Broadband Commission for Digital Development, The State of Broadband 2015, September 2015. Available at: http://www.broadbandcommission.org/Documents/reports/bb-annualreport2015.pdf*

Public Sentiment about Surveillance

In the absence of other data, SMEX created a poll[6] on its Twitter account on August 31, 2016, that lasted for seven days to gauge its followers' perceptions of digital surveillance in Lebanon. At the time of the polling, the account had 5,310 followers, out of which 75 engaged with the question, "Do you feel you have been subjected to digital surveillance in Lebanon before?



Legal Frameworks for Privacy

International Framework

6. Lebanon is one of the 48 initial adopters of the Universal Declaration of Human Rights (UDHR), in which Article 12 states:

> *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."*

7. Similarly, the International Covenant on Civil and Political Rights, to which Lebanon is a party, provides that "no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation."[7]

"The United Nations General Assembly, 'expressed deep concern at the negative impact that surveillance and interception of communications may have on human rights.'"

8. In the aftermath of former National Security Agency contractor Edward Snowden's leaks in the summer of 2013, revealing indiscriminate and global mass surveillance by the U.S. government, the international legal framework for the right to privacy became a focus of attention. As such, Resolution 68/167, adopted in December 2013 by the United Nations General Assembly, "expressed deep concern at the negative impact that surveillance and interception of communications may have on human rights."[8]

9. In July 2015, the first-ever Special Rapporteur on the right to privacy Prof. Joseph Cannataci was appointed by the United Nations Human Rights Council. His first report, which highlighted seven areas of concern, was released in March 2016. Areas of concern particularly relevant to this report are "Security, surveillance, proportionality and cyberpeace" and "biometrics and privacy."[9]

National Legal Framework

10. The preamble of the Lebanese Constitution[10] affirms that Lebanon is,

> *"A founding and active member of the United Nations Organization and abides by its covenants and by the Universal Declaration of Human Rights. The Government shall embody these principles in all fields and areas without exception."*

---

[6] *SMEX. [SMEX], "Do you feel you have been subjected to digital surveillance in Lebanon before?" August 31, 2016, 4:56 am. [Tweet] Available at: https://twitter.com/SMEX/status/770968518510649344*
[7] *United Nations Office of the High Commissioner of Human Rights, "The Right to Privacy in the Digital Age." Accessed December 12, 2016. Available at: http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx*
[8] *Ibitd.*
[9] *United Nations Office of the High Commissioner of Human Rights, "Special Rapporteur on the right to privacy." Accessed December 12, 2016. Available at: http://www.ohchr.org/Documents/Issues/Privacy/SRonprivacy_Statement_HRC_9March2016.pdf*
[10] *Lebanese Constitution. Available at: http://smex.silk.co/page/Constitution%20(7)*

11. Article 14 of the Lebanese Constitution ensures the inviolability of the home:

> *"The citizen's place of residence is inviolable. No one may enter it except in the circumstances and manners prescribed by Law."*

12. Articles 8 and 13 of the Constitution indirectly protect the right to privacy[11] with the former guaranteeing individual liberty and the latter freedom of expression. These laws have been interpreted to guarantee the secrecy of all means of communications, including mail and telephone calls.[12]

13. Article 98 of the Lebanese Code of Civil Procedures regulates the regime applicable to search and seizures.

14. Law No. 140, also known as the Eavesdropping Law, is the only law that legislates communication surveillance in Lebanon and was last revised in 1999.[13] As stated in articles 1 and 2, the law intends to protect the secrecy of all means of communication and stipulates that the right to secrecy of communications, both internal and external, by all means wired or wireless (landlines and mobile of all types, including fax and electronic mail) is guaranteed and protected by law and cannot be subject to any form of tapping, surveillance, interception, or violation except in those cases, and by the means and procedures, prescribed by law.

