PRIVACY INTERNATIONAL

Universal Periodic Review
Stakeholder Report: 23rd Session, Lebanon

The Right to Privacy in Lebanon

Submitted by Privacy International, Social Media Exchange and the Association for Progressive Communication

The Right to Privacy in Lebanon

Stakeholder Report
Universal Periodic Review
23rd Session - Lebanon

Submitted by Privacy International, Social Media Exchange and the Association for Progressive Communication

March 2015

Introduction

1. This stakeholder report is a submission by Privacy International, Social Media Exchange and Association for Progressive Communication. **Privacy International (PI)** is an international human rights organisation that works to advance and promote the right to privacy around the world. The **Social Media Exchange (SMEX)** is a registered Lebanese nonprofit that conducts training, research, and advocacy on strategic communications and human rights in the digital era. The **Association for Progressive Communication (APC)** is an international organization and network with ECOSOC Status. Its mission is to empower and support organizations, social movements and individuals in and through the use of information and communication technologies.

2. Together PI, SMEX and APC wish to bring their concerns about the protection and promotion of the right to privacy in Lebanon before the Human Rights Council for consideration in Lebanon's upcoming review.

The right to privacy

3. Privacy is a fundamental human right, enshrined in numerous international human rights instruments.[1] It is central to the protection of human dignity and forms the basis of any democratic society. It also supports and reinforces other rights, such as freedom of expression, information and association. The right to privacy embodies the presumption that individuals should have an area of autonomous development, interaction and liberty, a "private sphere" with or without interaction with others, free from arbitrary State intervention and from excessive unsolicited intervention by other uninvited individuals.[2]

4. Activities that restrict the right to privacy, such as surveillance and censorship, can only be justified when they are prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued.[3]

5. As innovations in information technology have enabled previously unimagined forms of collecting, storing and sharing personal data, the right to privacy has evolved to encapsulate State obligations related to the protection of personal data.[4] A number of international

---

1 Universal Declaration of Human Rights Article 12, United Nations Convention on Migrant Workers Article 14, UN Convention of the Protection of the Child Article 16, International Covenant on Civil and Political Rights, International Covenant on Civil and Political Rights Article 17; regional conventions including Article 10 of the African Charter on the Rights and Welfare of the Child, Article 11 of the American Convention on Human Rights, Article 4 of the African Union Principles on Freedom of Expression, Article 5 of the American Declaration of the Rights and Duties of Man, Article 21 of the Arab Charter on Human Rights, and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; Johannesburg Principles on National Security, Free Expression and Access to Information, Camden Principles on Freedom of Expression and Equality.

2 Martin Scheinin, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 2009, A/HRC/17/34.

3 Universal Declaration of Human Rights Article 29; General Comment No. 27, Adopted by The Human Rights Committee Under Article 40, Paragraph 4, Of The International Covenant On Civil And Political Rights, CCPR/C/21/Rev.1/Add.9, November 2, 1999; see also Martin Scheinin, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," 2009, A/HRC/17/34.

4 Human Rights Committee general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17).

instruments enshrine data protection principles,[5] and many domestic legislatures have incorporated such principles into national law.[6]

Follow up to the previous UPR

6. There was no mention of the right to privacy and data protection either in the National Report submitted by Lebanon or in the report of the Working Group.

7. However, at the last review, Armenia submitted a recommendation to Lebanon on guaranteeing freedom of expression which read, *"Continue to guarantee freedom of expression[7] creating additional conditions for its fulfilment."*[8]

Domestic laws and regulations related to privacy

8. Article 14 of the Lebanese Constitution does ensure 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."*

9. Articles 8 and 13 of the Constitution indirectly protect the right to privacy[9] with the former guaranteeing individual liberty and the latter freedom of expression. It had been interpreted that these laws include the secrecy of all means of communications, both mail and telephone calls.[10]

10. The Law No. 140 related to the protection of secrecy of communications carried out by all means of communication, 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 mails) is guaranteed and protected by law and cannot be subjected to any forms of tapping, surveillance, interception or violation except in the cases, and by the means and procedures, prescribed by law. Article 98 of the Lebanese Code of Civil Procedures regulates the regime applicable to search and seizures.

