Submission from Social Media Exchange and the Association for Progressive Communications to the United Nations Human Rights Committee in advance of its review of Lebanon

April 2017

1. Introduction

This submission highlights areas of concern that Social Media Exchange (SMEX) and the Association for Progressive Communications (APC)[1] hope will inform the Human Rights Committee's consideration of the Lebanese government's compliance with the International Covenant on Civil and Political Rights (ICCPR) concerning Article 17, on the right to privacy. This submission examines the shortcomings of Lebanon's domestic legal framework to protect the right to privacy, and documents state-led mass communications surveillance, as well as other threats to the right to privacy in Lebanon[2] for the period of 2011-2016. While we focus this submission on Article 17, it is important to recognise that the exercise of the right to privacy is important for the realisation of other human rights, including the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association, and is one of the foundations of a democratic society.[3]

We hope this submission will inform the Committee's pre-sessional review of Lebanon and that the concerns highlighted here will be reflected in the list of issues submitted to the Lebanese government ahead of its review.

[1]SMEX is a registered Lebanese non-profit organisation working to advance self-regulating information societies in the Middle East and North Africa (www.smex.org). APC is an international network and non-profit organisation founded in 1990 that wants everyone to have access to a free and open internet to improve lives and create a more just world (https://www.apc.org).

[2]This report relies on Privacy International's working definition of "communications 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." See: https://www.privacyinternational.org/node/10

[3]Human Rights Council Resolution 34/7, "The right to privacy in the digital age". 22 March 2017. http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/34/L.7/Rev.1

For deeper analysis of these issues, please see the following SMEX reports:

Mapping the Landscape of Digital Surveillance in Lebanon: https://www.smex.org/wp-content/uploads/2016/12/SMEX-Landscape-Mapping-of-Digital-Surveillance-in-Lebanon.pdf

Joint stakeholder report for the 23rd session of the Universal Periodic Review: The Right to Privacy in Lebanon: https://www.smex.org/wp-content/uploads/2015/09/Lebanon_UPR_23rd_session_Joint_Stakeholder_submission_0.pdf

2. Legal framework

In Lebanon, some protections for the right to privacy are contained in the constitution and other pieces of domestic legislation; however, the existing framework fails to ensure that any interference with the right to privacy meets international human rights standards, namely the principles of legality, necessity and proportionality. The existing legal framework includes the following:

- Article 14 of the Lebanese Constitution ensures the inviolability of the home, establishing, "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 protect the right to privacy[4] 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 both mail and telephone calls.[5]
- Article 98 of the Lebanese Code of Civil Procedures regulates the regime applicable to search and seizures.
- 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.[6] As stated in Articles 1 and 2, the law intends to protect the secrecy of all means of communications 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 mobile telephone, fax, electronic mail) is guaranteed and protected by law and cannot be subject to any forms of tapping, surveillance, interception or violation except in those cases, and by the means and procedures, prescribed by law.[7]
- There is no specific data protection legislation in place; however, various laws do protect aspects of personal data, including Article 2 of the Banking Secrecy Law of 3 September 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 22 February 1994) protects the confidentiality of physician and patient relationships, and Articles 51 and 58 of the Consumer Protection Code (Law No. 659 of 4 February 2005) establish that suppliers must not disclose data without the consent of the consumer.
- Article 85 of the most recent draft of the Electronic Transactions and Personal Data Law (last amended on 9 June 2015) defines electronic personal data, data processing procedures, data

[4]Special Tribunal of Lebanon, Case No. STL-11-01/T/TC, para. 29. www.stl-tsl.org/en/the-cases/stl-11-01/main/filings/replies-and-responses/defence-team-counsel/f1857

[5]HiiL, "The Rule of Law in Lebanon: Prospects and Challenges," Hill Rule of Law Quick Scan Series, April 2012, p. 18. www.hiil.org/data/sitemanagement/media/Quickscan_Lebanon_160812_digitaal_def.pdf