15. While there is no specific data protection legislation in place, various laws do protect aspects of personal data, including Article 2 of the Banking Secrecy Law of September 3, 1956, and in the penal code, articles 579, 580, and 581, which relate to the violation of secrets. Article 7 of the Code of Medical Ethics (Law No. 288 of February 22, 1994) protects the confidentiality of physician and patient relationships, and articles 51 and 58 of the Consumer Protection Code (Law No. 659 of February 4, 2005) stipulate that suppliers must not disclose data without the consent of the consumer.

Draft Electronic Transactions and Personal Data Law

16. Article 85 of the most recent draft of the Electronic Transactions and Personal Data law (last amended on June 9, 2015) defines electronic personal data, data processing procedures, data ownership, and the parties responsible for data processing.[14] While there are some concerns about ambiguity in the language, attorney Charbel Kareh considers that establishing a legal baseline dealing with data-related issues to be a good start. While imperfect, he noted, this legislation presents the only alternative to the current vacuum that exists in the Lebanese legal system.

Main State Actors Involved in Mass Surveillance

17. The Ministry of Telecommunications: According to the ministry's website, the Ministry of Telecommunications "undertakes the construction and equipping, operation, and maintenance of all telecommunications services in Lebanon comprising fixed, mobile, all Internet, and postal services."[15] The ministry also sets fees and manages mobile operator licenses (Zain and Orascom) in accordance with the state monopoly on fixed and mobile telecom and Internet services.

Plans to liberalize or privatize[16] the telecom sector have been afoot since 2002, when a new law (Law 431[17]) to privatize and regulate the telecom sector—including the establishment of an independent Telecom Regulatory Authority (TRA)—was passed. While the TRA was established, privatization has not materialized. In effect, the ministry acts as operator, regulator, and supervisor of the telecom sector, which is one of the government's biggest sources of income. In 2014, telecom revenue amounted to about 15 percent of the total fiscal

---

[11] Special Tribunal of Lebanon, Case No. STL-11-01/T/TC, para. 29.
Available at: http://www.stl-tsl.org/en/the-cases/stl-11-01/main/filings/replies-and-responses/defence-team-counsel/f1857
[12] HiiL, "The Rule of Law in Lebanon: Prospects and Challenges," Hill Rule of Law Quick Scan Series, April 2012, p. 18.
Available at: http://www.hiil.org/data/sitemanagement/media/Quickscan_Lebanon_160812_digitaal_def.pdf
[13] SMEX Digital Rights Datasets, Eavesdropping law, Lebanon. Accessed November 29, 2016. Available at: http://smex.silk.co/page/Eavesdropping-law
[14] Draft text of the Electronic Transactions and Personal Data Law, http://bit.ly/2hkQQfh
15 Republic of Lebanon - The Ministry of Telecommunications, About MPT. Accessed November 29, 2016.
Available at: http://www.mpt.gov.lb/index.php/en/about-mpt-2/mpt-info/mpt-brief
[16] Al Akhbar English, "Is the telecom minister preparing to privatize the sector?" May 16, 2014. Accessed December 12, 2016.
Available at: https://english.al-akhbar.com/node/19802
[17] Telecommunications Regulatory Authority, Law 431/2002. Available at: http://www.tra.gov.lb/Telecom-Law-431-2002

revenues, or about $1.43 billion.[18] The current telecom minister is member of the Lebanese Parliament Boutros Harb.[19] In 2015, Harb announced the $600 million five-year "Lebanon 2020 Digital Telecom Vision"[20] to revamp Lebanon's telecom infrastructure. While the minister previously had authority to approve (or deny) requests to collect communications data[21], this authority was transferred, at least temporarily, to the Cabinet of Ministers in September 2014.[22]

18. The Ministry of the Interior:[23] Established in 1943 and renamed in 2000, the Ministry of the Interior and Municipalities is a huge government department that engages in domestic affairs at the governorate, caza, and municipality levels; is responsible for oversight of political parties and elections; and also encompasses bodies responsible for intelligence gathering, including the General Directorate of General Security and Internal Security Forces. The ministry was created in the first post-independence government in 1943. Its current minister is member of the Lebanese Parliament Nohad Machnouk.[24]

19. General Security[25]: The General Directorate of General Security is a Lebanese intelligence agency that was founded on July 21, 1921. With the adoption of Decree No. 139 of June 12, 1959, the General Security Directorate became a special branch of the Ministry of the Interior. Its main task and function is to collect and gather intelligence with a specific focus on monitoring foreigners, and to report its findings to the Lebanese government with the aim of ensuring national security and public order throughout the territory of the Republic of Lebanon.