11. Whilst there is no data protection framework in place, various laws protect personal data including, Article 2 of the Banking Secrecy Law of September 3, 1956 (the Banking Secrecy Law), and the penal code under Article 579, 580 and 581 relating 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 patients relationships, and Articles 51 and 58 of the Consumer Protection Code (Law no. 659 of 4 February 2005) says that suppliers must not disclose data without the consent of the consumer.

---

5 See the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981; the Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980); and the Guidelines for the regulation of computerized personal data files (General Assembly resolution 45/95 and E/CN.4/1990/72)

6 As of December 2013, 101 countries had enacted data protection legislation: David Banisar, National Comprehensive Data Protection/Privacy Laws and Bills 2014 Map (January 28, 2014). Available at SSRN: http://ssrn.com/abstract=1951416 or http://dx.doi.org/10.2139/ssrn.1951416

7 A/HRC/16/18, Report of the Working Group on the Universal Periodic Review, Lebanon, Human Rights Council, Sixteenth session, Agenda item 6. Available at: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G11/102/11/PDF/G1110211.pdf?OpenElement

8 As noted by Frank La Rue, "The right to privacy is often understood as an essential requirement for the realization of the right to f

9 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

10 HiiL, *The Rule of Law in Lebanon: Prospects and Challenges,* Hill Rule of Law Quick Scan Series, April 2012, pp. 18. Available at: http://www.hiil.org/data//media/Quickscan_Lebanon_160812_digitaal_def.pdf

International obligations related to privacy

12. Lebanon is a signatory to the Universal Declaration of Human Rights ('UDHR'), for which it was on the drafting Committee, and has ratified the International Covenant on Civil and Political Rights ('ICCPR'). Article 17 of the ICCPR, which reinforces Article 12 of the UDHR, provides that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation". The Human Rights Committee has noted that states parties to the ICCPR have a positive obligation to "*adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right [privacy].*"[11]

13. The preamble of the Lebanese Constitution states:
"

"Lebanon is also 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."

14. In addition, the Appeals Chamber's[12] jurisprudence affirms that the right to privacy, as provided for in the UDHR and the ICCPR, has constitutional value under Lebanese law.

15. The International Principles on the Application of Human Rights to Communications Surveillance[13] are not legally binding but provide clarity as to how international human rights law applies in the current digital environment. In order to meet their international human rights obligations to uphold the fundamental right to privacy, States must comply with the principles these principles set out including: legality, legitimate aim, necessity, adequacy, proportionality, competent judicial authority, due process, user notification, transparency, public oversight, integrity of communications and systems, safeguards for international cooperation, safeguards against illegitimate access and right to effective remedy.

16. By co-sponsoring both UN General Assembly on the right to privacy in the digital age, A/RES/68/167 adopted in December 2013 and A/RES/69/166 adopted in December 2014, Lebanon re-affirmed its commitment to promoting, respecting and ensuring the right to privacy as a human right.

Areas of Concern

I. Lack of constitutional protection of the right to privacy

17. The Constitution in Lebanon does not explicitly protect the right to privacy. The Constitution only protects the inviolability of the home, but fails to protect the secrecy of communications.

18. Given the information provided below on the extensive powers of the Lebanese government to conduct surveillance of communications, this Constitutional oversight is worrying, especially in light of the lack of other robust privacy safeguards elsewhere under Lebanese law.

---

11 General Comment No. 16 (1988), para. 1

12 See CH/AC/2011101, Decision on partial appeal by Mr El Sayyed of Pre-Trial Judge's decision of 12 May 2011, 19 July 2011, para. 60 and footnote 102; Lebanese Constitutional Council, decision no. 2/2001, 10 May 200 I, published in Al-majless al-doustouri (200 1-2005) [Constitutional Council review (200 1-2005)], para. 61.

13 See: https://necessaryandproportionate.org/

II. Communication surveillance

19. Lebanon was the first Arab country to introduce, in 1999, a legal framework for the interception of communications, although the law was not adopted by the Cabinet until 2009.

20. The first provision of the Telecommunication Interception Act of 27 October 1999 (thereafter referenced as Law 99/140) establishes the principle according to which the right to make confidential internal or external calls by using telecommunications means (such as fixed telephones, mobile devices of any type whatsoever including cellular phones, fax, e-mail) is protected by the law and is not to be subject to any form of wiretapping, monitoring, interception or disclosure.