[6]SMEX Digital Rights Datasets, Eavesdropping Law, Lebanon. http://smex.silk.co/page/Eavesdropping-law

[7]Law No. 140 requires that requests for access to communications be approved by a judge, but this aspect of the law is not being applied in practice, as demonstrated in the following section.

ownership, and the parties responsible for data processing.[8] While there are some concerns about ambiguity in the language, having a legal baseline dealing with data-related issues is a good start. While imperfect, an attorney specialising in information technology law noted, this legislation presents the only alternative to the current vacuum that exists in the Lebanese legal system.[9]

The national legal framework for the protection of the right to privacy in Lebanon reflects several shortcomings. The framework itself is weak, established only through the constitution, obliquely through the eavesdropping law (Law No. 140), and in a few sectoral laws. In addition, there is no overall data protection law, nor is there an independent data protection authority in place. Without statutes establishing legal norms for data protection or the institutions to uphold them, several areas are potential sites for data exploitation, including the national fixed-line and mobile networks over which personal data travel and the servers – whether maintained by the government or its contractors – where these data are stored.

3. Areas of concern

3.1 Evidence of mass surveillance of digital communications by the Government of Lebanon

In the absence of a robust legal framework, the Lebanese government has engaged in mass surveillance of digital communications. Since there is a lack of transparency or public oversight of communications surveillance policies and practices in Lebanon, most of the information comes from disclosures made public by non-governmental organisations and whistleblowers. The following are some of the main cases that have occurred in Lebanon between 2011 and 2016:

- The General Directorate of General Security and the Internal Security Forces (ISF) have used FinFisher spyware software for surveillance activities in Lebanon, according to the Citizen Lab's[10] October 2015 report "Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation".[11] The General Security and ISF involvement was noted because it is linked to a mail server with both agencies' domain name registrations.
- The WikiLeaks database[12] reveals that in February 2015, the Cybercrime Bureau communicated with Hacking Team, requesting details about their new software, Galileo Remote Control System (RCS),[13] its features, price, contact person, and support information. The leaks also exposed proof of a concept demo carried out in Beirut.[14] The Bureau had communications with both the Gamma Group and Hacking Team offensive surveillance agencies,[15] with Hacking Team leaks showing that the firm produced a demo for Galileo RCS software focusing on mobile infection and

[8]Draft text of the Electronic Transactions and Personal Data Law. http://bit.ly/2hkQQfh

[9]SMEX interview with attorney-at-law Charbel Kareh, November 2016.

[10]The Citizen Lab, About the Citizen Lab. https://citizenlab.org/about

[11]The Citizen Lab, "Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation," October 15, 2015. https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation

[12]WikiLeaks, Hacking Team (email), February 27, 2015. https://wikileaks.org/hackingteam/emails/emailid/131690

[13]Windows Central, "Galileo - Remote Control System" [Video]. https://www.youtube.com/watch?v=8oilhYYj8_g

[14]WikiLeaks, Hacking Team (email), February 28, 2015. https://wikileaks.org/hackingteam/emails/emailid/11959

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

interception. The Bureau later signed a EUR 450,000 contract with Hacking Team to enable the hacking of 50 individuals.[16]

- Leaks also revealed invoices from Hacking Team addressed to the Lebanese Army Intelligence,[17] totalling more than EUR 1 million, receivable for the purchase of the Galileo RCS, along with other equipment. Neither the targets nor the content subjected to surveillance was determined.
- Blue Coat PacketShaper installations were found on two netblocks – or groups of IP addresses – associated with private internet service providers (ISPs) IncoNet Data Management and Virtual ISP Lebanon, according to a Citizen Lab report in 2013.[18] These providers are part of two dozen private ISPs that buy legal internet from the Ministry of Telecommunications.
- 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 in 2015.[19] In addition, security agencies in Lebanon have confirmed that they have been using the software since 2009, alleging IMSIs are needed to expose Israeli agents.[20]
- Lebanese ISPs were instructed by the General Prosecutor in a 7 June 2013 order 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."[21] 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."