20. Internal Security Forces: The General Directorate of Internal Security Forces (ISF) is the national police and security force of Lebanon. It reports directly to the Ministry of the Interior.

a. The Cybercrime and Intellectual Property Unit:[26] The Cybercrime and Intellectual Property Rights Bureau, commonly known as the Cybercrime Bureau [hereinafter: the Bureau], was established by means of Memorandum 204/609 in 2006. It is tasked with investigating cybercrimes involving electronic monetary fraud and theft, intellectual property rights, and child pornography. Its legality, however, has repeatedly come into question since it was established without a legislative decree. The Legal Agenda (LA), a Beirut-based non-governmental organization that monitors and analyzes law and public policy in Lebanon, deems it illegal. In addition, in the absence of laws protecting Internet users in Lebanon, the Bureau's powers have continuously grown. It now deals with most matters related to the Internet, treating potential online defamation and libel as cybercrimes. In effect, the Bureau's expansive powers have allowed it to summon, detain, and question journalists, bloggers, and activists for articles and online posts written or shared on their social media accounts.[27] The LA warns that the Bureau "jeopardize[s] basic freedoms associated with online activity, such as the freedom of expression and the right to privacy."[28]

b. Information Branch of the ISF: The intelligence-oriented Information Branch of the ISF was established in 1991 after the issuance of Law No. 17 and decree No. 1157. Its activities quickly grew, "intervening into Lebanese political life at the beginning of the year 2000, in the shadow of the Syrian presence, and there was more likely than not cooperation between the two. It returned to the fore very prominently after 2005 and the withdrawal of Syrian troops from Lebanon, expanding both in terms of number of personnel and amount of available equipment. It was also allotted a significant budget, allowing it to

---

[18] BLOM The Research Blog, "The Lebanese Mobile Market: Strident Steps in 2014 to revitalize the Sector," July 26, 2014. Accessed December 12, 2016. Available at: http://blog.blominvestbank.com/wp-content/uploads/2014/09/2014-07-The-Lebanese-Mobile-Market-Strident-Steps-in-2014-to-revitalize-the-Sector.pdf

[19] Harb, Boutros. [Harb_Boutros]. Accessed November 29, 2016. [Twitter account] Available at: https://twitter.com/Harb_Boutros

[20] Ministry of Telecommunications, "Lebanon 2020 Digital Telecom Vision." Accessed December 12, 2016. Available at: http://www.mpt.gov.lb/index.php/en/about-mpt-2/mpt-news/48-latest/374-lebanon-2020-digital-telecom-vision

[21] Naharnet, "Sehnaoui Meets Berri: Whoever Acquires Telecom Data Can Spy on Everyone in Lebanon," April 12, 2012. Accessed December 12, 2016. Available at: http://www.naharnet.com/stories/en/36569-sehnaoui-meets-berri-whoever-acquires-telecom-data-can-spy-on-everyone-in-lebanon

[22] The Daily Star, "Lebanon's Cabinet extends security agencies telecoms data access," April 27, 2016. Accessed December 12, 2016. Available at: https://www.dailystar.com.lb/News/Lebanon-News/2016/Apr-27/349488-telecoms-data-to-top-government-meet.ashx

[23] Ministry of Interior and Municipalities, Main Page. Updated November 29, 2016. Available at: http://www.interior.gov.lb/