21. Law 99/140 restricts any breach of secrecy and limits interferences with privacy to cases of extreme urgency and upon obtaining a judicial or administrative order.

22. 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.

23. 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.

24. As a safeguard against abuse, Article 16 stipulates that such administrative decisions must be verified by an independent judicial commission. The judicial panel consisting 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.

25. Whilst the law seems to provide the necessary safeguards, in practice systematic failures to abide by the law are directly threatening the right to privacy of Lebanon's citizens.

Lack of application of judicial oversight of administrative authorisation

26. Based on information obtained by Al-Ahkbar, a Beirut-based media outlet, 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.[14]

27. This situation is very concerning as allowing a member of the executive branch to authorise the interception of communications undermines accountability and increases the likelihood of arbitrary and politically motivated surveillance. As the UN Special Rapporteur on the freedom

14 Nazzal, M., *The surveillance state: No privacy for the Lebanese,* Al-Akhbar, 13 May 2014. Available at: http://english.al-akhbar.com//19751node

of expression and opinion stated in his 2013 report, Article 12 UDHR implies that "[...] State surveillance of communications must only occur under the most exceptional circumstances and exclusively under the supervision of an independent judicial authority."[15] Political authorisation does not place a sufficient check on what is an extremely invasive intrusion into the enjoyment of the right to privacy.

28. In failing to implement and respect Article 16 of the law, Lebanon is failing to meet its their international human rights obligations in relation to protecting the right to privacy when conducting communications surveillance. Determinations related to communications surveillance must be made by a competent judicial authority that is impartial and independent.[16] In addition, the Lebanese authorities should establish independent oversight mechanisms to ensure the transparency and accountability of the surveillance authorisation processes. The oversight mechanism must be independent of the executive, properly resourced to conduct investigations, and able to command public confidence through regular reporting and public sessions.

Unauthorised bulk interception of data

29. It is clear that at least one Lebanese security agency, the Internal Security Forces ('ISF') engages in the unauthorised bulk interception of data for prolonged periods of time.

30. In December 2012, it was reported that the Information Branch of the ISF had sought the interception and retention of all SMS text messages sent in Lebanon from 13 September to 10 November 2012. The ISF justified its request 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. The details of the types of data requested was contested but a leaked document from the Ministry of Information showed that the types of data included 2G and 3G data subscribers in Lebanon, including log files, IP addresses, usernames, phone numbers, addresses, names, and passwords.[17]

31. Lebanon's Telecommunications Minister, Nicolas Sehnaoui, refused the request[18] but it was reported that the government nevertheless obtained access to this data.[19]

32. In March 2014, another controversial debate arose as the government approved a proposal permitting the ISF full, unrestricted access to the electronic communications data of all Lebanese citizens.[20] Judge Awny Ramadan, head of the Lebanese accountability agency, said that the blanket and arbitrary government requests for the communication data of all four million Lebanese citizens is a violation of the Law 99/140 given that every single citizens cannot be a suspect of a crime.[21] Also, the decision permitted full access for a period of six months, which is far beyond the two months permitted by the Law 99/140 under Article 9.

33. The United Nations International Independent Investigation Commission (UNIIIC), and the Special Tribunal for Lebanon (STL), which were set up to investigate assassinations in the country, particularly that of the late prime minister Rafik Hariri in 2005, have also taken

15 A/HRC/23/40 at para. 81
16 www.necessaryandproportionate.org
17 Bowe, R., *Data Request from Lebanese Security Agency Sparks Controversy*, Electronic Frontier Foundation, 27 December 2012. Available at: https://www.eff.org/deeplinks/2012/12/lebanese-security-agency-user-data-request-sparks-controversy
18 Republic of Lebanon, Ministry of Telecommunication, *The Ministry of Communications will not implement any Data request if it touched the freedoms of the Lebanese and represented an assault to their privacy.* Available at: http://www.mpt.gov.lb/index.php/en/about-mpt-2/mpt-in-press/118-the-ministry-of-communications-will-not--any-data-request-if-it-touched-the-freedoms-of-the-lebanese-and-represented-an-assault-on-their-privacy
19 Chakrani, H., *Lebanon Security Forces: Give Us Your Facebook Password,* Al-Akhbar, 4 December 2012. Available at: http://english.al-akhbar.com/content/lebanon-security-forces-give-us-your-facebook-password
20 Global Voices Advocacy, *Law 140: Eavesdropping on Lebanon*, 10 April 2014. Available at: http://.globalvoicesonline.org/2014/04/11/law-140-eavesdropping-on-lebanon/
21 Ibid