3.2 Additional concerns

- **Relinquishment of judicial oversight of surveillance requests to security agencies:** 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.[22] In April 2016, the Council extended this access for one additional year.[23] These decisions not only breach the Lebanese Constitution but also Law No. 140, which states clearly 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.[24]

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

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

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

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

[20]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

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

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

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

[24]This is especially concerning given the views that high-ranking officials within Lebanon's security apparatus have voiced regarding communications surveillance. For example, 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

- **Use of biometric technology without a data protection framework:** In late 2015, the General Directorate of General Security announced that biometric technology would be adopted for Lebanese passports.[25] Inkript, a Lebanon-based provider of "secure solutions to governments, telecom operators and financial institutions,"[26] will be the main implementer, supported by the Dutch digital security company Gemalto as a subcontractor. The new technology is being used without any data protection guarantees.[27] 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.[28]
- **Proposed deployment of street cameras and closed circuit television:** In 2014, the municipality of Beirut approved Beirut City Surveillance, a project to install about 1,850 cameras in 350 locations around the city. Images collected from these cameras will be piped via the internet to a real-time monitoring room. The USD 36 million project[29] was awarded to Guardia Systems,[30] 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.[31]

4. List of issues

Based on the above observations, SMEX and APC propose the following questions for the List of Issues on Lebanon:

- What steps has the government taken to adopt a data protection law that complies with international standards, and to establish an independent data protection authority to protect personal data?
- Can the government provide information on how it is taking steps towards compliance with international human rights law and standards? In particular, by ensuring the application of the principles articulated in the International Principles on the Application of Human Rights to Communications Surveillance,[32] namely, legality, legitimacy, necessity, adequacy, proportionality, authorisation from a competent judicial authority, due process, user notification, transparency, public oversight, respect for the integrity of communications and systems, safeguards against illegitimate access, and the right to effective remedy.

reasons to impose internet surveillance; political to maintain public security and maintain 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." See: SMEX, "Are internet users in Lebanon illegally monitored?" December 11, 2015. Available in Arabic at: http://bit.ly/2c9Eo1h

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

[26]Inkript, "Our Company." www.inkript.com/our-company .

[27]SMEX, "Questions the Lebanese Government Should Answer about the New Biometric Passports," July 19, 2016. http://www.smex.org/legitimate-questions-about-biometric-passport-lebanese-government-should-answer

[28]The Daily Star, "Lebanon seeking refugee biometric data: Derbas," May 30, 2014. https://www.dailystar.com.lb/News/Lebanon-News/2014/May-30/258268-government-has-refugee-eye-scans-derbas.ashx

[29]InAVateonthenet, "Beirut Surveillance Project protects the city," May 23, 2016. http://www.inavateonthenet.net/case-studies/article/beirut-surveillance-project-protects-the-city

[30]Guardia Systems, "About Us." http://guardiasystems.com/about

[31]SMEX, "2000 Eyes to Surveil Beirut by Year's End," June 13, 2016. http://www.smex.org/2000-eyes-to-surveil-beirut-by-years-end

[32]https://necessaryandproportionate.org/principles

- Has the government investigated claims that illegal communications interception and access to data are routinely undertaken by the security services and other state authorities?
- How is the government ensuring that the illegal interception of communications and access to data are ended and that responsible individuals are held to account, if the claims are verified, and victims are provided redress for the violation they experienced?
- What steps is the government taking to ensure that there are appropriate controls to prevent the use of private surveillance industry products to facilitate human rights abuses?
- How is the government ensuring that the state surveillance of online and offline activities is lawful and does not infringe on human rights defenders' right to freedom of expression and ability to defend human rights, including through the use of information and communication technologies?