24 Nohad Machnouk. [NohadMachnouk]. Accessed November 29, 2016. [Twitter account]. Available at: https://twitter.com/NohadMachnouk

[25] General Directorate of General Security, About GS - Functions of the General Security. Updated December 6, 2016. Available at: http://www.general-security.gov.lb/en/posts/3

[26] The Beirut Report, "Who's got your data?" July 13, 2015. Available at: http://www.beirutreport.com/tag/cyber-crime-bureau

[27] Al-Akhbar English, "Cybercrime Bureau's ever-growing powers threatening freedoms in Lebanon," November 22, 2014. Available at: https://english.al-akhbar.com/node/22605

[28] The Legal Agenda, "Lebanon's Cybercrime Bureau: A License to Censor?" February 27, 2014. Available at: http://legal-agenda.com/en/article.php?id=590&lang=en

play a very central role in regulating security and fighting crime and terrorism, in collaboration with other similar security apparatus, regionally and abroad."[29]

21. The Military Intelligence Directorate[30]: A department of the army, referred to in Article 4 of Decree No. 3771 of January 22, 1981, the Military Intelligence Directorate is under the supervision of the army chief of staff, who is informed of all available information, pursuant to the provisions of Article 28 of the National Defence Act. The department's tasks revolve around protecting the army from any internal or external danger. This includes in particular:

a. The collection of strategic information on plans for and the conduct of military operations.
b. Strategic investigation about the enemy, its goals and warfare doctrine, organization, and military capacity.
c. Developing measures to combat espionage and sabotage related to military security.
d. Interrogating prisoners of war and conducting the necessary investigations in accordance with the applicable laws.
e. Inquiring about military personnel's security and morale, and securing military installations, documents, and all forms of communication.
f. Securing links to foreign military personnel authorized to operate in Lebanon.
g. Preparing and training elements of the Intelligence Directorate in the field of competence.

"All Internet traffic within Lebanon goes through OGERO's servers."

22. OGERO[31]: OGERO is the Organisme de Gestion et d'Exploitation de l'ex-société Radio-Orient. It was founded by the Lebanese state in 1972 to continue the work of the former French company Radio Orient. Since then, OGERO has become the main operator of the fixed telecommunications network in Lebanon for the benefit of the Lebanese Ministry of Telecommunications. OGERO and the Ministry of Telecommunications work hand-in-hand to provide the services of the telecom sector. OGERO runs landline operations; resells Internet bandwidth to private Internet service providers; and is the main Internet service provider for end users and private companies. All Internet traffic within Lebanon goes through OGERO's servers.

Instances of the Use of Mass Digital Surveillance Technologies in Lebanon

The following are some of the main digital surveillance cases that have occurred in Lebanon since 2011:

23. The General Directorate of General Security (GDGS) and the Internal Security Forces (ISF) have used FinFisher spyware software for surveillance activities in Lebanon, according to the Citizen Lab's[32] October 2015 report, "Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation."[33] The General Security and ISF involvement was noted because it is linked to a mail server with both agencies' domain name registrations.

24. In 2015, WikiLeaks[34] published leaked emails between the General Security and the offensive surveillance company Hacking Team, indicating that communication between both parties started in early 2012. It is not clear, however, whether a business relationship was ultimately initiated.

25. The WikiLeaks database[35] reveals that in February 2015, the Bureau communicated with Hacking Team, requesting details about their new software GALILEO Remote Control System[36] (RCS), its features, price, contact person, and support information. The leaks also exposed proof of a concept demo carried out in Beirut.[37] The Bureau had communications with both Gamma Group and Hacking Team offensive surveillance