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.[22] There are some cases pending before the Special Tribunal for Lebanon where the expansive access to user data is being challenged.[23]

34. An independent commission in Lebanon confirmed that, even in the context of intelligence gathering, as opposed to judicial investigations, *"providing the full communication database on all Lebanese territories in a periodic manner violates the provisions of effective laws because it amounts to a clear violation of basic freedoms."*[24] This independent commission also considered that the transfer of the full contents of SMSs sent through the two operating mobile telephone companies all over the Lebanese territories was unlawful.[25]

35. These findings comport with that of the UN High Commissioner for Human Rights, Navi Pillay, in her 2014 report on the right to privacy in the digital age, in which she stated that *"that any capture of communications data is potentially an interference with privacy and, further, that the collection and retention of communications data amounts to an interference with privacy whether or not those data are subsequently consulted or used.... The very existence of a mass surveillance programme thus creates an interference with privacy."*[26]

36. The bulk interception of and access to data directly challenges the principles of necessity and proportionality that must be applied when conducting any activities which interfere with fundamental human rights. Communications surveillance (including interception and access to data) should be regarded as a highly intrusive act that interferes with human rights and threatens the foundations of a democratic society. Decisions about such activities must consider the sensitivity of the information accessed and the severity of the infringement on human rights and other competing interests.

Monitoring by non-state actors

37. The US State Department reported in its Human Rights Report of Lebanon in 2013, that "militias and non-Lebanese forces operating outside the area of central government authority also frequently violated citizens' privacy rights. Various factions, such as Hizballah, used informer networks and telephone monitoring to obtain information regarding their perceived adversaries."[27] The ability of non-state actors to conduct communications monitoring is of extreme concern given these activities are unregulated by law which is heightened by the lack of safeguard in place to protect the privacy of citizens.

Purchase of internet monitoring systems

38. In January 2013, the Citizen Lab of the University of Toronto published a research brief[28] in which it reported that researchers had discovered three Blue Coat PacketShaper

22 Freedom House, *Freedom on the Net 2014: Lebanon*. Available at: https://freedomhouse.org/report/freedom-net/2014/lebanon
23 See for example: *Prosecution v Ayyash et al.,* Case No. STL-11-01/T/TC. Available at: Available at: http://www.stl-tsl.org/en/the-cases/stl-11-01/main/filings/replies-and-responses/defence-team-counsel/f1857
24 In an opinion dated 8 November 2012 on a Council of Ministers Decision taken in application of article 9 of Law 140/99 to authorise the transfer of the entire communication data of Lebanon from 19 September 2012 to 31 December 2012 data to security and military agencies, 4D00104
25 In an opinion dated 21 November 2012 on a Council of Ministers Decision taken in application of article 9 of Law 140/99 to authorise the transfer of the full contents of SMSs sent through MIC1 and MIC2 all over the Lebanese territories, 4DOO105.
26 A/HRC/27/37 at para. 20
27 U.S. State Department, *Lebanon 2013 Human Rights Report*. Available at : http://www.state.gov/documents/organization/220575.pdf
28 CitizenLab, *Planet Blue Coat: Mapping Global Censorship and Surveillance Tools*, Research Brief, Number 13, January 2013, University of Toronto, MUNK School of Global Affairs. Available at: https://citizenlab.org/wp-content/uploads/2013/01/Planet-Blue-Coat.pdf

installations[29] 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.[30] Whilst such tools can be used for legitimate aims, such as controlling bandwidth costs, they also have the functionality to permit 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)."[31]

39. The discovery of the installations came in the context of the government drafting a regulation pertaining to controlling online content concerning public morals. Although this draft regulation was later abandoned, the researchers noted that this was an interesting finding given that Lebanon did not have a history of internet filtering prior to the publication of the draft regulation.[32]

Limiting access to internet and mobile services

40. Often held out to be one of the more liberal countries in the region in terms of openness and diversity of the media, limitations on the freedom to express do occur in Lebanon[33] and there have been several alleged attempts by State institutions and non-State actors to censor or shut down online forums and social media platforms.[34]