---

[29] *Carnegie Endowment for International Peace, The Security Sector in Lebanon: Jurisdiction and Organization, September 2012. Available at: http://carnegieendowment.org/files/Security_Sector_in_Lebanon2.pdf*
[30] *Ibid.*
[31] *OGERO, About - Organization Profile. Updated February 3, 2015. Available at: https://www.ogero.gov.lb/Published/EN/profile.html*
[32] *The Citizen Lab, About the Citizen Lab. Accessed November 30, 2016. Available at: https://citizenlab.org/about/*
[33] *The Citizen Lab, "Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation," October 15, 2015. Available at: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/*
[34] *WikiLeaks, Hacking Team (email), March 17, 2012. Available at: https://wikileaks.org/hackingteam/emails/emailid/605898*
[35] *WikiLeaks, Hacking Team (email), February 27, 2015. Available at: https://wikileaks.org/hackingteam/emails/emailid/131690*
[36] *Windows Central, "Galileo - Remote Control System" [Video]. Accessed December 6, 2016. Available at: https://www.youtube.com/watch?v=8oilhYYj8_g*
[37] *WikiLeaks, Hacking Team (email), February 28, 2015. Available at: https://wikileaks.org/hackingteam/emails/emailid/11959*

agencies,[38] with Hacking Team leaks showing that the firm produced a demo for Galileo RCS software focusing on mobile infection and interception. The Bureau later signed a 450,000 euro contract with Hacking Team to enable the hacking of 50 individuals.

"The Bureau later signed a 450,000 Euro contract with Hacking Team to enable the hacking of 50 individuals."

26. Leaks also revealed invoices from the Hacking Team addressed to the Lebanese Army Intelligence,[40] totaling more than 1 million euros, receivable for the purchase of the Galileo RCS, along with other equipment. Neither the targets nor the content subjected to surveillance was determined.

27. Blue Coat PacketShaper installations were found on two netblocks—or groups of IP addresses—associated with IncoNet Data Management and Virtual ISP Lebanon private Internet service providers, according to a Citizen Lab report in 2013.[41] These providers are part of two dozen private ISPs that buy legal Internet from the Ministry of Telecommunications.

28. IMSI catchers—devices that act like a cell tower for the purposes of intercepting mobile communications or tracking a user's movements—are being used in Lebanon, according to documents released by the Swiss government[42] in 2015. In addition, security agencies in Lebanon have confirmed that they have been using the software since 2009, alleging IMSI's are needed to expose Israeli agents.[43]

29. Lebanese Internet service providers (ISPs) were instructed[44] in a June 7, 2013, order by the general prosecutor 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 specified that data collected and held should include username, IP address, the sites accessed, protocols used, and the user's location. One ISP CEO confirmed that his company was logging "who emails whom, not the content of the messages."

Additional Concerns

30. In September 2014, the Lebanese Council of Ministers relinquished its authority to approve or deny telecom data requests by giving full telecom data access to security agencies.[45] In April 2016, the Council extended this access for one additional year.[46] These decisions not only breach the Lebanese Constitution but also Law No. 140, which clearly states in its first two articles that surveillance should be limited to a specific number of people, for a specific time period, and must be approved by a judge.

31. In late 2015, the General Security announced that biometric technology would be adopted for Lebanese passports.[47] Inkript, a Lebanon-based provider of "secure solutions to governments, telecom operators and financial institutions,"[48] will be the main implementer, supported by the Dutch digital security company Gemalto

---

[38] *SMEX, "#HackingTeam Leaks: Lebanon's Cybercrime Bureau Exploited Angry Birds to Surveil Citizens' Mobile Devices," July 28, 2015. Available at: http://www.smex.org/hackingteam-leaks-lebanons-cybercrime-bureau-exploited-angry-birds-to-surveil-citizens-mobile-devices/*

[39] *Advox, "#HackingTeam Leaks: Lebanon's Cybercrime Bureau Exploited Angry Birds to Surveil Citizens' Mobile Devices," July 28, 2015. Available at: https://advox.globalvoices.org/2015/07/28/hackingteam-leaks-lebanons-cybercrime-bureau-exploited-angry-birds-to-surveil-citizens-mobile-devices/*