41. Research conducted by Social Media Exchange into the blocking of websites in Lebanon in 2013 showed that the blocking of websites is being done inconsistently across ISPs.[35]

42. In accordance with the 2002 Telecommunication Act[36], some Voice over Internet Protocol (VoIP) applications are blocked, but some not all.[37] There seems to be no clear and transparent policy as to how such decisions are made. The government claims that VoIP are impossible to ban but must be deregulated as they causes millions of dollars of loss, "The Ministry teams are currently working on a formula that would allow private operators to sell the service, provided they share revenues with the State".[38] VoIP applications are more secure, and thus an increasing number of individuals are resorting to using them such as journalists, political activists, but if people are forced to use traditional phone lines, then there is a concern that it is providing the government with an increase ability to conduct surveillance.

Restrictions and limitation on anonymity

29 Ibid, pp. 25. "All three were initially identified by Shodan in December 2012 and were verified as accessible. These were on netblocks associated with Hughes Network Systems, which is a satellite-based Internet provider. The hostnames of the IP addresses of these installations resolve to the iWayAfrica domain, which is an African provider of broadband Internet service."
30 Blue Coat, *Applications that Blue Coat PacketShaper Classifies and Controls*. Available at: http://.bluecoat.com/sites/default/files/documents/files/PacketShaper_Application_List.c.pdf
31 CitizenLab, *Appendix A: Summary Analysis of Blue Coat "Countries of Interest*, 15 January 2015. Available at: www://citizenlab.org/2013/01/appendix-a-summary-analysis-of-blue-coat-countries-of-interest/
32 CitizenLab, *Planet Blue Coat: Mapping Global Censorship and Surveillance Tools*, Research Brief, Number 13, January 2013, University of Toronto, MUNK School of Global Affairs. Available at: https://citizenlab.org/wp-content/uploads/2015/03/Planet-Blue-Coat-Mapping-Global-Censorship-and-Surveillance-ToolsPlanet-Blue-Coat-Mapping-Global-Censorship-and-Surveillance-Tools.pdf
33 Zayadin, H., *Lebanese government moves to control expression in the online realm*, IFEX, 28 March 2014. Available at: https://www.ifex.org/lebanon/2014/03/28/bloggers_facing_threats/
34 Freedom House, *Freedom on the Net 2014: Lebanon*. Available at: https://freedomhouse.org/report/freedom-net/2014/lebanon
35 Social Media Exchange, *Blocked websites in Lebanon 2013*,8 January 2014. Available at: http://www.smex.org/blocked-websites-in-lebanon-2013/
36 Telecommunication Law 431/2002. Available at: http://www.tra.gov.lb/Telecom-Law-431-2002
37 Freedom House, *Freedom on the Net 2014: Lebanon*. Available at: https://freedomhouse.org/report/freedom-net/2014/lebanon
38 Ministry of Telecommunications, *Progress Report 2013*, pp. 30. Available at: http://www.tayyar.org/tayyar/tempMOT_2013_En.pdf

43. There have been unconfirmed reports of extralegal methods used to identify anonymous online users.

44. A report by the Open Society Foundation notes how such incidents remain low-profile and are often not reported by the individual as they feel intimidated and threatened.[39]

45. When anonymity is challenged or undermined this means that citizens, and in particular those speaking out against the government, have little or no protection from surveillance, facilitating the government's efforts to monitor and identify them.

Lack of oversight of security agencies

46. There are several state institutions which have the power to conduct surveillance and access user data, namely the General Directorate of General Security.[40], the General Directorate of Internal Security Forces (ISF)[41] and the Army Intelligence Directorate.

47. The General Directorate of General Security, is a Lebanese intelligence agency, which was founded on 21 July 1921. With the adoption of Decree No. 139 of 12 June 1959, the General Security Directorate became a special branch of the Ministry of Interior. Its main task and function is to collect and gather Intelligence, and to inform the Lebanese government with the aim of ensuring the national security and public order throughout the territory of the Republic of Lebanon.