[40] *Advox, "For Arab Human Rights Defenders, Hacking Team Files Confirm Suspicions of State Surveillance," July 8, 2015.Available at: https://advox.globalvoices.org/2015/07/08/for-arab-human-rights-defenders-hacking-team-files-confirm-suspicions-of-state-surveillance/*

[41] *The Citizen Lab, Appendix A: Summary Analysis of Blue Coat "Countries of Interest," January 15, 2013. Available at: https://citizenlab.org/2013/01/appendix-a-summary-analysis-of-blue-coat-countries-of-interest/#39*

[42] *Privacy International, "Swiss Government forced to reveal destinations, cost of surveillance exports," January 14, 2015. Available at: https://www.privacyinternational.org/node/98*

[43] *Lebanon Files, "IMSI-catcher contributed to the interception of communication by Mossad-affiliated cells," June 10, 2009. Available in Arabic at: http://www.lebanonfiles.com/news/125553*

[44] *NOW, "Providers tracking customers' Internet use," November 29, 2013. Available at: https://now.mmedia.me/lb/en/reportsfeatures/523209-523209-523209-providers-tracking-customers-internet-use*

[45] *Lebanese Republic - Presidency of the Council of Ministers, "Session Decisions," April 29, 2015. Available at: http://www.pcm.gov.lb/english/subpg.aspx?pageid=6959*

[46] *An-Nahar English, "Security agencies maintain access to telecom data," April 27, 2016. Available at: http://en.annahar.com/article/367264-cabinet-prolongs-securities-agencies-access-to-telecom-data*

[47] *The Daily Star, "New passports to survive biometric age," January 9, 2016. Accessed December 12, 2016. Available at: https://www.dailystar.com.lb/News/Lebanon-News/2016/Jan-09/330986-new-passports-to-survive-biometric-age.ashx*

[48] *Inkript, "Our Company." Accessed December 12, 2016. Available at: http://www.inkript.com/our-company*

as a subcontractor. The new technology is being used without any data protection guarantees.[49] In addition, the United Nations High Commissioner for Refugees (UNHCR) is collecting biometric data on all refugees in Lebanon, to which the General Security has requested access.[50]

"There are many reasons to impose Internet surveillance."
—General Security Captain Yusuf Al-Badawi

32. In late 2015, a roundtable discussion about new media and challenges was hosted by the Studies and Publications Directorate at the Ministry of Information. The legality of Internet surveillance came into question, with General Security Captain Yusuf Al-Badawi stating, "There are many reasons to impose Internet surveillance; political to maintain public security and public order and combat terrorism, and other economic reasons, especially to maintain the overall investment climate and the national economy and currency. Also, the social causes that include fighting sectarian blocs, racial discrimination, ideas that destroy the social fabric."[51]

33. In 2014, the Beirut municipality approved Beirut City Surveillance, a project to install about 1,850 cameras in 350 locations around Beirut. Images collected from these cameras will be piped via the Internet to a real-time monitoring room. The $36 million project[52] was awarded to Guardia Systems,[53] the local systems integrator in the security and fire industry. SMEX and other civil society groups fear that this project threatens to violate the privacy of Beirut's inhabitants and its one million daily visitors.[54]

34. The state-run company OGERO is the country's sole Internet service provider. However, the Telecommunications Ministry has repeatedly warned and cracked down on illegal internet providers over the years. In 2009, authorities discovered an elaborate network of illegal ISPs in the town of Al-Barouk in the Shouf district.[55] The Al-Barouk network allegedly had satellite links to Israel and was being used by a number of government offices. More recently, in March 2016, two Lebanese nationals were indicted for establishing unlicensed Internet networks. In a press conference held to address the issue, Telecommunications Minister Boutros Harb asserted that illegal ISPs pose a threat to national security. Harb explained that these networks are being used by Israel to spy on Lebanese citizens and state institutions, calling on bandwidth providers in Turkey and Cyprus to stop the "aggressions against Lebanon."[56] Some Internet users, however, reportedly believe that "national security is being used as a pretext to keep the state's monopoly" over the Internet.[57]

Conclusion

This report maps the current environment of mass digital surveillance in Lebanon and how it is setting the stage for privacy and other rights' violations. Notable features of this landscape include a weak legal framework for the protection of privacy in a digital age. Particularly troubling, given the Council of Ministers September 2014 and April 2016 decisions, is the absence of any established due process by which either individual citizens or civil society as a whole can challenge mass digital surveillance or data collection in the country. Whether this will be addressed by the passage of the current draft Electronic Transactions and Personal Data law remains to be seen.