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

49. The Cybercrime and Intellectual Property Rights Bureau officially operates under the umbrella of the judicial police but its legality is contested, given that it was established under a memorandum of service rather than by the Law or Decree.[42] There have been reports of the Bureau acting as a censorship authority mainly targeting journalists, bloggers and online activists.[43] Its expansive powers illustrate the poor oversight under which in operates, and raises concerns as to the lack of safeguards protecting privacy and regulating the powers of the Bureau.

50. Article 16 of the Law 99/140 restricts the powers of the Ministry of Interior to wiretap, but in practice this provision does not seem to be respected. It was reported by *A*l-Akhbar, a Beirut-based media outlet, based on information obtained from high-level judicial and parliamentary sources 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 away from any legal oversight."[44] In addition, in the same article, 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."

39 Open Society Foundations, *Mapping Digital Media: Lebanon,* 15 March 2012, pp. 92. Available at: http://.opensocietyfoundations.org/sites/default/files/mapping-digital-media-lebanon-20120506.pdf
40 General Directorate of General Security. See: http://www.general-security.gov.lb/Default.aspx?lang=en-us
41 Interior Security Forces. See: http://www.isf.gov.lb/en
42 Al-Akhbar, Cybercrime Bureau's ever-growing powers threatening freedoms in Lebanon, 22 November 2014. Available at: http://english.al-akhbar.com/node/22605
43 Zayadin, H., *Lebanese government moves to control expression in the online realm*, IFEX, 28 March 2014. Available at: https://www.ifex.org/lebanon/2014/03/28/bloggers_facing_threats/
44 Nazzal, M., *The surveillance state: No privacy for the Lebanese,* Al-Akhbar, 13 May 2014. Available at: *http*://english.al-akhbar.com//19751node

51. These various security agencies are failing ensure that their policies and practices adhere to international human rights and adequately protect the rights to privacy and freedom of expression. The different various security services, their remit and operations must be reviewed to meet/ the standards set by International Principles on the Application of Human Rights to Communications Surveillance.[45] The State should be transparent about the use and scope of communications surveillance techniques and powers.

Foreign spying

52. There have been on-going reports of attempts by the Israeli government to infiltrate the Lebanese telecommunication system.[46] Incidents have occurred after announcement of Israel having destroyed spying equipment in Lebanon which was then discovered by the Lebanese authorities. Such incidents took place in December 2011, February and July 2012,[47] and more recently in September 2014.[48]

53. In 2012, Kaspersky Lab[49], a Russian multinational computer security company, published 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 infected machines were in Lebanon.[50] The research was unable to determine whether the bank component of the malware was used to spy on financial/banking transaction or steal money, but some have argued that given in was state-created, it is likely the motivation was not only economic gain but sought counterintelligence data too.[51]

54. Such spying facilities and use of such sophisticate espionage tools directly threaten the privacy of Lebanese citizens as well as the security of the telecommunication network and infrastructure, and the financial sector. These threats emphasise the need for the implementation of strong data protection standards to ensure that the Lebanese government meets its international legal obligations to protect the privacy of its citizens from external threats.

III. Data protection

55. Lebanon does not have a law regulating the protection of personal data. Privacy is regulated by other provisions as outlined above, including the Law 99/140 related to the protection of secrecy of communications carried out by all means of communication, the law 03/09/1956 on banking secrecy, and the penal code under Article 579, 580 and 581 relating to the violation of secrets.

45 Launched in September 2013 following a year of consultation, the International Principles on the Application of Human Rights to Communications Surveillance a set of standards that interpret States' human rights obligations in light of new technologies and surveillance capabilities. The Principles are endorsed by 410 civil society organisations around the world, over 40 leading experts, academics and prominent individuals, as well as 4 elected officials. The Principles set for the first time an evaluative framework for assessing surveillance practices in the context of international human rights law. Please refer to the www.necessaryandproportionate.org website for further details.

46 Freedom House, *Freedom on the Net 2014: Lebanon*. Available at: https://freedomhouse.org/report/freedom-net/2014/lebanon

47 BBC News, *Israel destroys 'spy devices' in souther Lebanon*, 3 July 2012. Available at: http://www.bbc.co.uk/news/world-middle-east-18691792

48 The Associated Press and Khoury, J., *Israel detonates spying device in south Lebanon*, report says, 6 September 2014. Available at: http://www.haaretz.com/news/diplomacy-defense/1.614343

49 Kaspersky,*Kaspersky Lab Discovers 'Gauss' – A New Complex Cyber-Threat Designed to Monitor Online Banking Accounts,* 9 August 2012. Available at: http://www.kaspersky.com/about/news/virus/2012/Kaspersky_Lab_and_ITU_Discover_Gauss_A_New_Complex_Cyber_Threat_Designed_to_Monitor_Online_Banking_Accounts

50 Raad, M., *Surveilling the banking sector in Lebanon,* published in Global Information Society Watch 2014: Communications Surveillance in the Digital Age. Available at: http://giswatch.org/en/country-report/communications-surveillance/lebanon

51 Zetter, K., *Flame and Stuxnet cousin target Lebanese bank customer carries mysterious payload*, Wired, 8 September 2012. Available at: http://www.wired.com/2012/08/gauss-espionage-tool/

56. Given the lack of a data protection regime, the current issues of concern in the area of data protection include:

Unique ID number e-government initiative and the impending deployment of biometric passports

57. In 2002, Lebanon launched its first e-government initiative which was then updated in 2007 to include the establishment of a Unique Identity Number (UIN) under the 'e-citizen' pillar of the strategy. The government noted that this was a pre-requisite to the Smart card.[52] The identity card includes 10 fingerprints and palm prints as well as the holder's mother's and father's name.
58. In 2013, the government of Lebanon announced that it would start using biometrics passports as a result of a request by the United National International Civil Aviation Organization (ICAO). ICAO has set a deadline of 24 November 2015 for all of its members to adopt biometric technologies.

59. It was recently announced[53] that Inkript, a Lebanon-based Resource Group Holding (RGH), who had submitted a joint offer with Gemalto, a digital security company with its headquarters in the Netherlands, had won the tender to supply Lebanon with security-print biometric passports. Inkript would manage the programming and software development in-house, and Gemalto would be in charge of manufacturing the passports and the match programme's interface with the coding machines.

60. The passport will include a SIM card-sized chip which would include data on the identify and criminal history of the passport holder as well as fingerprints and facial recognition.

61. Given the lack of a data protection framework and a robust Constitutional protection of the right to policy, biometric passports will be deployed in a complete legal void which will fail to regulate and limit the purpose of the use of biometric data of citizens. Thus, it can potentially be used as a tool for surveillance through profiling, data mining and big data analysis.

62. The use of biometric technology can be problematic:[54]
    - The data processed is at risk of being misused and is subject to fraud;
    - It can result in misidentification and inaccuracies;
    - Its nature renders it exclusionary
    - Its unregulated retention raises questions of "function creep" (uses of biometric data for purposes for which it was not originally collected) and concerns around the safety of the data

63. Additionally, the physical or digital structure in which biometric data is stored must be developed to ensure the safety of the data. If they are to be used, centralised mass data systems must be regulated by clear legislation in order to eliminate the possibility of the government or third parties (i.e. private sector actors) taking advantage of the existence of the data for (new) unforeseen purposes.

64. An additional concern is the involvement of a non-Lebanese company, Gemalto, in the process raises concerns as to the ownership of data, and the responsibility and accountability of the government and the company to protect the data from abuse, theft, and loss. Given that Lebanon does not have a data protection law, it is essential that the government takes the steps necessary to ensure the protection of its citizens' personal data

52 Minister of State for Administrative Reform, *High Level e-government strategy Document: Lebanon*, e-Gov 2007, pp. 12. Available at: http://www.omsar.gov.lb/Cultures/en-US/Publications/Strategies/Documents/4a8c1c25f5f9444aa94923c5e4d38cacHighLevelEGovernmentStrategyAM21Jan08.pdf

53 Bank Audi, *The Lebanon Weekly Monitor*, February 23-March, 01, 2015, Week 09, p. 9. Available at: http://www.bankaudi.com.lb/GroupWebsite/openAudiFile.aspx?id=2534

54 Privacy International (2013) *Biometrics: Friend or foe of privacy?* Available at: https://www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/biometrics_friend_or_foe.pdf

when engaging with third parties. Given the recent revelations that Gemalto's office network had been the target of attacks in 2010 and 2011, "probably"[55] by the NSA, the U.S. intelligence agency, and GCHQ, the British intelligence agency, it is important to note how such companies have now become the target of intelligence agencies, and so they are vulnerable to attacks.