Documents highlighted in this report also reveal that the various security agencies in Lebanon are working independently from one another. Further, they also appear to have access to funds that allow them to acquire millions of dollars worth of surveillance technology without any judicial monitoring, approval, or public oversight. Taxpayers are not even aware if such purchases are included in the budget, as the Lebanese government has not had a budget since 2005, making it difficult to track such expenditures.

---

[49] *SMEX, "Questions the Lebanese Government Should Answer about the New Biometric Passports," July 19, 2016. Available at: http://www.smex.org/legitimate-questions-about-biometric-passport-lebanese-government-should-answer/*
[50] *The Daily Star, "Lebanon seeking refugee biometric data: Derbas," May 30, 2014. Available at: https://www.dailystar.com.lb/News/Lebanon-News/2014/May-30/258268-government-has-refugee-eye-scans-derbas.ashx*
[51] *SMEX, "Are Internet users in Lebanon illegally monitored?" December 11, 2015.Available in Arabic at: http://bit.ly/2c9Eo1h*
[52] *InAVateonthenet, "Beirut Surveillance Project protects the city," May 23, 2016. Available at: http://www.inavateonthenet.net/case-studies/article/beirut-surveillance-project-protects-the-city*
[53] *Guardia Systems, "About Us." Accessed December 6, 2016. Available at: http://guardiasystems.com/about/*
[54] *SMEX, "2000 Eyes to Surveil Beirut by Year's End," June 13, 2016. Available at: http://www.smex.org/2000-eyes-to-surveil-beirut-by-years-end/*
[55] *NOW, " Illegal internet neither begins nor ends with Barouk," September 2, 2009. Available at: https://now.mmedia.me/lb/en/reportsfeatures/illegal_internet_neither_begins_nor_ends_with_barouk_*
[56] *The Daily Star, " Lebanon telecoms minister links illegal internet to Israeli spy networks," March 16, 2016. Availabe at: https://www.dailystar.com.lb/News/Lebanon-News/2016/Mar-16/342479-lebanon-telecoms-minister-links-illegal-internet-to-israeli-spy-networks.ashx*
[57] *Middle East Eye, "Lebanon's illegal internet boom sparks crackdown and calls for reform," April 11, 2016. Available at: http://www.middleeasteye.net/news/boom-illegal-internet-providers-sparks-crackdown-lebanon-502165956*

As the powers of security agencies responsible for mass surveillance expand and as their tools grow, the lack of clear and specific guidelines regulating their mandate is a threat to the right to privacy. Biometric passports, IDs, and car registrations are some of the new projects the Lebanese government has started implementing without a clear framework for the protection of the data being collected. The potential for the misuse of personally identifiable data is a risk that all of Lebanon's citizens, residents, and visitors face. This concern, as the 2014 breach reveals, is legitimate.[58]

A rigorous and formal data protection system must be developed, enacted, and enforced, alongside guidelines regulating security agencies' functions. In parallel, citizens must have access to due process of law that enables them to hold the Lebanese government accountable for both preserving their universally declared right to privacy and the protection of their personally identifiable data.

[58] *Slate, "In Lebanon, Apps Let You Get Someone Else's Personal Info With Ease," May 14, 2014. Available at: http://www.slate.com/blogs/future_tense/2014/05/15/in_lebanon_apps_let_you_get_someone_else_s_personal_info_with_ease.html*