Data retention[56]

65. It was reported in 2013, that an order issued on 7 June 2013 by the Public Prosecutor's office requested 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.[57] 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."[58] The order also outlines the type of user data that must retained including the username, user's IP address, the websites to which s/he connected, and the protocols used in the process, in addition to specifying the user's location.

66. Data retention is broadly presented as a method to combat serious crime such as organized crime and terrorism[59]. These goals are generally considered adequate objectives to attempt to combat. That does not mean that all measures taken in achieving that objective are legitimate, and it raises question of necessity and proportionality.[60]

67. As was noted by the UN Office of the High Commissioner for Human Rights (OHCHR) in its report on the right to privacy in the digital age,[61] *"any capture of communications data is potentially an interference with privacy and, further, that the collection and retention of communications data amounts to an interference with privacy whether or not those data are subsequently consulted or used. Even the mere possibility of communications information being captured creates an interference with privacy with a potential chilling effect on rights, including those to free expression and association."*

E-transaction bill

68. In 2010, Lebanon proposed a new Law on electronic transactions.[62] The Law was intended to address multiples 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 freedoms.

---

55 Gemalto, *Gemalto presents the findings of its investigations into the alleged hacking of SIM card encryption keys by Britain's Government Communications Headquarters (GCHQ) and the U.S. National Security Agency (NSA)*, 25 February 2015. Available at: http://www.gemalto.com/press/Pages/Gemalto-presents-the-findings-of-its-investigations-into-the-alleged-hacking-of-SIM-card-encryption-keys.aspx

56 Privacy International, *Mass Surveillance*, Privacy 101. Available at: https://www.privacyinternational.org/resources/privacy-101/mass-surveillance

57 Freedom House, *Freedom on the Net 2014: Lebanon*. Available at: https://freedomhouse.org/report/freedom-net/2014/lebanon

58 Nash, M., *Providers tracking customers' Internet use*, Now, 29 November 2013. Available at: https://now.mmedia.me/lb/en/reportsfeatures/523209-523209-523209-providers-tracking-customers-internet-use

59 Digital Rights Ireland v Minister for Communications, Marine and Natural Resources et al., European Court of Justice, C-293/12, para. 41-44. Available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=322968.

60 Klass and Others v Germany, European Court of Human Rights, Application No. 5029/71, para. 49. Available at: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57510

61 A/HRC/27/37, para 20

62 Khaddaj, A., *Lebanon's proposed internet law struggles to gain IT sector support*, Al-Shorfa, 17 August 2011. Available at: http://al-shorfa.com/en_GB/articles/meii/features/main/2011/08/17/-02

69. 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. and Article 70 on the Electronic Signature & Services Authority, a new regulatory and licensing body with practically unchecked powers. One main criticism was that the Bill had not been opened for public consultation thus failing to allow civil society and other stakeholders from contributing and being part of the law making process.[63]
70. In 2012, the E-transaction bill was sent to Parliament under Decree, No. 9341 dated of 8 October 2012, but this law remains a draft law.

Recommendations

71. We recommend that the government of Lebanon to:

- Recognise and take steps towards compliance with international human rights law and standards by ensuring the application of the following principles to communication surveillance as articulated in the International Principles on the Application of Human Rights to Communications Surveillance namely, legality, legitimacy, necessity, adequacy, proportionality and respecting process of authorisation from a competent judicial authority, with due process, user notification, transparency, public oversight and respect for the integrity of communications and systems as well as ensuring safeguards against illegitimate access and right to effective remedy;

- Investigate claims that illegal communications interception and access to data is routinely undertaken by the security services and other state authorities; ensure that such practices are ended and responsible individuals held to account if the claims are verified and victims redressed for the violation they experienced;

- Ensure that there are appropriate controls to prevent the use of private surveillance industry products to facilitate human rights abuses;

- Ensure 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 use of the information communication technologies;

- Immediately enact data protection legislation that complies with international standards;

- Establish an independent data protection authority

- Make further efforts to ensure freedom of opinion and expression in the country, including by ensuring that blocked or filtered websites are based on lawful criteria.

63 Social Media Exchange, *ACT NOW: Postpone the Vote on the E-Transaction Law*, 14 June 2010. Available at: http://www.smex.org/act-now-postpone-the-vote-on-the-e-transactions-law/